TD Maths $\mathcal{C}\,i\,\mathbb{R}^2$ — Groupes

Exercice 3

Posons $\zeta = e^{\frac{2\pi i}{n}}$ et $U = \{\zeta^k \mid k \in \mathbb{Z}\}$.

a)

U est un groupe:

- $1 \in U$ car $1 = \zeta^0$
- pour $x, y \in U$: $x = \zeta^k$, $y = \zeta^\ell$ avec $k, \ell \in \mathbb{Z}$, donc $x \cdot y = \zeta^k \cdot \zeta^\ell = \zeta^{k+\ell} \in U$ puiavec sque $k + \ell \in U$
- avec la même notation: $x^{-1} = \zeta^{-k} \in U$ puisque $-k \in \mathbb{Z}$

Puisque $\zeta^n = 1$, alors $U = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ (et n est le plus petit tel entier): groupe d'ordre n.

b)

Puisque $\zeta^k\zeta^\ell = \zeta^{k+\ell}$ et $\zeta^k = \zeta^\ell \iff k \equiv \ell \bmod n$, on voit que $(U, \cdot)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Explicitement: la fonction $f : \mathbb{Z}/n\mathbb{Z} \to U$ définie par $f(k) = \zeta^k$ est un isomomorphisme.

- bien définie puisque $\zeta^n = 1$
- surjective par définition
- morphisme puisque $\zeta^{k+\ell} = \zeta^k \cdot \zeta^\ell$
- injective puisque $\zeta^k = \zeta^\ell \implies k \equiv \ell \bmod n$ (ou alors puisqu'on a une surjection entre deux ensembles de même taille)

c)

$n = 12$:

élément	orbite	ordre
1	1	1
ζ	$1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8, \zeta^9, \zeta^{10}, \zeta^{11}$	12
ζ^2	$1, \zeta^2, \zeta^4, \zeta^6, \zeta^8, \zeta^{10}$	6
ζ^3	$1, \zeta^3, \zeta^6, \zeta^9$	4
ζ^4	$1, \zeta^4, \zeta^8$	3
ζ^5	$1, \zeta^5, \zeta^{10}, \zeta^3, \zeta^8, \zeta, \zeta^6, \zeta^{11}, \zeta^4, \zeta^9, \zeta^2, \zeta^7$	12
ζ^6	$1, \zeta^6$	2
ζ^7	$1, \zeta^7, \zeta^2, \zeta^9, \zeta^4, \zeta^{11}, \zeta^6, \zeta, \zeta^8, \zeta^3, \zeta^{10}, \zeta^5$	12
ζ^8	$1, \zeta^8, \zeta^4$	3
ζ^9	$1, \zeta^9, \zeta^6, \zeta^3$	4
ζ^{10}	$1, \zeta^{10}, \zeta^8, \zeta^6, \zeta^4, \zeta^2$	6
ζ^{11}	$1, \zeta^{11}, \zeta^{10}, \zeta^9, \zeta^8, \zeta^7, \zeta^6, \zeta^5, \zeta^4, \zeta^3, \zeta^2, \zeta$	12

Figure: ça ressemble fort à une horloge ! (qui tourne dans le sens trigonométrique, avec l'originie à droite)

d)

En général: l'ordre de $x_k = \zeta^k$ est $\frac{n}{\mathrm{PGCD}(n,k)}$.

En effet: notons $d = \mathrm{PGCD}(n,k)$ et écrivons $n = dn'$, $k = dk'$ avec $\mathrm{PGCD}(n',k') = 1$.

Dans un sens: $(x_k)^{n'} = \zeta^{kn'} = \zeta^{dk'n'} = (\zeta^n)^{k'} = 1^{k'} = 1$ donc l'ordre de x_k divise n'.

Dans l'autre sens: si $(x_k)^m = \zeta^{km} = 1$ alors $km = dk'm$ divise $n = dn'$. Comme k' et n' sont premiers entre eux on en conclut que m divise n'.

Conclusion: $n' = \frac{n}{d}$ est l'odre de x_k.

Exercice 4

a)

Les fonctions $f_1(x) = x$, $f_2(x) = 1 - x$, $f_3(x) = \frac{1}{x}$ sont des bijections de $E = \mathbb{R} \setminus \{0, 1\}$ dans lui-même.

(à vérifier ! exercice en étude de fonctions)

On en conclut que $f_4(x) = \frac{1}{1-x} = f_3 \circ f_2(x)$, $f_5(x) = 1 - \frac{1}{x} = f_2 \circ f_3(x)$ et $f_6 = \frac{x}{x-1} = \frac{1}{1-\frac{1}{x}} = f_3 \circ f_5(x)$ le sont également par composition.

b)

Table de l'opération (lue de gauche à droite):

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

c)

Montrer que $F = \{f_1,\ f_2,\ f_3,\ f_4,\ f_5,\ f_6\}$ est un groupe pour $\circ$:

- F est stable sous $\circ$
- associativité: propriété générale de la composée de fonctions
- neutre: c'est la fonction identité f_1
- symétriques: on le voit dans la table $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_5$, $f_5^{-1} = f_4$, $f_6^{-1} = f_6$

d)

À partir de la table on voit les sous-groupes:

ordre 1 — $\{f_1\}$

ordre 2 — $\{f_1,\ f_2\}$, $\{f_1, f_3\}$ $\{f_1,\ f_6\}$

ordre 3 — $\{f_1,\ f_4,\ f_5\}$

ordre 6 — F

e)

Isomorphisme avec S_3: avec un petit abus de notation on peut considérer que ces 6 fonctions permutent $0, 1, \infty$ entre eux, ex. pour f_4:

$f_4(0) = 1$, $f_4(1) = \infty$, $f_4(\infty) = 0$

donc f_4 correspond à la permutation $(0,\ 1,\ \infty)$ dans $S_{\{0,1,\infty\}}$.

La fonction $\varphi : F \to S_{\{0,1,\infty\}}$ qui associe à chaque fonction f la permutation σ associée est un isomorphisme. Explicitement:

$f_1 \longleftrightarrow \mathrm{id}$

$f_2 \longleftrightarrow (0,\ 1)$

$f_3 \longleftrightarrow (0,\ \infty)$

$f_4 \longleftrightarrow (0,\ 1,\ \infty)$

$f_5 \longleftrightarrow (0,\ \infty,\ 1)$

$f_6 \longleftrightarrow (1,\ \infty)$

ce qui est cohérent avec tous les calculs ci-dessus.

Exercice 5

- $(E, \star)$ et $(F, \otimes)$ deux groupes
- $f : E \to F$ un morphisme de groupes

a)

Pour H un sous-groupe de E, montrons que $\overrightarrow{f}(H)$ l'image de H dans F est un sous-groupe.

1. $1_F = f(1_E) \in \overrightarrow{f}(H)$ car car $1_E \in H$
2. Pour $x, y \in \overrightarrow{f}(H)$: écrivons $x = f(a)$, $y = f(b)$, alors
   $x \otimes y = f(a) \otimes f(b) = f(a \star b) \in \overrightarrow{f}(H)$ puisque $a \star b \in H$
3. Avec la même notation, $x^{-1} = f(a^{-1}) \in \overrightarrow{f}(H)$ puisque $a^{-1} \in H$

b)

Pour K un sous-groupe de F, montrons que la préimage $\overleftarrow{f}(K)$ de K est un sous-groupe de E

1. $1_E \in \overleftarrow{f}(K)$ puisque $f(1_E) = 1_F \in K$
2. Si $a, b \in \overleftarrow{f}(K)$: $f(a \star b) = f(a) \otimes f(b) \in K$ donc $a \star b \in \overleftarrow{f}(K)$
3. Avec la même notation, $f(a^{-1}) = f(a)^{-1} \in K$ donc $a^{-1} \in \overleftarrow{f}(K)$

c)

Pour $x \in E$, montrons que l'ordre de $f(x)$ divise l'ordre de x.

Si $n \in \mathbb{N}$ est l'ordre de x: alors $x^n = 1_E$, donc $f(x)^n = f(1_E) = 1_K$.

Par propriété de l'ordre, on sait donc que n est un multiple de l'ordre de $f(x)$.

d)

Si $f : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/13\mathbb{Z}$ est un morphisme (additif): l'ordre de $f(1)$ divise 7 d'après c), mais divise également 13; il divise donc $\mathrm{PGCD}(7, 13) = 1$, conclusion $f(1) = 0$ et donc $f(k) = kf(1) = 0$ pour tout k.

Se généralise facilement: le seul morphisme $\mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ est la fonction nulle lorsque $\mathrm{PGCD}(a, b) = 1$.

e)

Si $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ est un morphisme (additif): l'ordre de $f(1)$ divise $\mathrm{PGCD}(3, 12) = 3$ donc $f(1) \in \{0, 4, 8\}$. On vérifie que ces trois choix donnent des morphismes: $f(k) = 0$, $g(k) = 4k$ et $h(k) = -4k$.

Exercice 6

a)

$\sigma = (1,\, 3,\, 6,\, 9)\,(2,\, 5,\, 7)\,(4,\, 10,\, 12,\, 8,\, 11)$

décomposition en cycles disjoints, en transpositions (non unique), par exemple:

$\sigma = (1,\, 3)\,(3,\, 6)\,(6,\, 9)\,(2,\, 5)\,(5,\, 7)\,(4,\, 10)\,(10,\, 12)\,(12,\, 8)\,(8,\, 11)$

$\mathrm{sg}(\sigma) = -1$

b)

Composée de 2 cycles dont les support ont exactement 1 élément en commun:

disons $\sigma = (i_1,\, i_2,\, \ldots,\, i_\ell)$ et $\tau = (j_1,\, j_2,\, \ldots,\, j_k)$ avec sans perte de généralité $i_1 = j_1 = a$

On trouve alors: $\sigma \circ \tau = (a,\, j_2,\, \ldots,\, j_k,\, i_2,\, \ldots,\, i_\ell)$ — faire un dessin !

c)

Décomposition de deux cycles dont les supports on exactement 2 éléments en commun:

disons $\sigma = (a, \underbrace{\dots}_{A}, b, \underbrace{\dots}_{B})$ et $\tau = (a, \underbrace{\dots}_{C}, b, \underbrace{\dots}_{D})$

On trouve alors $\sigma \circ \tau = (a, \underbrace{\dots}_{C}, \underbrace{\dots}_{B})\,(b, \underbrace{\dots}_{D}, \underbrace{\dots}_{A})$ — faire un dessin !!

d)

$$\sigma = \begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ p & v & l & w & i & h & c & b & f & a & z & o & t & e & q & k & d & x & n & s & u & y & m & g & j & r \end{bmatrix}$$

$\sigma = (a,\ p,\ k,\ z,\ r,\ x,\ g,\ c,\ l,\ o,\ q,\ d,\ w,\ m,\ t,\ s,\ n,\ e,\ i,\ f,\ h,\ b,\ v,\ y,\ j)$

un 25-cycle (u est un poitn fixe), signature $\mathrm{sg}(\sigma) = (-1)^{24} = +1$

Exercice 7: Groupe des permutations

1)

a) $(1,\ 2)\,(1,\ 3)\cdots(1,\ i) = (1,\ i,\ i-1,\ \dots\ 3,\ 2)$

b) $(1,\ i)\,(1,\ i-1)\cdots(1,\ 2) = (1,\ 2,\ \dots,\ i-1,\ i)$

c) $(1,\ i)\,(1,\ j)\,(1,\ i) = (i,\ j)$

d) $(j+1,\ j,\ j-1,\ \dots,\ 2,\ 1)\,(1,\ 2,\ \dots,\ j-1,\ j) = (j,\ j+1)$

e) $(i,\ i+1)\,(i+1,\ i+2)\cdots(j-2,\ j-1)\,(j-1,\ j) = (i,\ i+1,\ i+2,\ \dots,\ j-2,\ j-1,\ j)$

f) $(j,\ j-1)\,(j-1,\ j-2)\ \dots\ (3,\ 2)\,(2,\ 1) = (1,\ j,\ j-1,\ 3,\ 2)$

g) $(i,\ i+1,\ \dots,\ j-2,\ j-1)\,(j,\ j-1,\ \dots,\ i+1,\ i) = (i,\ j)$

2)

a) Toute permutation peut s'écrire comme composée d'éléments de A: en effet toute permutation peut s'écrire comme composée de transpositions, et par c) ci-dessus toute transposition peut s'écrire comme produit d'éléments de A.

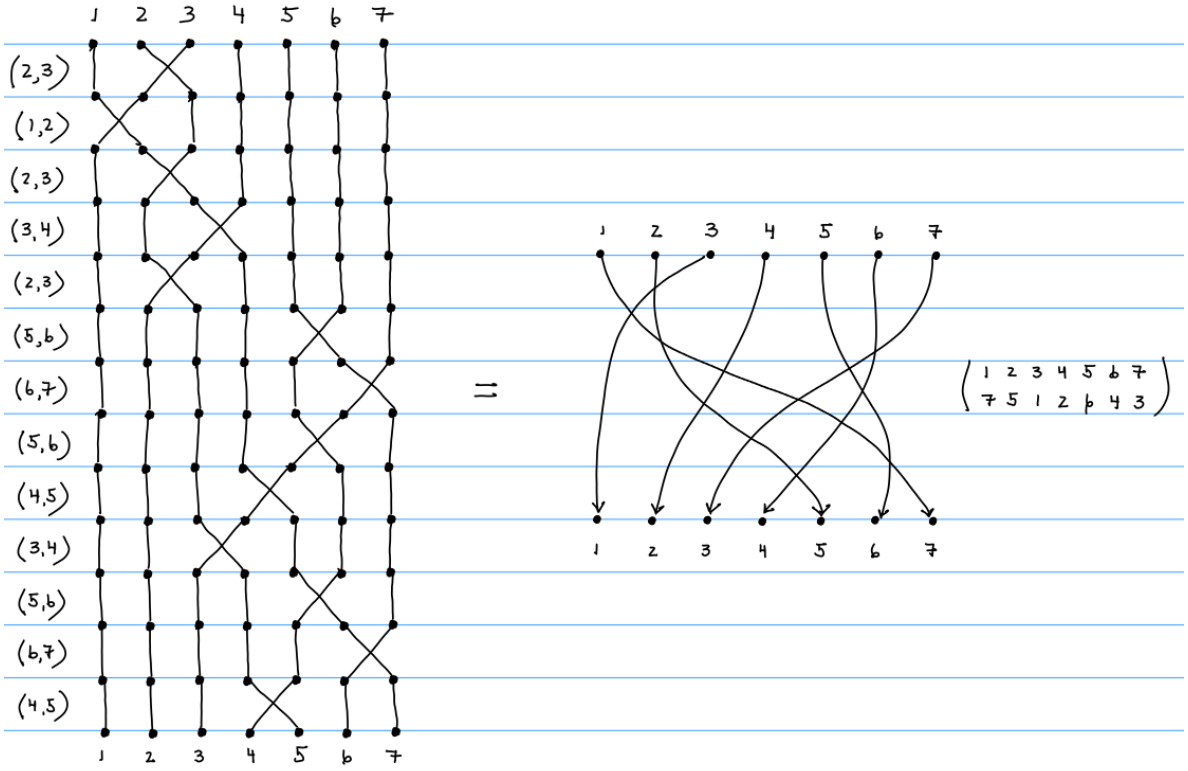
Par exemple: $\sigma = (1,\ 7,\ 3)\,(2,\ 5,\ 6,\ 4) = (1,\ 7)\,(7,\ 3)\,(2,\ 5)\,(5,\ 6)\,(6,\ 4)$

$\sigma = \underbrace{(1,\ 7)\,(1,\ 7)}_{\mathrm{id}}\,(1,\ 3)\,(1,\ 7)\,(1,\ 2)\,(1,\ 5)\,(1,\ 2)\,(1,\ 5)\,(1,\ 6)\,(1,\ 5)\,(1,\ 6)\,(1,\ 4)\,(1,\ 6)$

b) Toute permutation peut s'écrire comme composée d'éléments de B: en effet toute permutation peut s'écrire comme composée de transpositions, et d'après g) + e) toute transposition peut s'écrire comme composée de transpositions adjacentes — ce sont les croisements dans un diagramme sagittal.

Par exemple:

$\sigma = (4,\ 5)\,(6,\ 7)\,(5,\ 6)\,(3,\ 4)\,(4,\ 5)\,(5,\ 6)\,(6,\ 7)\,(5,\ 6)\,(2,\ 3)\,(3,\ 4)\,(2,\ 3)\,(1,\ 2)\,(2,\ 3)$



3)

Pour $\tau = (i,\, j)$, $\tau' = (k,\, \ell)$ deux transpositions, regardons le cardinal n de l'ensemble $\{i,\, j,\, k,\, \ell\}$ support de $\tau\,\tau'$:

- $n = 2$: ça signifie que $\tau = \tau'$, donc $\tau\,\tau' = \mathrm{id}$
- $n = 3$: disons SPDG $i = k$, alors $\tau\,\tau' = (i,\, j)\,(i,\, \ell) = (i,\, \ell,\, j)$ un 3-cycle, on a $(\tau\,\tau')^3 = \mathrm{id}$
- $n = 4$: alors τ et τ' commutent, on a $(\tau\,\tau')^2 = \tau^2\,(\tau')^2 = \mathrm{id}$

Dans tous les cas, $\tau\,\tau'$ est d'ordre ≤ 3

4)

Soit σ une permutation commutant avec toutes les transpositions.

a) Considérons $\tau = (1,\, 2)$. Puisque $(\sigma\,\tau)(n) = \sigma(n)$ doit être égal à $(\tau\sigma)(n) = \tau(\sigma(n))$, on conclut que $\sigma(n)$ doit être un point fixe de τ, i.e. $\sigma(n) \neq 1, 2$.

b) Dans l'argument précédent, on utilise le fait que $n > 1$ et $n > 2$. En prenant $\tau = (i,\, j)$ avec $i < j < n$ on conclut similairement que $\sigma(n) \neq i, j$. La seule possibilité est donc que $\sigma(n) = n$.

c) Par récurrence descendante, on voit que $\sigma(j) = j$ pour tout j, i.e. $\sigma = \mathrm{id}$.

Pour $n \geq 3$, la seule permutation commutant avec toutes les autres permutations (puisqu'elles sont engendrées par les transpositions) est id. (Qu'en est-il pour $n \leq 2$?)