

Jean Franchini
Jean-Claude Jacquens

Agrégation
interne

L'oral en poche

Agrégation interne de mathématiques



2^e édition

ellipses

Leçon 101 : Groupes monogènes, groupes cycliques. Exemples.

Prérequis : groupes, sous-groupes, morphismes de groupes, structures d'anneaux de \mathbb{Z} , de $\mathbb{Z}/n\mathbb{Z}$, structure de groupe multiplicatif de \mathbb{C}^\star .

G désigne un groupe, n un élément de \mathbb{N}^\star .

1. Groupe monogène

1.1. Définition

G est monogène s'il est engendré par l'un de ses éléments g ,
ie. s'il est additif, $G = \{kg \mid k \in \mathbb{Z}\}$ et, s'il est multiplicatif, $G = \{g^k \mid k \in \mathbb{Z}\}$.

Remarque : un tel groupe est commutatif, la loi sera l'addition sauf mention contraire.

1.2. Surjection

Si g engendre G alors $\varphi : \mathbb{Z} \rightarrow G, k \mapsto kg$ est un morphisme surjectif.

1.3. Groupe monogène infini

Si G est monogène infini engendré par g alors le morphisme précédent est un isomorphisme. Le seul groupe monogène infini est donc \mathbb{Z} à isomorphisme près.

1.4. Exemples de groupes monogènes de cardinal n .

$\mathbb{Z}/n\mathbb{Z}$ est un groupe additif monogène de cardinal n , l'ensemble \mathbb{U}_n des racines n -ièmes de 1 est un sous-groupe multiplicatif de \mathbb{C}^\star monogène de cardinal n .

De plus $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{U}_n, k \mapsto e^{2ik\pi/n}$ est un isomorphisme.

2. Ordre d'un élément

2.1. Définition

Soient $g \in G$ puis f le morphisme de \mathbb{Z} dans G défini par : $\forall k \in \mathbb{Z}, f(k) = kg$.
On dit que g est d'ordre fini si f n'est pas injective.
Dans ce cas l'ordre de g est l'unique élément n de \mathbb{N}^\star tel que $\text{Ker}(f) = n\mathbb{Z}$.

Remarque : avec les notations précédentes $n = \min \{k \in \mathbb{N}^\star \mid kg = 0\}$.

2.2. Application

une partie finie non vide H d'un groupe additif G en est un sous-groupe si, et seulement si, elle est stable par l'addition.

3. Groupe cyclique

3.1. Définition

G est cyclique s'il est monogène et fini.

3.2. Théorème

À isomorphisme près $\mathbb{Z}/n\mathbb{Z}$ est le seul groupe cyclique additif de cardinal n .

3.3. Théorème

Si $d \in \mathbb{N}^\star$ alors \mathbb{U}_d est le seul sous-groupe de \mathbb{C}^\star de cardinal d .

Corollaire 1

| Soit $d \in \llbracket 1, n \rrbracket$. \mathbb{U}_d est un sous-groupe de \mathbb{U}_n de cardinal d si, et seulement si, d divise n .

Remarque : cela veut aussi dire que le cardinal d d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est un diviseur de n et que, pour chaque diviseur d de n , $\mathbb{Z}/n\mathbb{Z}$ a un et un seul sous-groupe de cardinal d et que ce sous-groupe est cyclique.

Corollaire 2

| Tout sous-groupe d'un groupe monogène est monogène

3.4. Générateurs de $\mathbb{Z}/n\mathbb{Z}$ **3.4.1. Théorème et définition**

| L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
| On note $\varphi(n)$ son cardinal.

3.4.2. Théorème

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

4. Exemples**4.1. Nombre premier**

| Un groupe dont le cardinal est un nombre premier est cyclique.

4.2. Groupe d'un polygone régulier

| Le groupe des isométries directes laissant invariant un polygone régulier à n sommets est cyclique de cardinal n .

4.3. Groupe engendré par un r -cycle

Un r -cycle de \mathfrak{S}_n engendre un groupe cyclique de cardinal r .

Théorème

| Deux cycles de \mathfrak{S}_n commutent si ou bien leurs supports sont disjoints ou bien ils engendrent le même groupe.

4.4. Groupe des unités de $\mathbb{Z}/p\mathbb{Z}$

| Si p est un nombre premier le groupe des unités de $\mathbb{Z}/p\mathbb{Z}$ est cyclique.

Remarque : plutôt que d'examiner les unités de $\mathbb{Z}/p^n\mathbb{Z}$ on peut plutôt montrer que le groupe des unités de $\mathbb{Z}/2^n\mathbb{Z}$ n'est pas cyclique si $n \geq 3$.

Développements possibles :

le théorème 3.3. et ses corollaires ;

le théorème 3.4.2 ;

un des exemples à l'exception du premier. Bien entendu l'exemple 4.2 est bien plus facile que les deux autres.

Leçon 102 : Permutations d'un ensemble fini, groupe symétrique. Applications

Prérequis : groupes, algèbre linéaire

n désigne un entier naturel supérieur ou égal à 2.

1. Groupe symétrique

1.1. Définition

On appelle permutation de $\llbracket 1, n \rrbracket$ toute bijection de $\llbracket 1, n \rrbracket$ sur lui-même, l'ensemble de ces permutations est un groupe pour la composition appelé groupe symétrique de $\llbracket 1, n \rrbracket$ et noté \mathfrak{S}_n . Son neutre est noté e , son cardinal est $n!$.

Remarques

- Si E est un ensemble de cardinal n et si φ est une bijection de E sur $\llbracket 1, n \rrbracket$ alors, en notant $\text{Bij}(E)$ l'ensemble des bijections de E sur lui-même, $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ est un morphisme bijectif de groupes entre $\text{Bij}(E)$ et \mathfrak{S}_n .
- \mathfrak{S}_n n'est commutatif que si $n = 2$, cyclique que si $n = 2$.

On se limitera par la suite à l'étude de \mathfrak{S}_n .

1.2. Support et orbites

Soit $\sigma \in \mathfrak{S}_n$.

On appelle support de $\sigma \in \mathfrak{S}_n$ l'ensemble des éléments k de $\llbracket 1, n \rrbracket$ tels que $\sigma(k) \neq k$, on le note $\text{Supp}(\sigma)$.

Comme \mathfrak{S}_n est un groupe fini σ est d'ordre fini r et engendre un groupe $\langle \sigma \rangle$ qui opère sur $\llbracket 1, n \rrbracket$ par $(\sigma^p, k) \mapsto \sigma^p(k)$.

Si $k \in \llbracket 1, n \rrbracket$ son orbite est $\mathcal{O}(k) = \{\sigma^p(k) \mid p \in \llbracket 0, r-1 \rrbracket\}$, son cardinal est un diviseur de r , elle est réduite à k si k est un point fixe de σ et les autres orbites forment une partition de $\text{Supp}(\sigma)$.

1.3. Transpositions

1.3.1. Définition

Une transposition est un élément τ de \mathfrak{S}_n dont le support est de cardinal 2.

Si son support est $\{i, j\}$ on la note (i, j) .

Propriété : le centre de \mathfrak{S}_n est réduit à son élément neutre.

Théorème

Tout élément de \mathfrak{S}_n est produit d'au plus $n - 1$ transpositions.

La partie $\{(1, i) \mid i \in \llbracket 2, n \rrbracket\}$ est une partie génératrice minimale de \mathfrak{S}_n .

1.4. Signature

1.4.1. Définition

Soient $\sigma \in \mathfrak{S}_n$ et $(i, j) \in \llbracket 1, n \rrbracket^2$ tel que $i < j$. On dit que (i, j) est en inversion pour σ si $\sigma(j) < \sigma(i)$. La permutation σ est dite paire si elle présente un nombre pair d'inversions, elle est dite impaire sinon.

La signature $\varepsilon(\sigma)$ de la permutation σ est 1 si elle est paire, -1 sinon.

Comme σ est une permutation de $\llbracket 1, n \rrbracket$ on a également $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

1.4.2. Théorème

| ε est un morphisme surjectif du groupe σ_n sur le groupe $\{-1, 1\}$.

1.4.3. Définition

| Le noyau du morphisme ε , ensemble des permutations paires, est appelé groupe alterné et noté \mathcal{A}_n , c'est un sous-groupe distingué de \mathfrak{S}_n de cardinal $n!/2$.

Propriété : le centre de \mathcal{A}_n est réduit à l'élément neutre.

1.5. Cycles**1.5.1. Cycles**

| Si $r \in \llbracket 2, n \rrbracket$ on dit qu'un élément σ de \mathfrak{S}_n est un r -cycle si sous son action l'ensemble $\llbracket 1, n \rrbracket$ a une orbite de cardinal r , toutes les autres orbites étant réduites à un point.

1.5.2. Théorème

| Deux cycles dont les supports sont disjoints commutent. Si deux cycles commutent et ont des supports non disjoints alors ils engendrent le même groupe.

1.5.3. Théorème

| Toute permutation est produit de cycles à supports disjoints, cette décomposition est unique à l'ordre près des facteurs.
 | $((1, 2), (1, 2, \dots, n))$ est une famille minimale de générateurs du groupe \mathfrak{S}_n .

1.5.4. Génération de \mathcal{A}_n

| $\{(1, 2, k) \mid k \in \llbracket 3, n \rrbracket\}$ engendrent le groupe \mathcal{A}_n si $n \geq 3$.

2. Applications**2.1. Théorème de Cauchy**

| Soient (G, \cdot) un groupe fini d'ordre n et p un nombre premier divisant n .
 | Le nombre de solutions dans E de l'équation $x^p = 1$ est divisible par p .

2.2. Groupe d'un tétraèdre régulier

| Le groupe G des isométries laissant un tétraèdre régulier invariant est isomorphe à \mathfrak{S}_4 et le sous-groupe des rotations est isomorphe à \mathcal{A}_4 .

2.3. Déterminants

Soit E un espace vectoriel de dimension n .

Théorème

1. Si $\mathcal{B} = (e_1, \dots, e_n)$ est une base de E , il existe une unique forme n -linéaire alternée f sur E telle que $f(e_1, \dots, e_n) = 1$. On l'appelle déterminant dans la base \mathcal{B} et on la note $\det_{\mathcal{B}}$.
2. Caractérisation du caractère basique d'une famille de vecteurs.
3. Déterminant d'un endomorphisme, composition, cas des automorphismes.
4. Déterminant d'une matrice carrée, produit, inversibilité, transposition.

Développements possibles :

théorème 1.4.2, théorème 1.5.3 ou une partie du théorème sur les déterminants.

Leçon 103 : Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

Prérequis : arithmétique de \mathbb{Z} , groupes, anneaux

n désigne un élément de \mathbb{N}^* .

1. Définition de $\mathbb{Z}/n\mathbb{Z}$

1.1. Congruence

| Si $(a, b) \in \mathbb{Z}^2$ on dit que a est congru à b modulo n et on écrit $a \equiv b [n]$ si $a - b \in n\mathbb{Z}$.

Remarque : la congruence modulo n est une relation d'équivalence.

1.2. Définitions

| L'ensemble quotient de \mathbb{Z} par cette relation est noté $\mathbb{Z}/n\mathbb{Z}$.

| Si $a \in \mathbb{Z}$ on note $Cl_n(a)$ sa classe d'équivalence.

2. Structure d'anneau

2.1. Proposition

| Si $(a, b) \in \mathbb{Z}^2$, les relations $Cl_n(a) + Cl_n(b) = Cl_n(a + b)$ et $Cl_n(a)Cl_n(b) = Cl_n(ab)$ définissent des lois internes dans $\mathbb{Z}/n\mathbb{Z}$ qui en font un anneau commutatif.

2.2. Sous-groupes additifs

Soit p un diviseur de n , $n = pq$.

Théorème

| $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe de cardinal p , il est engendré par $Cl_n(q)$.

2.3. Surjection canonique et idéaux

| L'application $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $k \mapsto Cl_n(k)$ est un morphisme surjectif d'anneaux dont le noyau est $n\mathbb{Z}$. Tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est principal.

2.4. Unités

2.4.1. Définitions

| L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est noté \mathcal{U}_n , c'est un groupe multiplicatif commutatif, on l'appelle aussi groupe des unités.

| Son cardinal est noté $\varphi(n)$. L'application φ est appelée indicatrice d'Euler.

2.4.2. Théorème

| Si $a \in \mathbb{Z}$ alors $Cl_n(a) \in \mathcal{U}_n \iff \text{pgcd}(a, n) = 1$.

| \mathcal{U}_n est l'ensemble des générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

2.5. Structure de corps

2.5.1. Théorème

| $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, $\mathbb{Z}/n\mathbb{Z}$ est intègre ou encore si, et seulement si, n est un nombre premier.

2.5.2. Petit théorème de Fermat

| Soient p un nombre premier et x un nombre entier.

| Si $x \notin p\mathbb{Z}$ alors $x^{p-1} \equiv 1 [p]$. Dans tous les cas $x^p \equiv x [p]$.

Corollaire

Si p est un nombre premier distinct de 2 et si $x \in \mathcal{U}_p$ alors x est le carré d'un élément de \mathcal{U}_p si, et seulement si, $x^{\frac{p-1}{2}} = 1$.

2.5.3. Théorème de Wilson

Si p est un nombre premier alors $(p-1)! \equiv -1 \pmod{p}$.

2.6. Théorème chinois**2.6.1. Théorème**

$\mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $Cl_{mn}(x) \mapsto (Cl_m(x), Cl_n(x))$ est un isomorphisme d'anneaux si m et n sont premiers entre eux.

Remarque : si $mu + nv = 1$ et $(a, b) \in \mathbb{Z}^2$ alors $Cl_{mn}(mub + nva)$ est l'antécédent de $(Cl_m(a), Cl_n(b))$ par l'application précédente. On vient donc d'explicitier l'isomorphisme réciproque.

2.6.2. Indicatrice d'Euler

Si p_1, \dots, p_k sont les nombres premiers distincts intervenant dans la décomposition de n alors $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$. D'autre part $n = \sum_{d|n} \varphi(d)$.

3. Applications**3.1. Exercice**

Si p est un nombre premier et $p \geq 5$ on écrit $\sum_{i=1}^{p-1} \frac{1}{i} = \frac{A_p}{B_p}$ irréductible dans \mathbb{Q} .

Montrer $A_p \equiv 0 \pmod{p^2}$.

3.2. Application du théorème chinois

Soit $(m, n, a, b) \in (\mathbb{N}^*)^2 \times \mathbb{Z}^2$. Résoudre dans \mathbb{Z} le système $(\Sigma) \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$

3.3. Critère d'Eisenstein

Soit $A = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier.
Si p divise tous les coefficients de A à l'exception de a_n et si p^2 ne divise pas a_0 alors A est irréductible dans $\mathbb{Q}[X]$.

3.4. Point périodique d'un endomorphisme

Soient ℓ un automorphisme de \mathbb{R}^n . On suppose que \mathbb{Z}^n est stable par ℓ et par ℓ^{-1} et que ℓ n'admet aucune valeur propre complexe de module 1. Un élément x de \mathbb{R}^n est appelé point périodique s'il existe un entier naturel non nul p tel que $\ell^p(x) - x \in \mathbb{Z}^n$.

Alors x est périodique si, et seulement si, $x \in \mathbb{Q}^n$.

3.5. Théorème des deux carrés

Un entier est somme de deux carrés d'entiers si, et seulement si, dans sa décomposition en produit de facteurs premiers les exposants des nombres premiers congrus à 3 modulo 4 sont pairs.

Développements possibles :

2.3. mais c'est un peu rapide, 2.6.2 ou 3.2.

Leçon 104 : Structures quotients, exemples et applications

Prérequis : Équivalence, loi de composition, structures algébriques, morphisme.

1. Ensembles

\mathcal{R} désigne une relation d'équivalence sur E , si $x \in E$ on note \bar{x} sa classe d'équivalence.

1.1. Théorème et définition

L'ensemble des classes d'équivalence est une partition de E , l'ensemble de ces classes d'équivalence est appelé ensemble quotient de E par \mathcal{R} et est noté E/\mathcal{R} .

L'application $\pi : E \rightarrow E/\mathcal{R}$, $x \mapsto \bar{x}$ est surjective et appelée projection canonique.

1.2. Exemple fondamental

Si H est un sous-groupe d'un groupe $(G, *)$ la relation \mathcal{R} définie sur G par $g\mathcal{R}h$ si $gh^{-1} \in H$ est une équivalence, l'ensemble quotient est noté G/H , si $n \in \mathbb{N}^*$ la relation \mathcal{R} définie sur \mathbb{Z} par $a\mathcal{R}b$ si $a - b \in n\mathbb{Z}$ est une équivalence et le quotient est de cardinal n et noté $\mathbb{Z}/n\mathbb{Z}$.

1.3. Théorème de factorisation

Si f est une application de E dans F il existe une unique application g de E/\mathcal{R} dans F telle que $f = g \circ \pi$ si, et seulement si, la restriction de f à chaque classe d'équivalence est constante.

g est injective si, et seulement si, $(\forall (x, y) \in E^2, f(x) = f(y) \iff x\mathcal{R}y)$

g est surjective si, et seulement si, f l'est.

1.4. Compatibilité avec une loi interne

Si \top est une loi interne sur E on dit que \mathcal{R} est compatible avec \top si

$$\forall (x, y) \in E^2, x' \in \bar{x} \text{ et } y' \in \bar{y} \Rightarrow x \top y = x' \top y'$$

Dans ce cas $\bar{x} \top \bar{y} = \overline{x \top y}$ définit une loi de composition interne sur E/\mathcal{R} encore notée \top et π est un morphisme. De plus si f est un morphisme de (E, \top) dans (F, \perp) et si la restriction de f à chaque classe d'équivalence est constante alors la solution g du théorème de factorisation est un morphisme de $(E/\mathcal{R}, \top)$ dans (F, \perp) .

2. Groupes

G désigne un groupe multiplicatif et H en est un sous-groupe.

2.1. Sous-groupe normal

La relation \mathcal{R} définie sur G par $g\mathcal{R}h$ si $gh^{-1} \in H$ est compatible avec la loi de G si, et seulement si, $\forall g \in G, g^{-1}Hg \subset H$; on dit alors que H est un sous-groupe normal de G et on note $H \triangleleft G$. Dans ce cas la loi de G induit une loi de groupe sur G/H et π est un morphisme.

On remarquera que si G est commutatif tout sous-groupe est normal.

2.2. Théorème de factorisation

Si $H \triangleleft G$ et $f \in \text{Hom}(G, G')$ où G' est un groupe alors le théorème de factorisation admet une unique solution g si, et seulement si, $H \subset \text{Ker}(f)$. Si c'est le cas alors g est un morphisme de groupes, de plus il est injectif si, et seulement si, $H = \text{Ker}(f)$.

2.3. Exemples

$\mathbb{R}/2\pi\mathbb{Z}$ est isomorphe au groupe \mathbb{U} des nombres complexes de module 1, si \mathbb{K} est un corps $\text{GL}_n(\mathbb{K})/\text{SL}_n(\mathbb{K})$ est isomorphe à \mathbb{K}^* .

2.4. Corollaire

À isomorphisme près le seul groupe cyclique d'ordre n est $\mathbb{Z}/n\mathbb{Z}$ ou encore \mathbb{U}_n , groupe des racines complexes n -ièmes de l'unité. Tout sous-groupe d'un groupe cyclique d'ordre n est lui-même cyclique, son ordre est un diviseur de n et, si p est un diviseur de n il a un unique sous-groupe d'ordre p .

3. Anneaux commutatifs

$(A, +, *)$ désigne un anneau commutatif.

3.1. Compatibilité

Si I est un sous-groupe additif de A alors la relation \mathcal{R} définie sur A par $a\mathcal{R}b$ si $a - b \in I$ est compatible avec $*$ si, et seulement si, I est un idéal. Si c'est le cas les lois de A induisent une structure d'anneau sur A/I pour laquelle π est un morphisme surjectif, de plus A/I est un corps si, et seulement si, I est un idéal maximal.

Ainsi $\mathbb{Z}/p\mathbb{Z}$ est un corps si, et seulement si, p est un nombre premier.

3.2. Théorème de factorisation (the end)

Si I est un idéal de A , si $f \in \text{Hom}(A, B)$ où B est un anneau le théorème de factorisation admet une unique solution g si, et seulement si, $I \subset \text{Ker}(f)$. Si c'est le cas alors g est un morphisme d'anneaux, il est de plus injectif si, et seulement si, $I = \text{Ker}(f)$.

Définition

Si \mathbb{K} est un corps le noyau du morphisme f d'anneaux vérifiant $f(1) = 1_{\mathbb{K}}$ est de la forme $p\mathbb{Z}$ où p est un nombre nul ou premier car $f(\mathbb{Z})$ est isomorphe au corps $\mathbb{Z}/p\mathbb{Z}$. Le nombre p est la caractéristique de \mathbb{K} .

3.3. Lemme chinois

Si I_1, \dots, I_k sont des idéaux deux à deux premiers entre eux et si $I_0 = I_1 \dots I_k$ alors $A/I_0 \rightarrow A/I_1 \times \dots \times A/I_k$, $\bar{x}^0 \mapsto (\bar{x}^1, \dots, \bar{x}^k)$ (avec des notations cohérentes) définit un isomorphisme d'anneaux.

3.4. Corps des fractions

Soit A un anneau intègre. La relation \mathcal{R} définie sur $A \times (A \setminus \{0\})$ est une relation d'équivalence compatible avec les lois de A . L'ensemble $\mathbb{K} = A/\mathcal{R}$ est un corps appelé corps des fractions de A , l'application $i : A \rightarrow \mathbb{K}$, $a \mapsto (a, 1)$ est un morphisme injectif.

Exemples : \mathbb{Q} , $\mathbb{K}(X)$.

3.5. Éléments algébriques

Soient \mathbb{K} un sous-corps de \mathbb{L} et $x \in \mathbb{L}$. Le noyau du morphisme $\varphi : \mathbb{K}[X] \rightarrow \mathbb{L}$, $x \mapsto P(x)$ est un idéal principal (μ) . On dit que x est algébrique sur \mathbb{K} si μ est non nul. Dans ce cas μ est irréductible et $\text{Im}(\varphi) = \mathbb{K}[x]$ est un corps isomorphe à $\mathbb{K}[X]/(\mu)$. En fait x est algébrique si, et seulement si, $\mathbb{K}[x]$ est de dimension finie sur \mathbb{K} .

Exemple : \mathbb{C} est un corps isomorphe à $\mathbb{R}[X]/(X^2 + 1)$.

4. Algèbre linéaire

Si V et W sont des sous-espaces vectoriels supplémentaires de E alors la solution du théorème de factorisation pour le projecteur sur W de direction V est un isomorphisme d'espaces vectoriels de E/V sur W (on ne s'étendra donc pas sur cette notion de quotient).

Développements : 1.3 ou 2.3. ou 3.3.