HAX501X – Groupes et anneaux 1

CM9 12/10/2023

Clément Dupont

Retour sur les exercices du cours

Exercice 44
Montrer que si $G \simeq H$ et $H \simeq K$ alors $G \simeq K$.

Comme $G \simeq H$, il existe un isomorphisme de groupes $f : G \to H$. Comme $H \simeq K$, il existe un isomorphisme de groupes $g : H \to K$.

La composée $g \circ f : G \to K$ est un morphisme de groupes (résultat du cours) et est bijective (composée d'applications bijectives). Donc c'est un isomorphisme de groupes, et donc $G \simeq K$.

Exercice 45

Soit $n \in \mathbb{N}^*$. Montrer que les groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont isomorphes.

- On a vu en TD qu'on a une bijection

$$g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n \ , \ \overline{k} \mapsto e^{\frac{2i\pi k}{n}} = \left(e^{\frac{2i\pi}{n}}\right)^k .$$

- Il reste à montrer que g est un morphisme de groupes : pour $\overline{k}, \overline{k'} \in \mathbb{Z}/n\mathbb{Z}$ on a

$$g(\overline{k} + \overline{k'}) = g(\overline{k+k'}) = \left(e^{\frac{2i\pi}{n}}\right)^{k+k'} = \left(e^{\frac{2i\pi}{n}}\right)^k \left(e^{\frac{2i\pi}{n}}\right)^{k'} = g(\overline{k})g(\overline{k'}).$$

- Autre rédaction : on a vu que $\mathbb{U}_n$ est un groupe cyclique, engendré par $e^{\frac{2i\pi}{n}}$, qui est d'ordre n. Donc par le cours, $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. (L'isomorphisme donné par le cours est g...)

Exercice 46

Soient G et H deux groupes qui sont isomorphes.

1) Montrer que si G est abélien alors H est abélien.

1) Supposons que G est un groupe abélien. Comme G et H sont isomorphes, il existe un isomorphisme de groupes $f : G \to H$. Soient $y_1, y_2 \in H$. Comme f est surjectif, il existe $x_1, x_2 \in G$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. Alors on a, en utilisant le fait que f est un morphisme de groupes et le fait que G est abélien :

$$y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2) = f(x_2 x_1) = f(x_2)f(x_1) = y_2 y_1.$$

Donc H est un groupe abélien.

1') Autre rédaction. Supposons que G est un groupe abélien. Comme G et H sont isomorphes, il existe un isomorphisme de groupes $g : H \to G$. Soient $y_1, y_2 \in H$. On calcule, en utilisant le fait que g est un morphisme de groupes et le fait que G est abélien :

$$g(y_1 y_2) = g(y_1)g(y_2) = g(y_2)g(y_1) = g(y_2 y_1).$$

Comme g est injectif, on a donc $y_1 y_2 = y_2 y_1$. Donc H est abélien.

Exercice 46

Soient G et H deux groupes qui sont isomorphes.

2) Montrer que si G est cyclique alors H est cyclique.

2) On suppose que G est un groupe cyclique. Il existe donc $a \in G$ tel que

$$G = \langle a \rangle = \{a^k \ , \ k \in \mathbb{Z}\}.$$

Comme G et H sont isomorphes, il existe un isomorphisme de groupes $f : G \to H$. On montre que $H = \langle f(a) \rangle$. Soit $y \in H$. Comme f est surjectif, il existe $x \in G$ tel que $y = f(x)$. Or G est engendré par a donc il existe $k \in \mathbb{Z}$ tel que $x = a^k$. On a alors

$$y = f(x) = f(a^k) = f(a)^k$$

et donc $y \in \langle f(a) \rangle$. Donc $H = \langle f(a) \rangle$ et donc H est un groupe cyclique.

Remarque

On a utilisé le fait suivant : pour un morphisme de groupes $f : G \to H$ et pour $a \in G$ et $k \in \mathbb{Z}$ on a

$$f(a^k) = f(a)^k.$$

Exercice 46

Soient G et H deux groupes qui sont isomorphes.

3) Montrer que si l'équation $x^5 = e_G$ a 10 solutions $x \in G$ alors l'équation $y^5 = e_H$ a 10 solutions dans H.

3) Comme G et H sont isomorphes, il existe un isomorphisme de groupes $f : G \to H$. On montre que f induit une bijection entre les ensembles

$$\mathcal{S}_G = \{x \in G \mid x^5 = e_G\} \quad \text{et} \quad \mathcal{S}_H = \{y \in H \mid y^5 = e_H\}.$$

- Pour $x \in \mathcal{S}_G$ on a $f(x) \in \mathcal{S}_H$. En effet, si $x^5 = e_G$ alors $f(x)^5 = f(x^5) = f(e_G) = e_H$. Donc f induit bien une application

$$f' : \mathcal{S}_G \to \mathcal{S}_H \ , \ x \mapsto f(x)$$

- Soit $g : H \to G$ la réciproque de f, c'est un isomorphisme de groupes. Par le même raisonnement, g induit une application

$$g' : \mathcal{S}_H \to \mathcal{S}_G \ , \ y \mapsto g(y).$$

- Clairement, $g' \circ f'$ est l'identité de $\mathcal{S}_G$ et $f' \circ g'$ est l'identité de $\mathcal{S}_H$. Donc f' et g' sont des bijections, réciproques l'une de l'autre. Donc $|\mathcal{S}_G| = |\mathcal{S}_H|$.

Exercice 47

Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes (même s'il existe une bijection entre les ensembles sous-jacents à ces deux groupes).

- $\mathbb{Z}/4\mathbb{Z}$ est un groupe cyclique (engendré par $\overline{1}$).
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas un groupe cyclique (vu plus haut).
- Donc ces groupes ne sont pas isomorphes, par l'exercice précédent.

Exercice 48

Dans chaque cas, donner l'ordre de x dans le groupe G et décrire $\langle x \rangle$.

- $G = \mathbb{Z}$, $x = 1$.
  L'élément 1 est d'ordre infini dans le groupe $\mathbb{Z}$, et $\langle 1 \rangle = \mathbb{Z}$.
- $G = \mathbb{Z}$, $x = -1$.
  L'élément -1 est d'ordre infini dans le groupe $\mathbb{Z}$, et $\langle -1 \rangle = \mathbb{Z}$.
- $G = \mathbb{Z}$, $x = 2$.
  L'élément 2 est d'ordre infini dans le groupe $\mathbb{Z}$, et $\langle 2 \rangle = 2\mathbb{Z}$.
- $G = \mathbb{R}^*$, $x = 1$.
  L'élément 1 est d'ordre 1 dans le groupe $\mathbb{R}^*$ (c'est l'élément neutre), et $\langle 1 \rangle = \{1\}$.
- $G = \mathbb{R}^*$, $x = -1$.
  L'élément -1 est d'ordre 2 dans le groupe $\mathbb{R}^*$, et $\langle -1 \rangle = \{1, -1\}$.
- $G = \mathbb{R}^*$, $x = 2$.
  L'élément 2 est d'ordre infini dans le groupe $\mathbb{R}^*$, et

$$\langle 2 \rangle = \{2^n, n \in \mathbb{Z}\} = \{\ldots, \tfrac{1}{8}, \tfrac{1}{4}, \tfrac{1}{2}, 1, 2, 4, 8, \ldots\}.$$

- $G = \mathfrak{S}_4$, $x = (1\ 2\ 3)(3\ 4)$.
  On calcule :
  $$x = (1\ 2\ 3)(3\ 4) = (1\ 2\ 3\ 4).$$
  On a
  $$x^2 = (1\ 3)(2\ 4)\ ,\ x^3 = (1\ 4\ 3\ 2)\ ,\ x^4 = \mathrm{id}\,.$$
  Donc x est d'ordre 4 dans $\mathfrak{S}_4$, et
  $$\langle\, x \,\rangle = \{\mathrm{id}, x, x^2, x^3\}.$$
- $G = \mathrm{GL}_2(\mathbb{R})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On calcule :
  $$x^2 = -I_2\ ,\ x^3 = -x\ ,\ x^4 = I_2.$$
  Donc x est d'ordre 4 dans $\mathrm{GL}_2(\mathbb{R})$ et
  $$\langle\, x \,\rangle = \{\mathrm{id}, x, x^2, x^3\}.$$

- $G = \mathrm{GL}_2(\mathbb{R})$, $x = \begin{pmatrix} 2 & -2 \\ 4 & -7 \end{pmatrix}$.

  Il est compliqué (en général) de calculer les puissances d'une matrice ! C'est (notamment) à ça que sert la **réduction des endomorphismes**. On note A la matrice en question, son polynôme caractéristique est

  $$\chi_A(X) = X^2 + 5X - 6 = (X-1)(X+6).$$

  Il est scindé à racines (réelles) simples, donc A est diagonalisable : il existe une matrice $P \in \mathrm{GL}_2(\mathbb{R})$ telle que

  $$A = P \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} P^{-1}.$$

  Notamment, pour tout $n \in \mathbb{N}^*$ on a

  $$A^n = P \begin{pmatrix} 1 & 0 \\ 0 & (-6)^n \end{pmatrix} P^{-1}$$

  qui n'est jamais la matrice identité.
  Donc A est d'ordre infini dans $\mathrm{GL}_2(\mathbb{R})$, et

  $$\langle A \rangle = \{A^n,\, n \in \mathbb{Z}\} = \left\{ P \begin{pmatrix} 1 & 0 \\ 0 & (-6)^n \end{pmatrix} P^{-1},\, n \in \mathbb{Z} \right\}.$$

- $G = \mathbb{Z}/24\mathbb{Z}$, $x = \overline{14}$.
  On sait que dans $\mathbb{Z}/24\mathbb{Z}$ on a

$$\langle \overline{14} \rangle = \langle \overline{14 \wedge 24} \rangle = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{14}, \ldots, \overline{22}\}$$

  qui a 12 éléments. Donc l'ordre de $\overline{14}$ dans $\mathbb{Z}/24\mathbb{Z}$ est 12.

Exercice 49
Dans $\mathbb{Z}/n\mathbb{Z}$, quel est l'ordre d'un élément $\overline{k}$?

- L'ordre de $\overline{k}$ est égal à l'ordre du sous-groupe $\langle \overline{k} \rangle$ engendré par $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$. On a vu au chapitre 2 que

$$\langle \overline{k} \rangle = \langle \overline{k \wedge n} \rangle,$$

dont le cardinal est

$$\frac{n}{k \wedge n}.$$

- Conclusion : l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est

$$\frac{n}{k \wedge n}.$$

Exercice 50
Soit G un groupe, soit $x \in G$ un élément d'ordre fini n. Pour un élément $k \in \mathbb{Z}$, quel est l'ordre de x^k ?

On a un isomorphisme de groupes

$$\mathbb{Z}/n\mathbb{Z} \to \langle x \rangle \ , \ \overline{k} \mapsto x^k.$$

La question revient donc à se demander : quel est l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$?
On a vu que la réponse est

$$\frac{n}{k \wedge n} \ .$$

Le théorème de Lagrange

Théorème (Théorème de Lagrange)

Soit G un groupe fini et soit H un sous-groupe de G. Alors $|H|$ divise $|G|$.

Définition

*Soit G un groupe fini et soit H un sous-groupe de G. Le quotient $\frac{|G|}{|H|}$ est appelé l'***indice** *de H dans G.*

Le théorème de Lagrange pour l'ordre d'un élément

Théorème
Soit G un groupe fini et soit $x \in G$. Alors l'ordre de x divise $|G|$.

Démonstration. C'est une conséquence du théorème de Lagrange et du fait que l'ordre de x est égal à $|\langle x \rangle|$. □

- Une autre formulation, complètement équivalente :

Théorème
Soit G un groupe fini. Alors pour tout $x \in G$ on a :

$$x^{|G|} = e.$$

Remarque : congruence modulo un sous-groupe

- On a utilisé la relation $\sim$ sur G définie par :

$$x \sim y \quad \Longleftrightarrow \quad \exists h \in H,\, xh = y.$$

- Dans le cas où $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, cette relation est :

$$x \sim y \quad \Longleftrightarrow \quad \exists h \in n\mathbb{Z},\, x + h = y \quad \Longleftrightarrow \quad y - x \in n\mathbb{Z}.$$

  C'est la relation de congruence modulo n...

- La relation $\sim$ peut donc être appelée **relation de congruence à gauche modulo** H.
- On a aussi la **relation de congruence à droite modulo** H :

$$x \sim' y \quad \Longleftrightarrow \quad \exists h \in H,\, hx = y.$$

Classes à gauche, classes à droite

- La classe d'équivalence $\overline{x}$ qui apparaît dans la preuve du théorème est aussi notée xH et appelée la **classe à gauche** de x suivant le sous-groupe H.
- L'ensemble des classes à gauche est noté G/H.

- On peut aussi considérer la **classe à droite** Hx, qui est la classe d'équivalence de x pour la relation de congruence à droite modulo H.
- L'ensemble des classes à droite est noté $H\backslash G$.

- En général ces deux concepts sont différents : on peut avoir $xH \neq Hx$.
- Mais clairement ces deux concepts coïncident si G est un groupe abélien.
- Vous verrez au semestre prochain la notion de **sous-groupe distingué**, qui est un sous-groupe H de G tel que pour tout $x \in G$, $xH = Hx$, ou dit autrement tel que les relations de congruence à gauche et à droite coïncident.
- Cela permet de mettre une structure de groupe sur le quotient $G/H = H\backslash G$, qui s'appelle le **groupe quotient**.

Et un exercice

Exercice 51
Soit $G = \mathfrak{S}_3$ et soit $H = \langle \tau \rangle = \{\mathrm{id}, \tau\}$ où τ est la transposition $(1\ 2)$.
Lister les classes à gauche des éléments de G suivant H, puis les classes à droite.

Groupes d'ordre premier

Théorème
Soit G un groupe d'ordre premier p. Alors G est cyclique, c'est-à-dire isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

- À isomorphisme près, $\mathbb{Z}/17\mathbb{Z}$ est donc le seul groupe d'ordre 17.

Démonstration. Comme $p \geqslant 2$, il existe un élément $x \in G$ avec $x \neq e$. On considère le sous-groupe $\langle x \rangle$ de G engendré par x. Comme $x \neq e$, ce n'est pas le groupe trivial. Par le théorème de Lagrange, l'ordre de $\langle x \rangle$ est un diviseur de p, et comme p est premier, on a donc $|\langle x \rangle| = p$. Comme $|G| = p$, on a donc $G = \langle x \rangle$, et donc G est cyclique. □

Remarque
Le théorème est évidemment faux en général sans l'hypothèse "p premier". Par exemple, on rappelle que le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique.

Définition

Pour un entier $k \geqslant 2$ et des éléments $i_1, i_2, \ldots, i_k$ deux à deux disjoints dans $\{1, \ldots, n\}$, le **cycle** *(aussi appelé* **permutation circulaire***)*

$$\gamma = (i_1\ i_2\ \cdots\ i_k) \in \mathfrak{S}_n$$

est la permutation définie par

$$\begin{cases} \gamma(i_1) = i_2,\ \gamma(i_2) = i_3,\ \ldots,\ \gamma(i_{k-1}) = i_k,\ \gamma(i_k) = i_1 \\ \gamma(x) = x \quad \textit{pour tout } x \in \{1, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}. \end{cases}$$

L'ensemble $\{i_1, i_2, \ldots, i_k\}$ est le **support** *de γ. L'entier k est la* **longueur** *de γ. (On dit aussi que γ est un k-***cycle***.)*

- Un k-cycle est d'ordre k dans $\mathfrak{S}_n$.

Exercice 52

Réciproquement, est-ce que tout élément de $\mathfrak{S}_n$ d'ordre k est un k-cycle ?

Définition

Une **transposition** *est un cycle de longueur 2, c'est-à-dire de la forme $(i\ j)$ pour deux éléments $i \neq j$ de $\{1, \ldots, n\}$.*

Décomposition en produit de cycles de supports disjoints

Proposition

Soit $\sigma \in \mathfrak{S}_n$. Alors σ a une décomposition unique (à l'ordre des facteurs près) en produit de cycles de supports disjoints :

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r$$

avec $r \in \mathbb{N}$ et les γ_i des cycles de $\mathfrak{S}_n$ dont les supports sont deux à deux disjoints.

Remarque

Deux cycles $\gamma, \gamma' \in \mathfrak{S}_n$ de supports disjoints commutent : $\gamma\gamma' = \gamma'\gamma$.

Exemple

Dans $\mathfrak{S}_5$ on a $(1\ 5\ 2)(4\ 3) = (4\ 3)(1\ 5\ 2)$.

Et des exercices

Exercice 53

Déterminer la décomposition en produit de cycles à supports disjoints de la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 9 & 6 & 7 & 4 & 5 & 3 & 1 \end{pmatrix}.$$

Exercice 54

Calculer l'inverse de la permutation $(1\ 3\ 7)(2\ 9\ 4\ 5)(6\ 8) \in \mathfrak{S}_9$.

Exercice 55

Avec les notations de la proposition précédente, exprimer l'ordre de σ en fonction des longueurs des cycles γ_i. Quel est l'ordre maximal d'un élément du groupe symétrique $\mathfrak{S}_5$? de $\mathfrak{S}_6$? de $\mathfrak{S}_7$? de $\mathfrak{S}_8$?

$\mathfrak{S}_n$ est engendré par les transpositions

Proposition

Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions.

Exercice 56

Écrire la permutation de l'exercice 53 comme un produit de transpositions.

$\mathfrak{S}_n$ est engendré par les transpositions adjacentes

Proposition

Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions adjacentes $(i\ i+1)$ pour $1 \leqslant i \leqslant n-1$.

Théorème/définition

Théorème

Il existe un unique morphisme de groupes

$$\mathrm{sgn} : \mathfrak{S}_n \to \{-1, 1\}$$

qui est tel que $\mathrm{sgn}(\tau) = -1$ *pour* τ *une transposition.*

Définition

On appelle $\mathrm{sgn}(\sigma)$ *la* **signature** *de la permutation* $\sigma \in \mathfrak{S}_n$*.*

- On a donc, pour des transpositions $\tau_1, \ldots, \tau_k$:

$$\mathrm{sgn}(\tau_1 \cdots \tau_k) = (-1)^k.$$

- Le théorème implique que si l'on écrit une permutation donnée comme un produit de transpositions, la parité du nombre de transpositions qui apparaissent dans ce produit ne dépend pas du choix d'écriture.

Signature d'un cycle

Proposition

Pour tout $k \geqslant 2$, la signature d'un cycle de longueur k est $(-1)^{k-1}$.

- Cette proposition est utile pour calculer la signature d'une permutation qu'on a auparavant décomposée en produit de cycles : elle vaut $(-1)^r$ où r est le nombre de cycles de longueur paire qui interviennent dans la décomposition.

Le groupe alterné

Définition
Le **groupe alterné** *sur n éléments, noté $\mathfrak{A}_n$, est le noyau de la signature, c'est-à-dire l'ensemble des permutations $\sigma \in \mathfrak{S}_n$ telles que $\mathrm{sgn}(\sigma) = 1$.*

- C'est un sous-groupe de $\mathfrak{S}_n$ car c'est le noyau d'un morphisme de groupes.

Exercice 57
Lister les éléments de $\mathfrak{A}_3$ et de $\mathfrak{A}_4$.

Ordre du groupe alterné

Proposition

Pour $n \geqslant 2$, le groupe alterné $\mathfrak{A}_n$ est d'ordre $\frac{n!}{2}$. Dit autrement, c'est un sous-groupe de $\mathfrak{S}_n$ d'indice 2.

Démonstration. Notons $\mathfrak{S}_n^- \subset \mathfrak{S}_n$ l'ensemble des permutations de signature -1. (Ce n'est pas un sous-groupe de $\mathfrak{S}_n$.) On a donc une partition

$$\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{S}_n^-.$$

Soit $\tau = (1\ 2) \in \mathfrak{S}_n^-$. Pour tout $\sigma \in \mathfrak{A}_n$ on a $\tau\sigma \in \mathfrak{S}_n^-$ car $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma) = (-1) \times 1 = -1$. On a donc une application

$$\mathfrak{A}_n \to \mathfrak{S}_n^- \ , \ \sigma \mapsto \tau\sigma,$$

dont on voit facilement qu'elle est bijective (Montrez-le !). Cela implique que $|\mathfrak{A}_n| = |\mathfrak{S}_n^-|$ et donc que $|\mathfrak{S}_n| = |\mathfrak{A}_n| + |\mathfrak{S}_n^-| = 2|\mathfrak{A}_n|$, d'où le résultat. □