
G
O
D
O
O
O
D

Exercice 4

$n \geq 2$ S_n

$\sigma = (1 \quad 2 \dots n)$

(a) $\sigma = (1\ 2\ 3\ 4)$

$\sigma^2 = (1\ 3) \circ (2\ 4)$

$\sigma^3 = (1\ 4\ 3\ 2)$

$\sigma^4 = Id$

pour $k \equiv 1 \mod 2$

(B) $n = 6$ $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$

$\sigma^2 = (1\ 3\ 5) \circ (2\ 4\ 6)$

$\sigma^3 = (1\ 4) \circ (2\ 5) \circ (3\ 6)$

$\sigma^4 = (1\ 5\ 3) \circ (2\ 6\ 4)$

$\sigma^5 = \begin{pmatrix} 1 \to 2 \to 6 \\ 2 \to 3 \to 1 \\ 3 \to 4 \to 2 \\ 4 \to 5 \to 3 \\ 5 \to 6 \to 4 \\ 6 \to 1 \to 5 \end{pmatrix} = (1\ 6\ 5\ 4\ 3\ 2)$

$\sigma^6 = Id$

$\sigma^k = (a_1 \dots a_6)$ $k = 1, 5$

C) $\tau = \sigma^k = (1\ 2 \dots n) \circ \dots \circ (1\ 2 \dots n)$

$a \in \mathbb{Z}$ $a[n] = a \mod n$

$\sigma(i) = i+1 \ [n]$ car $\begin{cases} 1 \to 2 \\ 2 \to 3 \\ \vdots \\ n \to n+1 = 1 \bmod n \end{cases}$

$\sigma^m(i) = \sigma^{m-1} \circ \sigma(i) = \sigma^{m-1}(i+1)$

$= \sigma^{m-2}(\sigma(i+1)) = i+2$

$= \sigma^2(\sigma(i+m-3)) = \sigma^2(i+m-2) = \sigma \circ \sigma(i+m-2) = \sigma(i+m-1)$

$= i+m \ [n]$

$\sigma^l = (\sigma^m)^l = \sigma^{ml} = i+ml \ [n]$

d) $\sigma^n(i) = \sigma^{mn}(i) = i + mn \ [n]$

$\equiv 0$

$= i$

$\Rightarrow \sigma^n = Id$

$\sigma^l = \sigma^{lm}(i) = i + lm \ [n]$

$\{\sigma^l(i)\}_{0 \le l \le n-1} = \{i, i+m, i+2m, i+3m, \dots, i+(n-1)m\}$

$= Orb_\sigma(i)$ (par définition)

qui contient n éléments distincts d'après le cours.

$\sigma^k(i) = i+k$

$o(\sigma) = n \qquad o(\sigma^k) = \frac{n}{pgcd(n,k)} = n$ car $pgcd(n,k) = 1$

Donc σ^k contient un est un seul cycle.

e) Il $d = pgcd(k,n)$

$k = dk' \qquad n = dn'$

$\sigma^{n'}(i) = i + kn' = i + dn'k'$

$= i + nk' \ [n]$

$\equiv 0 \ [n]$

donc $\sigma^{n'} = Id$

$\{f^\ell(i)\}_{0\le \ell \le n-1} = \{ i,\ i+k,\ i+2k,\ \dots,\ i+(n'-1)k,\ i+n'k$
$\vdots$
$i+(n'+1)k$
$= i+n'k+k$
$\vdots$
$\simeq i+k \}$

donc les éléments après $\ell \ge n'$ sont déjà dans $\{f^\ell(i)\}$ et se répètent.

Donc $|\{f^\ell(i)\}| \le n'$

f) $Orbf(1) \neq Orbf(2)$

Ce qui signifie que $\exists\ \sigma_1, \sigma_2 \in S_n$
σ_3 (qui peut être Id)
tq $f = \sigma_1 \circ \sigma_2 \circ \sigma_3$

Exercices

$\alpha := i\sqrt{5}$ $\quad \alpha^2 = -5$

(a) $\mathbb{Z}[i\sqrt{5}] = \{z \in \mathbb{C} : \exists a, b \in \mathbb{Z},\ z = a + bi\sqrt{5}\}$

Soit $z, z' \in \mathbb{Z}[i\sqrt{5}]$

i.e $\exists\ a, b, c, d \in \mathbb{Z}$

$z = a + bi\sqrt{5}$ $\quad z' = c + di\sqrt{5}$

$z - z' = \underbrace{(a-c)}_{\in\mathbb{Z}} + \underbrace{(b-d)}_{\in\mathbb{Z}} i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ donc $\mathbb{Z}[i\sqrt{5}]$

$1 + 0i\sqrt{5} = 1 \in \mathbb{Z}[i\sqrt{5}]$ et un sous-groupe
$0 + 0i\sqrt{5} = 0 \in \mathbb{Z}[i\sqrt{5}]$ additif.

$z \cdot z' = \underbrace{ac - bd5}_{\in\mathbb{Z}} + \underbrace{(bc + da)}_{\in\mathbb{Z}} i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$

$z \cdot 1 + 0i\sqrt{5} = a + bi\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ donc c'est bien un sous-anneau.

b) Soit $z = a + b\alpha \in \mathbb{Z}[i\sqrt{5}]$

$|z|^2 = |a + bi\sqrt{5}|^2 = a^2 + 5b^2$

$N(z) = a^2 + 5b^2 = |z|^2$

Notons $w = c + d\alpha$

$zw = (a + b\alpha)(c + d\alpha)$

$= ac + ad\alpha + bc\alpha + bd\alpha^2$
$= (ac - 5bd) + (ad + bc)\alpha$ $\quad (bdi\sqrt{5})^2 = -bd5$

$N(zw) = (ac - 5bd)^2 + 5(ad + bc)^2 = a^2c^2 - 10acbd + 25b^2d^2$
$+ 5a^2d^2 + 10acbd + 5b^2c^2$

$N(z)N(w) = (a^2 + 5b^2)(c^2 + 5d^2) = a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$

$= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$

Donc $N(zw) = N(z)N(w) \quad \forall \; z, w \in \mathbb{Z}[i\sqrt{5}]$

c) Soit $z = a + b\alpha$

$N(z) = a^2 + 5b^2$

$a^2 + 5b^2 = 1 \Rightarrow a^2 = 1$ et $5b^2 = 0$
ou $a^2 = 0$ et $5b^2 = 1$

$a^2 = 1 \Rightarrow a = 1, \; a = -1$

$5b^2 = 1 \Rightarrow b = \pm\frac{1}{\sqrt{5}} \notin \mathbb{Z}$

Donc $N(z) = 1 \Rightarrow a = 1$ ou $a = -1$

d) Soit $z = a + b\alpha \in \mathbb{Z}[i\sqrt{5}]$ avec $a, b \in \mathbb{Z}$

$zz' = |z|^2 = N(z) = 1 \Rightarrow a = 1$ ou $a = -1$

Donc $z = 1$ ou $z = -1$

Donc les éléments possédants une inverse sont:
$z = 1$ et $z = -1$

e) Supposons
$$N(z) = a^2 + 5b^2 = 2$$

$\Rightarrow a^2 = 1$ et $5b^2 = 1$ → cas impossible
ou $a^2 = 0$ et $5b^2 = 2$ $b^2 = \frac{2}{5} \notin \mathbb{Z}$
ou $a^2 = 2$ et $5b^2 = 0$ cas impossible

$a = \pm\sqrt{2} \notin \mathbb{Z}$ cas impossible.
Donc $N(z) = 2$ n'est pas possible.

$N(z) = a^2 + 5b^2 = 3$

$a^2 = 1$ et $5b^2 = 2$ imposs
$a^2 = 0$ et $5b^2 = 3$ → imposs
$a^2 = 3$ imposs et $5b^2 = 0$
$a^2 = 2$ imposs et $5b^2 = 1$

donc
$N(z) = 3$ impossible.

f)