



Algèbre et Arithmétique 3

*Éléments de correction
de l'examen du vendredi 19 avril 2013*

Exercice 1

Soient $x, y \in E$ tels que $g(x) = g(y)$. Alors $f(g(x)) = f(g(y))$, soit $(f \circ g)(x) = (f \circ g)(y)$. Comme $f \circ g$ est injective, on en déduit $x = y$, ce qu'il fallait démontrer.

Exercice 2

Toutes les assertions étaient fausses.

1 Prenons $\mathbf{K} = \mathbf{R}$, et $P = (X^2 + 1)^2$. Alors pour tout $x \in \mathbf{R}$, on a $P(x) > 0$, donc P n'a pas de racine dans $\mathbf{R}$. Par contre P est de degré 4 et possède un diviseur de degré 2, donc P n'est pas irréductible.

2 Prenons $\mathbf{K} = \mathbf{R}$ et $P = X^2 + 1$. Comme P n'a pas de racine dans $\mathbf{R}$ et est de degré 2, P est irréductible dans $\mathbf{R}[X]$. Par contre l'écriture $X^2 + 1 = (X + i)(X - i)$ montre que P n'est pas irréductible dans $\mathbf{C}[X]$.

3 Prenons $p = 2$ et $x = y = [1]_2$ (on pouvait être plus précis et montrer que pour p donné, l'assertion est vraie si et seulement si p est congru à 3 modulo 4)

4 Le groupe $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, +)$ est cyclique (on rappelle que la loi de groupe est définie par $(a, b) + (a', b') = (a + a', b + b')$).

Pour $x, y \in \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, on a $2 \cdot (x, y) = (2 \cdot x, 2 \cdot y) = (0, 0)$. Ainsi l'ordre de tout élément de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ divise 2. En particulier $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ n'a aucun élément d'ordre 4. Étant de cardinal 4, il ne peut être cyclique.

5 1 est une racine n -ème de l'unité, mais est d'ordre 0.

6 Si r est le reste d'une division euclidienne de a par b , on doit avoir $N(r) < N(b)$, or ici $N(2 + i) = N(1 + 2i) = 1^2 + 2^2$.

Exercice 3

On renvoie au cours pour la correction.

Exercice 4

1 Pour $x \in \mathbf{Z}/17\mathbf{Z}$, on a

$$x^2 - [2]_{17} \cdot x + [2]_{17} = (x - [1]_{17})^2 - [1]_{17} + [2]_{17} = (x - [1]_{17})^2 - [16]_{17} = (x - [1]_{17} + [4]_{17})(x - [1]_{17} - [4]_{17}).$$

Ainsi

$$x^2 - [2]_{17} \cdot x + [2]_{17} = [0]_{17} \iff (x + [3]_{17})(x - [5]_{17}) = [0]_{17}$$

Comme 17 est premier, $\mathbf{Z}/17\mathbf{Z}$ est intègre, d'où

$$x^2 - [2]_{17} \cdot x + [2]_{17} = [0]_{17} \iff (x + [3]_{17} = [0]_{17} \text{ ou } x - [5]_{17} = [0]_{17})$$

Finalement

$$x^2 - [2]_{17} \cdot x + [2]_{17} = [0]_{17} \iff x \in \{[14]_{17}, [5]_{17}\}.$$

2 Pour $x \in \mathbf{Z}/p\mathbf{Z}$, on a

$$x^2 - [2]_p \cdot x + [2]_p = (x - [1]_p)^2 + [1]_p$$

soit

$$x^2 - [2]_p \cdot x + [2]_p = [0]_p \iff (x - [1]_p)^2 = [-1]_p.$$

Ainsi, si l'équation proposée a des solution, -1 est un carré modulo p (et d'après le cours cette condition équivaut à $p = 2$ ou p est congru à 1 modulo 4). Réciproquement, s'il existe $c \in \mathbf{Z}/p\mathbf{Z}$ tel que $[-1]_p = c^2$, on conclut comme dans la première question que les solutions de l'équations sont $[1]_p + c$ et $[1]_p - c$. Ainsi l'équation proposée a des solutions si et seulement si -1 est un carré modulo p si et seulement si $p = 2$ ou p est congru à 1 modulo 4.

Exercice 5

1 La signature d'un r -cycle est $(-1)^{r+1}$, et si $\sigma \in \mathfrak{S}_n$ s'écrit comme le produit de cycles à support disjoints $c_1 c_2 \dots c_k$, la signature de σ est $\varepsilon(c_1) \dots \varepsilon(c_k)$. Pour être complet dans la définition de la signature, il faut ajouter que par définition la signature de Id est 1.

2 Soit d_1, d_2, d_3 trois éléments deux à deux distincts de $\{1, \dots, n\}$ et $c = (d_1, d_2, d_3)$. On a (calcul immédiat) $(d_1, d_2, d_3)^2 = (d_1, d_3, d_2)$ d'où $(d_1, d_2, d_3)^3 = (d_1, d_3, d_2)(d_1, d_2, d_3) = \text{Id}$. Donc l'ordre de c divise 3, et comme $c \neq \text{Id}$, c est d'ordre 3.

3 Une première possibilité pour répondre à la question est d'écrire la liste de tous les éléments de $\mathfrak{S}_4$ (il y en a $4! = 24$) et en utilisant la définition de la signature de déterminer au cas par cas ceux qui parmi eux sont de signature 1.

Une manière un peu plus conceptuelle de raisonner est la suivante. Id est évidemment dans $\mathfrak{A}_4$. Les cycles qui sont dans $\mathfrak{A}_4$ sont les cycles de longueur impair. Comme la longueur d'un cycle de $\mathfrak{S}_4$ est 2, 3, ou 4, les cycles qui sont dans $\mathfrak{A}_4$ sont les 3-cycles. Le choix du support d'un 3-cycle correspond au choix de 3 éléments parmi 4, il y a donc 4 possibilités pour le support. Une fois le support $\{a, b, c\}$ fixé, on vérifie aisément qu'il n'y a exactement deux 3-cycles ayant un tel support à savoir (a, b, c) et (a, c, b) .

Les seuls éléments de $\mathfrak{S}_4$ qui ne sont pas des cycles et qui sont distincts de Id sont les produits $\sigma = \tau_1 \tau_2$ de deux transpositions à supports disjoints (en effet dans une décomposition en cycles à supports disjoints dans $\mathfrak{S}_n$, la somme des longueurs des cycles de la décomposition, qui n'est autre que le cardinal de l'union des supports, est toujours inférieure ou égale à n ; comme la longueur d'un cycle est au moins 2, on conclut aisément). Leur signature est $\varepsilon(\tau_1)\varepsilon(\tau_2) = (-1)^2 = 1$. Noter qu'un tel élément σ de $\mathfrak{S}_4$ n'a pas de point fixe, et qu'il est entièrement déterminé par l'image a de 1 : si on note $\{1, 2, 3, 4\} \setminus \{1, a\} = \{b, c\}$, on a $\sigma = (1, a)(b, c)$. Il y a donc 3 tels éléments dans $\mathfrak{A}_4$.

Finalement on a

$$\begin{aligned} \mathfrak{A}_4 = \{ & \text{Id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 2, 3), (1, 3, 2), \\ & (1, 2, 4), (1, 4, 2), (1, 3, 4), (1, 4, 3), (2, 3, 4), (2, 4, 3) \}. \end{aligned}$$

4 Comme un 3-cycle est d'ordre 3, d'après le théorème de Lagrange aucun 3-cycle ne peut être contenu dans un sous-groupe de K d'ordre 4. Ainsi tout sous-groupe de $\mathfrak{A}_4$ d'ordre 4 est nécessairement inclus dans le complémentaire de l'ensemble des 3-cycles dans $\mathfrak{A}_4$, donc dans

$$K \stackrel{\text{déf}}{=} \{ \text{Id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3) \}$$

Or K est de cardinal 4. Donc tout sous-groupe d'ordre 4 de $\mathfrak{A}_4$ est nécessairement égal à K . Il reste à vérifier que K est bien un sous-groupe de $\mathfrak{A}_4$. Ceci peut facilement (quoiqu'un poil fastidieusement) se faire à la main.

Il peut aussi être utile pour alléger les calculs de commencer par remarquer que si σ et τ sont deux éléments distincts de $K \setminus \{\text{Id}\}$, on a

$$K = \{\text{Id}, \sigma, \tau, \tau\sigma = \sigma\tau\}$$

et par ailleurs $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \text{Id}$.

5 Notons $a = (1, 0)$, $b = (1, 1)$, $c = (0, 1)$. On calcule facilement la table d'addition de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

Par ailleurs, en conservant les notations introduites précédemment, on calcule tout aussi aisément la table du groupe K .

$\circ$	Id	σ	τ	$\sigma\tau$
Id	Id	σ	τ	$\sigma\tau$
σ	σ	Id	$\sigma\tau$	τ
τ	τ	$\sigma\tau$	Id	σ
$\sigma\tau$	$\sigma\tau$	τ	σ	Id

Ce sont les « mêmes » tables, aux notations près ! Cela entraîne que l'application $\varphi : \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ définie par $\varphi(0) = \text{Id}$, $\varphi(a) = \sigma$, $\varphi(b) = \tau$ et $\varphi(c) = \sigma\tau$ est un isomorphisme de $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ sur K .

Exercice 6

1 Soit $z \in \mathbf{Z}[i]$ alors $z \in \mathbf{Z}[i]^\times$ si et seulement si $N(z) = 1$. On renvoie au cours pour la démonstration.

2 Non (bien qu'il soit de norme 1) car $\frac{1}{\sqrt{2}} \notin \mathbf{Z}$, donc en fait ce n'est même pas un élément de $\mathbf{Z}[i]$.

3 Comme $N(z)$ est premier, on a $N(z) \notin \{0, 1\}$, donc z n'est ni nul, ni inversible. Soit $u, v \in \mathbf{Z}[i]$ tels que $z = uv$. Alors $p = N(z) = N(u)N(v)$. Comme p est premier et $N(u)$ et $N(v)$ sont des entiers naturels, on a donc soit $N(u) = 1$, soit $N(v) = 1$, donc soit u inversible soit v inversible. Ainsi z est bien irréductible.

Exercice 7

1 Notons $c' = (\tau(d_1), \tau(d_2), \dots, \tau(d_{r-1}), \tau(d_r))$. Il s'agit d'un cycle de support $\{\tau(d_1), \dots, \tau(d_r)\}$. Il s'agit de vérifier l'égalité $\tau.c = c'\tau$.

Soit m qui n'est pas dans le support de c . Comme τ est une bijection, $\tau(m)$ n'est pas dans le support de c' , et on a

$$(c'\tau)(m) = c'(\tau(m)) = \tau(m) = \tau(c(m)) = (\tau.c)(m)$$

Pour $i \in \{1, \dots, r-1\}$, on a

$$(c'\tau)(d_i) = c'(\tau(d_i)) = \tau(d_{i+1}) = \tau(c(d_i)) = (\tau.c)(d_i)$$

et par ailleurs

$$(c'\tau)(d_r) = c'(\tau(d_r)) = \tau(d_1) = \tau(c(d_r)) = (\tau.c)(d_r)$$

On a donc bien l'égalité demandée.

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

3 D'après les deux questions précédentes on a

$$\tau.\sigma.\tau^{-1} = \tau(1, 3, 4)\tau^{-1}.\tau(6, 7)\tau^{-1}(\tau(1), \tau(3), \tau(4))(\tau(6), \tau(7))$$

Ainsi on a $\tau\sigma = \sigma\tau$ si et seulement si

$$(\tau(1), \tau(3), \tau(4))(\tau(6), \tau(7)) = (1, 3, 4)(6, 7)$$

Comme τ est une bijection, les cycles $(\tau(1), \tau(3), \tau(4))$ et $(\tau(6), \tau(7))$ sont bien à supports disjoints. Par unicité de la décomposition en cycles à supports disjoints, cette égalité est équivalente à $(\tau(1), \tau(3), \tau(4)) = (1, 3, 4)$ et $(\tau(6), \tau(7)) = (6, 7)$. On peut montrer (les détails sont laissés au lecteur intéressé qui n'aurait pas traité cette question) que les τ qui vérifient cette propriété sont exactement ceux qui s'écrivent

$$(1, 3, 4)^{\ell_1}(6, 7)^{\ell_2}(2, 5)^{\ell_3}$$

où $\ell_1 \in \{0, 1, 2\}$ et $\ell_2, \ell_3 \in \{0, 1\}$.

Exercice 8

Pour $a, b \in \text{Ker}(\varphi)$, on a $\varphi(a + b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$ et $\varphi(-a) = -\varphi(a) = 0$. Par ailleurs $0 \in \text{Ker}(\varphi)$. Ainsi $\text{Ker}(\varphi)$ est un sous-groupe de A . Pour $a \in \text{Ker}(\varphi)$ et $b \in A$, on a

$$\varphi(a \times b) = \varphi(a) \times \varphi(b) = 0 \times \varphi(b) = 0.$$

Ainsi $a \times b \in \text{Ker}(\varphi)$. Donc $\text{Ker}(\varphi)$ est bien un idéal de A .

Montrons que $\varphi(A)$ est un sous-anneau de B . Pour $a, a' \in A$, on a $a + a' \in A$, $-a \in A$, $\varphi(a) + \varphi(a') = \varphi(a + a')$ et $-\varphi(a) = \varphi(-a)$. Donc $\varphi(A)$ est stable par addition et passage à l'opposé. Par ailleurs $0_B = \varphi(0_A) \in \varphi(A)$. Donc $\varphi(A)$ est un sous-groupe de B .

Pour $a, a' \in A$, on a $a \times a' \in A$ et $\varphi(a) \times \varphi(a') = \varphi(a \times a') \in \varphi(A)$. Donc $\varphi(A)$ est stable par multiplication.

Enfin on a $1_B = \varphi(1_A) \in \varphi(A)$. Ceci conclut la démonstration