Colle MP*

Antoine Médoc

Semaine 1 (12 septembre 2022)

1 Planche 1

1.1 Question de cours

— Quels sont les sous-groupes de $\mathbb{Z}$?

1.2 Application

— Les sous-groupes de $\mathbb{Z}$ non réduit à $\{0\}$ sont-ils tous isomorphes ?
— De tels sous-groupes sont monogènes infinis, donc isomorphes à $\mathbb{Z}$.

1.3 Exercice

1. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 1 & 3 & 4 & 7 \end{pmatrix} \in \mathfrak{S}_7$.
   (a) — Décomposer σ en cycles à support disjoints et donner ses orbites.
   — On a $\sigma = (1\ 2\ 6\ 4)(3\ 5)$. Ses orbites sont $\{1, 2, 4, 6\}$, $\{3, 5\}$ et $\{7\}$.
   (b) — Calculer la signature de σ.
   — On a $\varepsilon(\sigma) = (-1)^{4-1}(-1)^{2-1} = 1$.
2. On s'intéresse au groupe alterné $\mathfrak{A}_n$ noyau de la signature $\varepsilon : \mathfrak{S}_n \to \{1, -1\}$.
   (a) — Caractériser les cycles qui appartiennent à $\mathfrak{A}_n$.
   — Soit $l \in [\![2, n]\!]$ et $c = (i_1 \dots i_l)$ un cycle. On a $c = (i_1\ i_2)(i_2\ i_3) \dots (i_{l-1}\ i_l)$ donc $\varepsilon(c) = (-1)^{l-1}$. Donc $c \in \mathfrak{A}_n$ si, et seulement si, l est impair.
   (b) — Montrer que $\mathfrak{A}_n$ est l'ensemble des produits d'un nombre pair de transpositions.
   — Soit $p \in \mathbb{N}^*$. Un produit de $2p$ transpositions est de signature $(-1)^{2p} = 1$ donc est un élément de $\mathfrak{A}_n$. Soit $\sigma \in \mathfrak{A}_n$. La permutation σ peut s'écrire comme un produit de q transpositions. Or $1 = \varepsilon(\sigma) = (-1)^q$ donc q est pair.
3. Soit $c = (i_1 \dots i_p) \in \mathfrak{S}_n$ un cycle de longueur $p \geqslant 2$. On considère son commutant $H := \left\{\sigma \in \mathfrak{S}_n \,\middle|\, \sigma c \sigma^{-1} = c\right\}$. *Pourquoi appelle-t-on cet ensemble son commutant ?*
   (a) — Est-ce un sous-groupe de $\mathfrak{S}_n$?
   — On a $\mathrm{Id} \in H$ donc $H \neq \emptyset$. Pour tout $\sigma \in H$, $\sigma c \sigma^{-1} = c$ i.e. $c = \sigma^{-1} c \sigma$ donc $\sigma^{-1} \in H$. Pour tous $\sigma, \sigma' \in H$, $\sigma_1 \sigma_2 c = \sigma_1 c \sigma_2 = c \sigma_1 \sigma_2$ donc $\sigma_1 \sigma_2 \in H$. Donc $H < \mathfrak{S}_n$.
   (b) — Soit $\sigma \in \mathfrak{S}_n$. Calculer $\sigma c \sigma^{-1}$.
   — Soit $\tau = \sigma c \sigma^{-1}$. Pour tout $k \in [\![1, p-1]\!]$, $\tau(\sigma(i_k)) = \sigma(i_{k+1})$ et $\tau(\sigma(i_p)) = \sigma(i_1)$. Soit $j \in [\![1, n]\!] \setminus \{\sigma(i_1), \dots, \sigma(i_p)\}$. On a $\sigma^{-1}(j) \notin \{i_1, \dots, i_p\}$ donc $c(\sigma^{-1}(j)) = \sigma^{-1}(j)$ donc $\tau(j) = j$. Ainsi $\tau = (\sigma(i_1) \dots (\sigma(i_p))$. En particulier, c'est un cycle de longueur p.

(c) — Donner tous les éléments de $\langle c\rangle$ et montrer que $\langle c\rangle \subset H$.
   — Le cycle c est d'ordre p donc $\langle c\rangle = \{\mathrm{Id}, c, \dots, c^{p-1}\}$. Or toute puissance de c commute avec c donc $\langle c\rangle \subset H$.

(d) — Montrer que $H = \langle c\rangle$.
   — Soit $\sigma \in H$. On a l'égalité des cycles $(\sigma(i_1) \dots (\sigma(i_p)) = (i_1 \dots i_p)$. Donc il existe $k \in [\![1, p]\!]$ tel que $\sigma(i_1) = i_k$ et on a l'égalité des p-uplets $(\sigma(i_1), \dots, (\sigma(i_p)) = (i_k, i_{k+1}, \dots, i_p, i_1, i_2, \dots, i_{k-1})$. Ainsi $\sigma = c^k$. Donc $\langle c\rangle \subset H$. Finalement, $H = \langle c\rangle$.

4. Soit $n \geqslant 2$. On s'intéresse à H le sous-groupe de $\mathfrak{S}_n$ engendré par $\{(i\ i+1)\ ;\ 1 \leqslant i \leqslant n-1\}$.

   (a) — Soit $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$. Montrer que $c_{i,j} := (i\ i+1 \dots j)$ et $c_{j,i} := (j\ j-1 \dots i)$ sont des éléments de H. Calculer $c_{i,j}c_{j,i}$.
   — On a $c_{i,j} = (i\ i+1)(i+1\ i+2)\dots(j-1\ j) \in H$ et $c_{j,i} = (j-1\ j)\dots(i+1\ i+2)(i\ i+1) \in H$. Par ailleurs, on reconnaît $c_{i,j} = c_{j,i}^{-1}$ d'où $c_{i,j}c_{j,i} = \mathrm{Id}$.

   (b) — Soit $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$. Montrer que $(i\ j) \in H$.
   — Si $j - i = 1$, $(i\ j) = (i\ i+1) \in H$. Si $j - i \geqslant 2$, $(i\ j) = c_{j,i+1}c_{i,j} \in H$.

   (c) — Montrer que $H = \mathfrak{S}_n$.
   — On sait que les transpositions engendrent $\mathfrak{S}_n$ et on a montré qu'elles appartiennent toutes à H. Ainsi $\mathfrak{S}_n \subset H \subset \mathfrak{S}_n$, i.e. $H = \mathfrak{S}_n$.

2 Planche 2

2.1 Question de cours

— Énoncer le théorème de décomposition d'une permutation en cycles à support disjoints. Montrer que $\mathfrak{S}_n$ est engendré par les permutations.

2.2 Application

— Montrer que la signature d'un cycle de longueur p est $(-1)^{p-1}$.
— On note $c = (i_1 \dots i_p)$ ce cycle. On a $c = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p)$ donc $\varepsilon(c) = (-1)^{p-1}$.

2.3 Exercice

Soit $(G, \cdot)$ un groupe d'élément neutre e

1. Supposons que, pour tout $x \in G$, $x^2 = e$.
   — Montrer que G est abélien.
   — Pour tous $x, y \in G$, $(xy)^2 = e$, i.e. $xy = y^{-1}x^{-1} = yx$.

2. Supposons G fini non trivial tel que, pour tout $x \in G$, $x^2 = e$.

   (a) — Justifier que G admet un système fini de générateurs $(x_1, \dots, x_n)$ de cardinal minimal.
   — Comme G est fini, il admet un système fini de générateurs (par exemple, G tout entier). Comme toute partie de $\mathbb{N}$ admet un minimum, G admet un système fini de générateurs de cardinal minimal.

   (b) — Montrer que l'application

$$\varphi : \left| \begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z})^n & \longrightarrow & G \\ (\bar{a}_1, \dots, \bar{a}_n) & \longmapsto & x^{a_1} \dots x^{a_n} \end{array} \right.$$

   est bien définie.

— Soit $x \in G$. Soit $(a,b) \in \mathbb{Z}^2$ tels que $\bar{a} = \bar{b}$ dans $\mathbb{Z}/2\mathbb{Z}$. Il existe $k \in \mathbb{Z}$ tel que $a - b = 2k$, donc $x^{a-b} = e$, i.e. $x^a = x^b$.

(c) — Montrer que φ est un morphisme de groupes surjectif.

— Soit $(\bar{a}_1, \ldots, \bar{a}_n), (\bar{b}_1, \ldots, \bar{b}_n) \in (\mathbb{Z}/2\mathbb{Z})^n$, notés a et b. On a, comme G est abélien, $\varphi(a+b) = x_1^{a_1} x_1^{b_1} \ldots x_n^{a_n} x_n^{b_n} = x_1^{a_1} \ldots x_n^{a_n} \times x_1^{b_1} \ldots x_n^{b_n} = \varphi(a)\varphi(b)$. Donc φ est un morphisme de groupes. Comme $(x_1, \ldots, x_n)$ est un système de générateurs, φ est surjectif.

(d) — Montrer que φ est un isomorphisme de groupes.

— Il reste à prouver que φ est injectif. Soit $a = (\bar{a}_1, \ldots, \bar{a}_n) \in \operatorname{Ker} \varphi \backslash \left\{(\bar{0}, \ldots, \bar{0})\right\}$. Il existe $i \in [\![1, n]\!]$ tel que $\bar{a}_i = \bar{1}$. On a $x_i = x_i^{-1} = \prod_{j \neq i} x_j^{a_j}$ donc $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ est un système de générateurs de cardinal $n-1$. Cela est absurde par minimalité du cardinal n. Ainsi $\operatorname{Ker} \varphi = \{(0, \ldots, 0)\}$, donc φ est injectif.

(e) — Quel est le cardinal de G ?

— On a $|G| = |(\mathbb{Z}/2\mathbb{Z})^n| = 2^n$.

3. Soit p premier. Supposons G fini de cardinal $2p$.

(a) — Supposons que G n'admet pas d'élément d'ordre p. Montrer que G n'est pas cyclique.

— Supposons G cyclique : il existe $x \in G$ d'ordre $2p$. L'élément x^2 est d'ordre p. Donc, par contraposée, G n'est pas cyclique.

(b) — Supposons encore que G n'admet pas d'élément d'ordre p. Quels sont les ordres possibles pour les éléments de G ?

— Par le théorème de Lagrange, les ordres des éléments de G divisent $2p$. Ainsi, par la question précédente, les éléments de G sont d'ordre 1 ou 2.

(c) — Par l'absurde, montrer que G admet un élément d'ordre p.

— Supposons que G n'admet pas d'élément d'ordre p. Comme $|G| = 2p \geqslant 2$, G admet un élément d'ordre 2, donc $p \geqslant 3$. Or, par le travail réalisé au début de l'exercice, on sait que le cardinal de G est une puissance de 2. Cela contredit $p \geqslant 3$. Donc, par l'absurde, G admet un élément d'ordre p.

3 Planche 3

3.1 Question de cours

— Énoncer les règles d'addition et de multiplications dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. Montrer qu'elles sont bien définies.

3.2 Application

— Donner le cardinal et les éléments inversibles des anneaux $A = \mathbb{Z}/3\mathbb{Z}$ et de $B = (\mathbb{Z}/2\mathbb{Z})^2$.

— On a $|A| = 3$. On a $\bar{2} \times \bar{2} = \bar{1}$ donc les éléments inversibles de A sont $\bar{2}$ et $\bar{3}$. On a $|B| = |\mathbb{Z}/2\mathbb{Z}|^2 = 4$. Les éléments $(\bar{1}, \bar{0})$ et $(\bar{0}, \bar{1})$ sont diviseurs de zéro donc non inversibles. Ainsi, le seul élément inversible de B est $(\bar{1}, \bar{1})$.

3.3 Exercice

Soit G un groupe.

1. — Soient $x, y \in G$ tels que xy est d'ordre fini. Montrer que yx est d'ordre fini et de même ordre.

— Soit $n \in \mathbb{N}^*$. On a $(xy)^n = x(yx)^{n-1}y$ donc $(xy)^n = e \Leftrightarrow x(yx)^{n-1}y = e \Leftrightarrow x(yx)^{n-1} = y^{-1} \Leftrightarrow (yx)^n = e$. Donc yx est d'ordre fini et de même ordre que xy.

2. Soient $x, y \in G$ d'ordres finis m et n premiers entre eux tels que $xy = yx$.

(a) — Montrer que xy est d'ordre fini p divisant mn.

— On a $(xy)^{mn} = (x^m)^n(y^n)^m = e$, donc xy est d'ordre fini p et $p|mn$.

(b) — Montrer que $m|pn$ et $n|pm$.

— On a $(xy)^p = e$ donc $x^p = y^{-p}$. Donc $x^{pn} = (y^{-p})^n = (y^n)^{-p} = e$, donc $m|pn$. De même, $y^{pm} = (x^{-p})^m = (x^m)^{-p} = e$ donc $n|pm$.

(c) — Montrer que $mn|p$ et conclure.

— On a $m|pn$ et $n|pm$. Or $m \wedge n = 1$ donc, par le lemme de Gauss, $m|p$ et $n|p$. En utilisant de nouveau $m \wedge n = 1$, $mn|p$. Or $p|mn$. Donc $p = mn$.

3. (a) — Calculer l'ordre r de $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 1 & 3 & 4 & 7 \end{pmatrix} \in \mathfrak{S}_7$.

— On a $\sigma = (1\ 2\ 6\ 4)(3\ 5)$ donc $\sigma^4 = \mathrm{Id}$ donc $r \in \{1, 2, 4\}$. Or $\sigma^1 = \sigma$ et $\sigma^2 = (1\ 6)(2\ 4)$. Donc $r = 4 \neq 2 \times 4$.

(b) — Soit $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{pmatrix} \in \mathfrak{S}_7$. Calculer σ^{2022}.

— On a $\sigma = (1\ 3\ 6\ 2\ 5)(4\ 7)$. Ces deux cycles commutent et sont d'ordres premiers entre eux, donc l'ordre r de σ est $r = 10$. Or $2022 \equiv 2\,[10]$ donc $\sigma^{2022} = \sigma^2 = (1\ 6\ 5\ 3\ 2)$.

4. Supposons G abélien fini. On définit son exposant r le plus grand des ordres des éléments de G.

(a) — Montrer que $r|\operatorname{Card} G$.

— Il existe un élément x de G d'ordre r donc, par le théorème de Lagrange, $r|\operatorname{Card} G$.

(b) — Soit $y \in G$ et q son ordre. Montrer, par l'absurde, que $q|r$.

— Supposons, par l'absurde, que q ne divise pas r. Il existe p premier, $\alpha, \beta, q', r' \in \mathbb{N}^*$ tels que $q = p^\alpha q'$, $r = p^\beta r'$, $p \wedge r' = p \wedge q' = 1$ et $\alpha > \beta$. Comme x est d'ordre r, $a := x^{p^\beta}$ est d'ordre r'. Comme y est d'ordre q, $b := y^{q'}$ est d'ordre p^α. Or $r' \wedge p^\alpha$ donc xy est d'ordre $p\alpha r' > r$. Cela contredit la définition de r comme ordre maximum, donc $q|r$.

4 Exercices supplémentaires

Exercice 1 ENS

— Quels sont les groupes dont l'ensemble E des sous-groupes est fini ?

— L'ensemble des parties d'un groupe fini est fini, donc l'ensemble des sous-groupes d'un groupe fini est fini. Soit G un groupe dont l'ensemble des sous-groupes est fini. Montrons que G est fini. On considère $E' := \left\{ H < G \,\middle|\, H \text{ monogène} \right\} \subset E$. Comme E est fini, E' est fini. Or $G = \bigcup_{g \in G} \langle g \rangle = \bigcup_{H \in E'} H$. Tout élément de G d'ordre infini engendre un sous-groupe isomorphe à $\mathbb{Z}$ qui admet une infinité de sous-groupes. Ainsi, tous les éléments de G sont d'ordre fini. Donc, pour tout $H \in E'$, H est fini. Une union finie d'ensembles finis est de cardinal fini, donc G est fini.

Exercice 2 ENS

— Quels sont les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$?

— Soit f un tel morphisme. Comme $\mathrm{Im} f < \mathbb{Z}$, il existe (un unique) $n \in \mathbb{N}$ tel que $\mathrm{Im} f = n\mathbb{Z}$. Supposons $n \neq 0$. Il existe $x \in \mathbb{Q}$ tel que $f(x) = n$, d'où $2.f(x/2) = n$, d'où $\frac{n}{2} = f(x/2) \in n\mathbb{Z}$, ce qui n'est pas. Ainsi, par l'absurde, $n = 0$. L'unique morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est donc le morphisme nul.