Groupes et géométrie, feuille 6

N. Perrin

À rendre le mercredi 18.03.2020

Correction le jeudi 20.03.2020

Exercice 1 ($7 \times 5 = 35$ Points) Soit A un anneau commutatif et n un entier.

(i) On note $A^\times$ l'ensemble des éléments inversibles de A. Montrer que $(A^\times, \times)$ est un groupe commutatif. Pour $A = \mathbb{Z}/n\mathbb{Z}$, on note $U(n)$ le groupe $A^\times$ et on note $\varphi(n)$ son ordre.

(ii) Montrer que $U(n) = \{[d] \in \mathbb{Z}/n\mathbb{Z} \mid d \text{ est premier avec } n\}$.

(iii) Montrer que $U(n)$ est cyclique pour $n \in \{2, 3, 5, 7\}$ mais que $U(8)$ n'est pas cyclique.

(iv) Montrer que si m et n sont premiers entre eux, alors $U(mn) \simeq U(m) \times U(n)$.

(v) Montrer que si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.

(vi) Le groupe $U(15)$ est-il cyclique ?

(vii) Montrer que $U(18)$ est cyclique et donner tous ses générateurs.

Solution. (i) On a $1 \in A^\times$ est l'élément neutre. Si $x, y \in A^\times$, alors $x^{-1} \in A^\times$ (avec $(x^{-1})^{-1} = x$) et $xy \in A^\times$ (avec $(xy)^{-1} = x^{-1}y^{-1}$.

(ii) Si d est premier avec n, alors il existe $u, v \in Z$ tels que $ud + vn = 1$ et modulo n, on obtient $[u][d] + [v][n] = [1]$ donc $[u][d] = 1$ et $[d]$ est inversible. Réciproquement, si $[d]$ est inversible, alors il existe $u \in \mathbb{Z}$ tel que $[u][d] = [1]$ donc $1 - ud$ est divisible par n *i.e.* il existe $v \in \mathbb{Z}$ tel que $1 - ud = vn$ et $ud + vn = 1$. On a bien que d et n sont premiers entre eux.

(iii) On a $U(2) = \{[1]\}$ qui est cyclique engendré par $[1]$. On a $U(3) = \{[1], [2]\}$ qui est cyclique engendré par $[2]$ (avec $[2]^2 = [1]$). On a $U(5) = \{[1], [2], [3], [4]\}$ qui est cyclique engendré par $[2]$: on a $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [3]$, $[2]^4 = [1]$. On a $U(7) = \{[1], [2], [3], [4], [5], [6]\}$ qui est cyclique engendré par $[3]$: on a $[3]^1 = [3]$, $[3]^2 = [2]$, $[3]^3 = [6]$, $[3]^4 = [4]$, $[3]^5 = [5]$, $[3]^6 = [1]$.

On a $U(8) = \{[1], [3], [5], [7]\}$ et $[1]^2 = [1]$, $[3]^2 = [1]$, $[5]^2 = [1]$ et $[7]^2 = [1]$. Donc tous les éléments sont d'ordre 2 et $U(8)$ est un groupe de Klein qui n'est pas cyclique.

(iv) Si m et n sont premiers entre eux, le lemme chinois nous dit que l'on a un isomorphisme $\mathbb{Z}/mn\mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. On obtient donc un ismorphisme $U(mn) = (\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/mZ)^\times \times (\mathbb{Z}/n\mathbb{Z})^\times = U(m) \times U(n)$

(v) Il suffit de dire que les cardinaux des deux groupes de la question (iv) sont égaux : $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux.

(vi) Le groupe $U(15)$ est isomorphe au produit $U(3) \times U(5)$. On a vu que $U(3)$ et $U(5)$ sont cycliques donc isomorphes respectivement à $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$. Le groupe $U(15)$ est don isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ qu in'est pas cyclique (par d'élément d'ordre 8.

(vii) On a $U(18) = \{[1], [5], [7], [11], [13], [17]\}$. On a $[5]^1 = [5]$, $[5]^2 = [7]$, $[5]^3 = [17]$, $[5]^4 = [13]$, $[5]^5 = [11]$ et $[5]^6 = 1$ donc $U(18)$ est cyclique et $[5]$ est un générateur. Le groupe $U(18)$ est donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$ donc les seuls générateurs sont 1 et son inverse -1. Donc $U(18)$ a deux générateurs : $[5]$ et son inverse $[5]^{-1} = [5]^5 = [11]$. ∎

Exercice 2 ($3 \times 5 = 15$ Points) Soit $\sigma = (3\ 7\ 1\ 4\ 2\ 6\ 9\ 8\ 5\ 10) \in \mathfrak{S}_{10}$.

(i) Écrire σ comme composée de cycles à supports disjoints.

(ii) Donner l'ordre de σ ainsi que $\varepsilon(\sigma)$ sa signature.

(iii) Calculer σ^{2019}.

Solution. (i) Pour trouver la décomposition en produit de cycles à supports disjoints, on regarde *les orbites de l'action de σ sur l'ensemble* $[1, 10]$ (cf. chapitre action d'un groupe sur un ensemble). On proc'ede de la manière suivante : on cherche tous les éléments qu'on peut obtenir à partir de 1 et en faisant agir σ :

$$1 \to \sigma(1) = 3 \to \sigma(3) = 1.$$

Ce sera notre premier cycle : [13] qui est la transposition qui échange 1 et 3. C'est un cycle de longueur 2. On continue avec le premier élément de $[1, 10]$ qu'on a pas encore trouvé, ici 2 :

$$2 \to \sigma(2) = 7 \to \sigma(7) = 9 \to \sigma(9) = 5 \to \sigma(5) = 2.$$

On obtient le cycle [2795] (c'est la permutation de support $\{2, 5, 7, 9\}$ qui envoie 2 sur 7, 7 sur 9, 9 sur 5 puis 5 sur 2). C'est un cycle de longueur 4. On continue avec 4 :

$$4 \to \sigma(4) = 4.$$

C'est un cycle de longueur 1 : [4] c'est en fait l'identité. En général on ne l'écrit pas. Le suivant est 6, encore une fois

$$6 \to \sigma(6) = 6.$$

C'est un cycle de longueur 1 : [6] c'est en fait l'identité. Le suivant est 8, encore une fois

$$8 \to \sigma(8) = 8.$$

C'est un cycle de longueur 1 : [8] c'est en fait l'identité. Le suivant est 10, encore une fois

$$10 \to \sigma(10) = 10.$$

C'est un cycle de longueur 1 : [10] c'est en fait l'identité. On obtient la décomposition

$$\sigma = [13][2795][4][6][8][10] = [13][2795].$$

(ii) Par la Proposition 3.8.6 et le Lemme 3.8.4, l'ordre d'un produit de cycles disjoints est le ppcm des ordres de chacun des cycles et l'ordre d'un cycle est égal /'a sa longueur. L'ordre de σ est donc $\text{ppcm}(2, 4, 1, 1, 1) = \text{ppcm}(2, 4, 1, 1, 1) = 4$

Par le Théorème 3.9.3, un cycle c est pair si et seulement si sa longueur r est impaire c'est-à-dire $\varepsilon(c) = (-1)^{r-1}$. On a donc $\varepsilon([13]) = (-1)^{2-1} = -1$, $\varepsilon([2795]) = (-1)^{4-1} = -1$ et $\varepsilon([4]) = \varepsilon([6]) = \varepsilon([8]) = \varepsilon([10]) = 1$? On obtient $\varepsilon(\sigma) = \varepsilon([13])\varepsilon([2795])\varepsilon([4])\varepsilon([6])\varepsilon([8])\varepsilon([10]) = (-1)^2 = 1$.

(iii) Comme σ est d'odre 4, on a $\sigma^4 = 1$ donc comme $2019 = 4 \times 504 + 3$, on a $\sigma^{2019} = \sigma^3 = [13][2597] = (3\ 5\ 1\ 4\ 9\ 6\ 2\ 8\ 7\ 10)$. ∎

Exercice 3 ($2 \times 10 = 20$ Points) Soit $G = \mathfrak{S}_4$.

(i) Calculer $D(G)$.

(ii) Calculer $D(\mathfrak{A}_4)$.

Solution. (i) On va montrer que $D(\mathfrak{S}_4) = \mathfrak{A}_4$. On sait que $D(G)$ est engendré par les commutateurs $(g,h) = ghg^{-1}h^{-1}$ pour $g, h \in G$. Mais on a $\varepsilon((g,h)) = \varepsilon(g)\varepsilon(h)\varepsilon(g)^{-1}\varepsilon(h)^{-1} = 1$ donc $(g,h) \in \mathfrak{A}_4$ et donc $D(G) \subset \mathfrak{A}_4$.

Réciproquement, il suffit de montrer que tous les 3-cycles sont dans $D(G)$ car $\mathfrak{A}_4$ est engendré par les 3-cycles (Théorème 3.9.3). Par exemple, on a $([12],[13]) = [12][13][12][13] = [123]$. De même on obtient tous les 3-cycles.

(ii) On va montrer que $D(\mathfrak{A}_4) = V_4 = \{\mathrm{Id}, [12][34], [13][24], [14][23]\}$. Pour celà, on remarque que $V_4 \triangleleft \mathfrak{A}_4$ (cf. TD 5) et que $[\mathfrak{A}_4 : V_4] = |\mathfrak{A}_4|/|V_4| = 3$ donc $\mathfrak{A}_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ est commutatif. Ceci impose l'inclusion $D(\mathfrak{A}_4) \subset V_4$ par le Lemme 2.5.2.(iv). On montre que $V_4 \subset D(\mathfrak{A}_4)$. On a $([123],[124]) = [123][124][132][142] = [12][34]$ qui est donc dans $D(\mathfrak{A}_4)$. De même, on obtient tous les éléments de V_4.

Exercice 4 ($3 \times 10 = 30$ Points) Soit n un entier

(i) Montrer que tout 3-cycle est un carré, c'est-à-dire de la forme σ^2 pour un $\sigma \in \mathfrak{S}_n$.

(ii) Montrer que $\mathfrak{A}_n = \langle \sigma^2 \mid \sigma \in \mathfrak{S}_n \rangle$.

(iii) Montrer que $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$.

Solution. (i) Soit σ un 3-cycle. On a $\sigma^3 = 1$ donc $\sigma = (\sigma^{-1})^2$ est un carré.

(ii) On a vu au (i) que tout 3-cycle est dans $\langle \sigma^2 \mid \sigma \in \mathfrak{S}_n \rangle$ et comme $\mathfrak{A}_n$ est engendré par les 3-cycles (Théorème 3.9.3), on obtient $\mathfrak{A}_N \subset \langle \sigma^2 \mid \sigma \in \mathfrak{S}_n \rangle$.

Par ailleurs $\varepsilon(g^2) = \varepsilon(g)^2 = 1$ donc $\langle \sigma^2 \mid \sigma \in \mathfrak{S}_n \rangle \subset \mathfrak{A}_n$.

(iii) Soit H un sous-groupe d'indice 2 de $\mathfrak{S}_n$. Montrons que $\mathfrak{A}_n = \langle \sigma^2 \mid \sigma \in \mathfrak{S}_n \rangle$ est contenu dans H. Soit $g \in \mathfrak{S}_n$, on a $[g]^2 = [1]$ dans $\mathfrak{S}_n/H$ car ce groupe est d'ordre 2. On a donc $g^2 \in H$ ce qui montre l'assertion. Mais $|H| = |\mathfrak{S}_n|/2 = |\mathfrak{A}_n|$ donc on a l'égalité $\mathfrak{A}_n = H$. ∎