Structures algébriques dec 2013, session 1, corrigé

Premier exercice

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 7 & 2 & 5 & 6 & 1 \end{pmatrix}$$

1) En appliquant l'algorithme, on trouve :

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

décomposition en cycles de supports disjoints

2) Comme les supports sont disjoints, les cycles commutent et

$$\sigma^2 = (1,3,7)\circ(2,4)\circ(1,3,7)\circ(2,4) = (1,3,7)^2\circ(2,4)^2$$
$$= (1,7,3)$$
$$\sigma^3 = (1,7,3)\circ(1,3,7)\circ(2,4) = (2,4)$$
$$\sigma^4 = (1,7,3)^2 = (1,3,7)$$
$$\sigma^5 = (1,7,3)\circ(2,4) \quad \text{par } \sigma^5 = \sigma^2\sigma^3$$
$$\underline{\sigma^6} = (\sigma^3)^2 = (2,4)^2 = \underline{id}$$

L'ordre de σ est six et $\langle\sigma\rangle = \{id, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$ est cyclique d'ordre six.

3) Le calcul fait précédemment montre que, comme les cycles de support disjoints commutent, on a :

si $s = s_{k_1}\circ s_{k_2}\circ\cdots\circ s_{k_\ell}$ où s_{k_i} est un k_i cycle

alors $s^m = s_{k_1}^m\circ s_{k_2}^m\circ\cdots\circ s_{k_\ell}^m$

Par unicité de la décomposition en cycles, $s^m = id$

$\Leftrightarrow \forall i \ s_{k_i}^m = id \Leftrightarrow \forall i \ k_i | m$.

La plus petite valeur de m est donc le ppcm des k_i

Par ailleurs, comme les cycles sont de supports disjoints
$k_1 + k_2 + \dots + k_\ell \leqslant 7$.

si $\ell = 1$: $k_1 \leqslant 7$, l'ordre maximal est 7

si $\ell = 2$ $k_1 + k_2 \leqslant 7$, on a $k_1 = 2$ $k_2 = 3, 4, 5$: ppcm max, 10
$k_1 = 3$ $k_2 = 3, 4$: ppcm max 12
$k_1 = 4$ $k_2 = 3$ ..

si $\ell = 3$ $k_1 + k_2 + k_3 \leqslant 7$ $k_1 = 2$, $k_2 = 2$, $k_3 = 2$
$k_1 = 2$, $k_2 = 2$, $k_3 = 3$ ...
$k_1 = 3$,

etc. le ppcm maximum est 12, obtenu par exple pour

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

Second exercice

1. $X^2 + \bar{1} \in \mathbb{F}_5[X]$; on cherche ses racines, ou par exemple, on remarque que :
$$X^2 + \bar{1} = X^2 - \bar{4} = (X - \bar{2})(X + \bar{2})$$, qui est une décomposition en irréductibles puisque tout polynôme du premier degré est irréductible.

L'idéal $I = (X^2 + \bar{1})$ n'est donc pas maximal puisque
$$(X^2 + \bar{1}) \subsetneq (X - \bar{2}) \subsetneq \mathbb{F}_5[X]$$
Le quotient $A = \mathbb{F}_5[X] / I$ n'est donc pas un corps.

2. D'après le rappel, $\operatorname{card} A = 5 \times 5 = 25$ car a et b parcourent $\mathbb{F}_5$

3. On peut affirmer que $1 + \alpha = \overline{X+1}$
est inversible car $(X + \bar{1}) \wedge (X^2 + \bar{1}) = 1$, d'après la factorisation précédente.

On peut calculer l'inverse de $1 + \alpha$ en partant de la division euclidienne : $X^2 + \bar{1} = (X + \bar{1})(X - \bar{1}) + \bar{2}$

d'où $0 = (1 + \alpha)(\alpha - 1) + 2$

ce qui donne $\underline{(1 + \alpha)^{-1} = 2\alpha + 3}$

3) Pour les calculs, on utilise $\alpha^2 = -\bar{1}$

$$(1+\alpha)^2 = 1 + 2\alpha + \alpha^2 = 2\alpha$$
$$(1+\alpha)^3 = 2\alpha(1+\alpha) = 2\alpha + 2\alpha^2 = \bar{2}\alpha - \bar{2} = \bar{2}\alpha + \bar{3}$$
$$(1+\alpha)^4 = (\bar{2}\bar{\alpha})^2 = \bar{4}\alpha^2 = -\bar{1} \times -\bar{1} = 1$$

L'ordre de $1+\alpha$ est donc 4. On aurait pu remarquer que $(1+\alpha)^3 = (1+\alpha)^{-1}$

4). Les non inversibles sont les classes des polynômes non premiers avec $X^2+\bar{1}$; ce sont donc les classes des polynômes de la forme $\bar{a}(X-\bar{2})$ et $\bar{a}(X+\bar{2})$

On trouve donc :

$$\bar{0},\ \alpha+3,\ 2\alpha+1,\ 3\alpha+4,\ 4\alpha+2$$
$$\alpha+2,\ 2\alpha+4,\ 3\alpha+1,\ 4\alpha+3$$

5) • Si a est un diviseur de zéro, il existe b non nul tel que $ab = 0$

a n'est pas inversible, sinon $a^{-1}(ab) = b = 0$ absurde.

• Supposons donc a non inversible :

L'application
$$\begin{aligned} B &\longmapsto B \\ x &\longmapsto ax \end{aligned}$$
n'est pas injective : sinon, comme B est fini, elle serait surjective et il existerait x tel que $ax = 1_B$, contrairement à l'hypothèse. Il existe donc $x \neq x'$ tel que $ax = ax'$.

Mézalor, $a(x-x') = 0$ prouve que a est un diviseur de zéro.

6) Les diviseurs de zéro sont donc huit :

On trouve facilement qu'un des éléments de la première ligne, comme $\alpha+3$, admet comme diviseur de zéro associé un de la seconde ligne :

$$(\alpha+3)(\alpha+2) = \alpha^2 + \bar{3}\alpha + \bar{2}\alpha + \bar{6} = \alpha^2 + \bar{1} = \bar{0}$$

7. Définissons φ par :

$$A \longrightarrow \mathbb{Z}[i]/(5) = C$$
$$\overline{a} + \overline{b}\alpha \longmapsto \overline{a+bi}$$

où $(\overline{a}, \overline{b}) \in \mathbb{F}_5$ et $\overline{a+bi}$ est la classe de $a+bi$ modulo (5)
$(a,b) \in \mathbb{Z}^2$

Il faut vérifier que φ est bien définie, bijective, et que c'est un morphisme.

Si $a \equiv a'(5)$ et $b \equiv b'(5)$ alors $a'+b'i = a+5q+(b+5q')i$
$= a+bi + 5(q+q'i)$

donc $\varphi(\overline{a}+\overline{b}\alpha)$ ne dépend pas des représentant.

Le même calcul montre que φ est surjective, car si $a+bi \in \mathbb{Z}[i]$, $a = 5q+r$ et $b = 5q'+r'$ donne $\overline{a+bi} = \overline{r+r'i} = \varphi(\overline{r}+\overline{r'}i)$; ainsi C admet 25 éléments comme A et φ est surjective.

Enfin $(\overline{a}+\overline{b}\alpha)(\overline{a'}+\overline{b'}\alpha) = \overline{aa'} - \overline{bb'} + (\overline{ab'}+\overline{a'b})\alpha$
et $(\overline{a+bi})(\overline{a'+b'i}) = \overline{aa'-bb'} + \overline{(ab'+a'b)}i$

prouve que φ est un isomorphisme.

Troisième exercice

1. Si $x \in G$, il existe n tel que $x \in \mathbb{U}_{2^n}$ et $x^{2^n} = 1$
Si $y \in G$, — m — — $y \in \mathbb{U}_{2^m}$ et $y^{2^m} = 1$

si $m \leq n$, alors $\left(y^{2^m}\right)^{2^{n-m}} = y^{2^n} = 1$

donc $xy \in \mathbb{U}_{2^n}$ et $xy \in G$; de même $x^{-1} \in \mathbb{U}_n$ donc $x^{-1} \in G$

2. $\mathbb{U}_4$ est inclus dans G ~~et~~ est un groupe ; c'est donc un sous-groupe.
Soit $F' \leq G$, $\operatorname{card} F' = 4$. Par le th de Lagrange,
$\forall x \in F'$, $x^4 = 1$ donc $F' \subset \mathbb{U}_4$ et il y a égalité car $\operatorname{card} F' = \operatorname{card} \mathbb{U}_4$

3. $(zz')^4 = z^4 z'^4$

4. $\forall x \in G$, $x = e^{\frac{2ki\pi}{2^n}}$ pour un $n \in \mathbb{N}$, $k \in \mathbb{Z}$.
alors $x' = e^{\frac{2ki\pi}{2^{n+4}}}$ vérifie $x'^4 = x$ et $x' \in \mathbb{U}_{2^{n+4}} \subset G$
Le th d'isom. permet de conclure