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, $G = \{kg | k \in \mathbb{Z}\}$ et, s'il est multiplicatif, $G = \{g^k | k \in \mathbb{Z}\}$.

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

1.2. Surjection

Si g engendre G alors $\varphi : \mathbb{Z} \to G,\ k \mapsto kg$ 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 $\mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n,\ \dot{k} \mapsto e^{2ik\pi/n}$ 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 $\mathrm{Ker}(f) = n\mathbb{Z}$.

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

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 $d \in [\![1, n]\!]$. $\mathbb{U}_d$ est un sous-groupe 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 $n \geqslant 3$.

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

Remarques

1. Si E est un ensemble de cardinal n et si φ est une bijection de E sur $[\![1,n]\!]$ alors, en notant $\mathrm{Bij}(E)$ l'ensemble des bijections de E sur lui-même, $\sigma \mapsto \varphi\circ\sigma\circ\varphi^{-1}$ est un morphisme bijectif de groupes entre $\mathrm{Bij}(E)$ et $\mathfrak{S}_n$.
2. $\mathfrak{S}_n$ 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 $[\![1,n]\!]$ tels que $\sigma(k) \neq k$, on le note $Supp(\sigma)$.
Comme $\mathfrak{S}_n$ est un groupe fini σ est d'ordre fini r et engendre un groupe (σ) qui opère sur $[\![1,n]\!]$ par $(\sigma^p, k) \mapsto \sigma^p(k)$.
Si $k \in [\![1,n]\!]$ son orbite est $\mathcal{O}(k) = \left\{\sigma^p(k) \middle| p \in [\![0, r-1]\!]\right\}$, 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 $Supp(\sigma)$.

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 $\left\{(1,i) \middle| i \in [\![2,n]\!]\right\}$ est une partie génératrice minimale de $\mathfrak{S}_n$.

1.4. Signature

1.4.1. Définition

Soient $\sigma \in \mathfrak{S}_n$ et $(i,j) \in [\![1,n]\!]^2$ 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 $[\![1,n]\!]$ on a également $\varepsilon(\sigma) = \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

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 $r \in [\![2,n]\!]$ on dit qu'un élément σ de $\mathfrak{S}_n$ est un r-cycle si sous son action l'ensemble $[\![1,n]\!]$ 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.
$\big((1,2),(1,2,\ldots,n)\big)$ est une famille minimale de générateurs du groupe $\mathfrak{S}_n$.

1.5.4. Génération de $\mathcal{A}_n$

$\big\{(1,2,k)\big|k \in [\![3,n]\!]\big\}$ engendre le groupe $\mathcal{A}_n$ si $n \geqslant 3$.

2. Applications

2.1. Théorème de Cauchy

Soient $(G,.)$ 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 $\mathcal{B} = (e_1,\ldots,e_n)$ est une base de E, il existe une unique forme n-linéaire alternée f sur E telle que $f(e_1,\ldots,e_n) = 1$. 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 $\mathbb{N}^\star$.

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 $\pi_n : \mathbb{Z}\to\mathbb{Z}/n\mathbb{Z},\ k\mapsto Cl_n(k)$ est un morphisme surjectif d'anneaux dont le noyau est $n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ est un anneau 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 $(p-1)! \equiv -1\ [p]$.

2.6. Théorème chinois

2.6.1. Théorème

$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $Cl_{mn}(x) \mapsto \big(Cl_m(x), Cl_n(x)\big)$ 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 $\big(Cl_m(a), Cl_n(b)\big)$ par l'application précédente. On vient donc d'expliciter l'isomorphisme réciproque.

2.6.2. Indicatrice d'Euler

Si $p_1, \ldots, p_k$ 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 $p \geqslant 5$ on écrit $\sum_{i=1}^{p-1} \frac{1}{i} = \frac{A_p}{B_p}$ irréductible dans $\mathbb{Q}$.

Montrer $A_p \equiv 0\ [p^2]$.

3.2. Application du théorème chinois

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

3.3. Critère d'Einsenstein

Soit $A = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ 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 : Nombres premiers. Propriétés et applications.

Prérequis : divisibilité dans $\mathbb{Z}$, groupes.

1. Généralités

1.1. Définition

Un entier naturel p est dit premier s'il a exactement deux diviseurs 1 et p dans $\mathbb{N}$.
On note $\mathcal{P}$ l'ensemble des nombres premiers.

Conséquence : si $p \in \mathcal{P}$ et $k \in [\![1, p-1]\!]$ alors $\binom{p}{k} \in p\mathbb{N}$.

1.2. Décomposition

1.2.1. Proposition

Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.

Remarque : si p est le plus petit diviseur de n dans $[\![2, n]\!]$, ou bien $p = n$ si $n \in \mathcal{P}$, ou bien $p \leqslant \sqrt{n}$ car il existe q dans $[\![p, n]\!]$ tel que $n = pq$.

On peut alors proposer le crible d'Erathosthène et même sa programmation si l'on sait faire.

1.2.2. Corollaire

L'ensemble $\mathcal{P}$ est infini

1.2.3. Théorème de décomposition

Tout nombre entier $n \geqslant 2$ admet une unique décomposition en produit de nombres premiers (à l'ordre près des facteurs), autrement dit il existe une unique application ω_n de $\mathcal{P}$ dans $\mathbb{N}$ à support fini telle que $n = \prod_{p \in \mathcal{P}} p^{\omega_n(p)}$.

1.2.4. Corollaire 1

Si $(a, b) \in \mathbb{Z}^2$ alors $|ab| = \operatorname{pgcd}(a, b) \operatorname{ppcm}(a, b)$.

1.2.5. Corollaire 2

Si $p_1, \ldots, p_k$ sont les nombres premiers distincts intervenant dans la décomposition de n alors $\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

1.3. Corps $\mathbb{F}_p$.

1.3.1. 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. Si c'est le cas ce corps est noté $\mathbb{F}_n$.

1.3.2. 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 $x \in \mathcal{U}_p$ groupe des unités de $\mathbb{F}_p$, alors x est le carré d'un élément de $\mathcal{U}_p$ si, et seulement si, $x^{\frac{p-1}{2}} = 1$.

1.3.3. Théorème de Wilson

Si p est un nombre premier alors $(p-1)! \equiv -1\ [p]$.

2. Applications

2.1. Centre d'un p-groupe

Soient p un nombre premier et G un groupe fini de cardinal p^α avec $\alpha \in \mathbb{N}^\star$ (un tel groupe est appelé un p-groupe). Le centre $\mathcal{Z}(G)$ de G possède au moins p éléments.
Dans le cas $\alpha = 1$, G est cyclique.
Dans le cas où $\alpha = 2$, G est nécessairement commutatif.

2.2. Théorème de Cauchy

Soient $(G, .)$ 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.

2.3. Critère d'Einsenstein

Soit $A = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ 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 $\mathbb{Q}[X]$.

2.4. 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.

2.5. Théorème des deux carrés

1. Un nombre premier p distinct de 2 est somme de deux carrés d'entiers si, et seulement si, $p \equiv 1\ [4]$.
2. 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.

2.6. Théorème de la progression arithmétique

Pour tout entier $n \geqslant 1$ et tout entier m premier avec n, il existe une infinité de nombres premiers congrus à m modulo n.

Exercice 1. a) Si p est un nombre premier et si $k \in \mathbb{N}^\star$ montrer que l'exposant de p dans la décomposition en produit de facteurs premiers de $n!$ est $\displaystyle\sum_{k=1}^{\infty} \left\lfloor np^{-k} \right\rfloor$.

b) Donner le nombre de zéros à la fin de l'écriture décimale de 1000!

Exercice 2.

Si $p \in \mathcal{P}$ et $p \geqslant 5$ on écrit $\displaystyle\sum_{i=1}^{p-1} \frac{1}{i} = \frac{A_p}{B_p}$ irréductible dans $\mathbb{Q}$. Montrer $A_p \equiv 0\ [p^2]$.

Développements possibles :
le théorème 1.2.3. très central bien sûr, l'application 2.2. jolie mais rapide, l'application 2.4.