

Chapitre 1

Correction des exercices

EXERCICE 1 : Soit A un anneau unitaire tel que $A^* = A \setminus \{0\}$ soit un groupe multiplicatif. Montrer que A est un corps.

Comme A est un anneau unitaire et A^* un groupe multiplicatif, tout élément de A^* est inversible et A est donc un corps.

EXERCICE 2 : Montrer qu'un anneau A est un corps si et seulement s'il a au moins deux éléments et que chacune des équations
$$\begin{cases} ax = b \\ ya = b \end{cases}$$
 possède au moins une solution dans cet anneau pour tout $a \in A^*$ et pour tout $b \in A$.

Soit K un corps. Quelque soit $a \neq 0$ dans K et quel que soit b dans K alors $ax = b$ et $ya = b$ ont chacune une solution unique $x = a^{-1}b$ et $y = ba^{-1}$.

Inversement soit A un anneau. Comme il contient au moins deux éléments, il n'est pas réduit à $\{0\}$. Soit $a \in A^*$. Il existe au moins un élément e tel que $ae = a$. Pour tout élément $r \in A$, il existe $s \in A$ tel que $r = sa$. Ainsi $re = sae = sa = r$. De même il existe e' tel que $e'a = a$ et s' tel que $r = as'$. Ainsi $e'r = e'as' = as' = r$. Donc e est un élément unité à droite et e' un élément unité à gauche.

On en déduit $e'e = e' = e$ et e est une unité de l'anneau A . Montrons que tout élément $a \in A^*$ est inversible. Choisissons $b = e$ dans les équations. Il existe donc a' et a'' dans A tel que $aa' = e$ et $a''a = e$. Ainsi $a''aa' = ea' = a' = a''e = a''$ et a est inversible. A est donc un corps.

EXERCICE 3 : Montrer que tout anneau intègre ayant un nombre fini d'éléments est un corps.

On suppose que l'anneau intègre A contient au moins deux éléments. Considérons la table de multiplication de A . La ligne associée à l'élément $a \in A^*$ correspond aux produits ax pour $x \in A$ et la colonne aux produits xa pour $x \in A$. Comme A est intègre $ax_1 = ax_2$ implique $x_1 = x_2$. Ainsi, comme A est fini, la ligne associée à a contient tous les éléments de A . On en déduit que l'équation $ax = b$ admet une solution. De même, en regardant la colonne passant par a , l'équation $ya = b$ admet une solution. D'après l'exercice 2, A est un corps.

EXERCICE 4 : Soit $\mathbb{H} = \left\{ \begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}, \alpha, \beta \in \mathbb{C} \right\}$.

$\mathbb{C}$ est un corps puisque $\mathbb{C}$ est un sous-anneau de $M_2(\mathbb{C})$ (avec l'addition et la multiplication des matrices) et $\mathbb{H}^*$ est un groupe (multiplicatif). Il est appelé corps des quaternions.

1. Montrer que tout élément $A \in \mathbb{H}$ s'écrit de manière unique

$$A = a1 + bI + cJ + dK \quad \text{avec } a, b, c, d \in \mathbb{R}$$

$$\text{où } 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

$$\text{Soit } A = \begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a+ib & -c-id \\ c-id & a-ib \end{pmatrix} \quad \text{avec } \begin{cases} \alpha = a+ib \\ \beta = c+id \\ a, b, c, d \in \mathbb{R} \end{cases}$$

$$A = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

$$= a1 + bI + cJ + dK. \quad a, b, c, d \in \mathbb{R}.$$

De plus cette décomposition est unique puisque si

$$A = a1 + bI + cJ + dK = a'1 + b'I + c'J + d'K$$

$$\Leftrightarrow \begin{pmatrix} a+ib & -c-id \\ c-id & a-ib \end{pmatrix} = \begin{pmatrix} a'+ib' & -c'-id' \\ c'-id' & a'-ib' \end{pmatrix} \Leftrightarrow \begin{cases} a+ib = a'+ib' \\ a-ib = a'-ib' \\ c+id = c'+id' \\ c-id = c'-id' \end{cases}$$

$$\Leftrightarrow \begin{cases} a' = a, & c' = c \\ b' = b, & d' = d \end{cases}.$$

2. Etablir la table de multiplication concernant les éléments $1, I, J, K$.

	1	I	J	K
1	1	I	J	K
I	I	-1	K	-J
J	J	-K	-1	I
K	K	J	-I	-1

par exemple $I \times I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$

$$I J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = K$$

$$I K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 0 & +1 \\ -1 & 0 \end{pmatrix} = -J$$

3. Soit $A = a1 + bI + cJ + dK$ un élément de $\mathbb{H}$.

On pose $\bar{A} = a1 - bI - cJ - dK$. Démontrer quelques propriétés de l'application $A \mapsto \bar{A}$ appelée conjugaison.

L'application conjugaison est une involution:

$$\overline{(\bar{A})} = A.$$

Mais ce n'est pas un morphisme de corps.

On a bien $\overline{A+B} = \bar{A} + \bar{B}$

mais $\overline{AB} \neq \bar{A} \cdot \bar{B}$

En effet si $A = a1 + bI + cJ + dK$ et $B = a'1 + b'I + c'J + d'K$

$$AB = (aa' - bb' - cc' - dd')1 + (ab' + ba' + cd' - dc')I \\ + (ac' - bd' + ca' + db')J + (ad' + bc' - cb' + da')K$$

donc $\overline{AB} = (aa' - bb' - cc' - dd')1 + (-ab' - ba' - cd' + dc')I \\ + (-ac' + bd' - ca' - db')J + (-ad' - bc' + cb' - da')K$

et $\bar{A} \bar{B} = (a1 - bI - cJ - dK)(a'1 - b'I - c'J - d'K) \\ = (aa' - bb' - cc' - dd')1 + (-ba' + cd' - dc' - ab')I \\ + (-bd' - ca' + db' - ac')J + (bc' - cb' - da' - ad')K$

En fait on a

$$\begin{aligned}\overline{B} \cdot \overline{A} &= (a'1 - b'I - c'J - d'K) (a1 - bI - cJ - dK) \\ &= (aa' - bb' - cc' - dd') 1 + (-a'b - b'a + c'd - d'c) I \\ &\quad (-a'c - b'd - c'a + d'b) J + (-a'd + b'c - c'b - d'a) K\end{aligned}$$

$$\overline{\overline{B} \cdot \overline{A}} = \overline{\overline{AB}}$$

On a aussi les propriétés suivantes : si $A = a1 + bI + cJ + dK$ $a, b, c, d \in \mathbb{R}$

$$\frac{\overline{A} + A}{2} = a1 \in \mathcal{M}_2(\mathbb{R}) \Rightarrow (A = a1 \Leftrightarrow \overline{A} = A)$$

$$\frac{A - \overline{A}}{2} = bI + cJ + dK \Rightarrow (A = bI + cJ + dK \Leftrightarrow \overline{A} = -A)$$

4. On considère $\mathbb{H}$ comme un espace vectoriel réel de dimension 4.
Montrer que l'application $A \mapsto \sqrt{A\overline{A}}$ est bien définie
et est une norme.

Soit $A = a1 + bI + cJ + dK$ avec $a, b, c, d \in \mathbb{R}$,
alors $A\overline{A} = (a1 + bI + cJ + dK)(a1 - bI - cJ - dK)$
 $= (a^2 + b^2 + c^2 + d^2) 1 + (-ab + ba + cd - dc) I$
 $\quad (-ac + bd + ac - bd) J + (-ad - bc + cb + da) K$
 $= (a^2 + b^2 + c^2 + d^2) 1$ identifié avec $a^2 + b^2 + c^2 + d^2 \in \mathbb{R}^+$

l'application $A \mapsto \sqrt{A\overline{A}} = \sqrt{a^2 + b^2 + c^2 + d^2}$ est donc
bien définie.

C'est bien une norme puisque $\sqrt{A\overline{A}} \geq 0$,
 $\sqrt{A\overline{A}} = 0 \Leftrightarrow \sqrt{a^2 + b^2 + c^2 + d^2} = 0 \Leftrightarrow a = 0 = b = c = d$
 $\Leftrightarrow A = 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$

et $\sqrt{\lambda A \cdot \overline{\lambda A}} = \sqrt{(\lambda a)^2 + (\lambda b)^2 + (\lambda c)^2 + (\lambda d)^2} = |\lambda| \sqrt{A\overline{A}}$
pour $\lambda \in \mathbb{R}$.

Il faut encore prouver que $\sqrt{(A+B)(\overline{A+B})} \leq \sqrt{A\overline{A}} \sqrt{B\overline{B}}$

EXERCICE 5 : On désigne par $\mathbb{Q}(\sqrt{2})$ l'ensemble des nombres réels de la forme $a+b\sqrt{2}$ avec $a, b \in \mathbb{Q}$.

Montrer que $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$

$$\text{On a } \mathbb{Q}(\sqrt{2}) = \{ a+b\sqrt{2} \mid a, b \in \mathbb{Q} \}.$$

Soit $a \in \mathbb{Q}$ alors $a = a+0 \times \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ donc $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$.

De plus $\mathbb{Q}(\sqrt{2})$ est un sous-ensemble non vide de $\mathbb{R}$ contenant

$$0 = 0+0\sqrt{2} \text{ et } 1 = 1+0\sqrt{2};$$

pour tous $a_0+b_0\sqrt{2}$ et $a_1+b_1\sqrt{2}$ appartenant à $\mathbb{Q}(\sqrt{2})$ on a

$$(a_0+b_0\sqrt{2}) + (a_1+b_1\sqrt{2}) = \underbrace{(a_0+a_1)}_{\in \mathbb{Q}} + \underbrace{(b_0+b_1)}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

$$\text{et } (a_0+b_0\sqrt{2}) \times (a_1+b_1\sqrt{2}) = \underbrace{(a_0a_1+2b_0b_1)}_{\in \mathbb{Q}} + \underbrace{(a_0b_1+b_0a_1)}_{\in \mathbb{Q}} \sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

$$\underbrace{-a_0}_{\in \mathbb{Q}} + \underbrace{(-b_0)}_{\in \mathbb{Q}} \sqrt{2}$$

donc l'opposé d'un élément de $\mathbb{Q}(\sqrt{2})$ est encore dans $\mathbb{Q}(\sqrt{2})$.

L'inverse d'un élément $a_0+b_0\sqrt{2} \neq 0$ est l'élément

$$* \underbrace{\frac{1}{a_0}}_{\in \mathbb{Q}} + \underbrace{\frac{1}{2b_0}}_{\in \mathbb{Q}} \sqrt{2} \quad \text{si } a_0 \neq 0 \neq b_0.$$

$$* \frac{1}{2b_0} \sqrt{2} \quad \text{si } a_0 = 0, b_0 \neq 0.$$

$$* \frac{1}{a_0} \quad \text{si } a_0 \neq 0 \text{ et } b_0 = 0.$$

donc c'est toujours un élément de $\mathbb{Q}(\sqrt{2})$.

$$\text{Ainsi } 0 \in \mathbb{Q}(\sqrt{2}), \quad -(a_0+b_0\sqrt{2}) \in \mathbb{Q}(\sqrt{2}) \quad \exists (a_0+b_0\sqrt{2}) + (a_1+b_1\sqrt{2})$$

$$\Rightarrow (\mathbb{Q}(\sqrt{2}), +) \text{ sous-groupe de } (\mathbb{R}, +)$$

$$1 \in \mathbb{Q}(\sqrt{2}), \quad (a_0+b_0\sqrt{2}) \times (a_1+b_1\sqrt{2}) \in \mathbb{Q}(\sqrt{2}) \text{ et } (a_0+b_0\sqrt{2})^{-1} \in \mathbb{Q}(\sqrt{2})$$

$$\Rightarrow (\mathbb{Q}^*(\sqrt{2}), \times) \text{ est un sous-groupe de } (\mathbb{R}^*, \times) \quad \text{si } a_0+b_0\sqrt{2} \neq 0$$

$$\Rightarrow \mathbb{Q}(\sqrt{2}) \text{ est un sous-corps de } \mathbb{R}.$$

EXERCICE 6 : Soient K_1 et K_2 deux corps. Soit $f: K_1 \rightarrow K_2$ un homomorphisme non nul de corps.

1. Montrer que f est injectif.

2. On suppose maintenant que $K_1 = K_2$ et que ce corps soit fini. Montrer alors que f est bijectif.

1. On sait que $\text{Ker } f$ est un idéal de K_1 . Or les seuls idéaux d'un corps sont $\{0\}$ et lui-même. Donc $\text{Ker } f = K_1$ ou $\text{Ker } f = \{0\}$. Si $\text{Ker } f = K_1$, alors $f \equiv 0$ ce qui est contraire à l'hypothèse de départ. Ainsi $\text{Ker } f = \{0\}$ et f est injective.

2. Une application injective entre deux ensembles ayant le même nombre d'éléments est surjective. L'homomorphisme f est donc aussi surjective. Elle est donc bijective.

EXERCICE 7 : Déterminer à isomorphisme près tous les corps de cardinalité 2, 3, 4 et 6.

Corps de cardinalité 2 : il est constitué de l'élément neutre pour l'addition et de l'élément neutre pour la multiplication.

+	0	ε
0	0	ε
ε	ε	0

x	ε
ε	ε

Corps de cardinalité 3 : $F_3 = \{0, \varepsilon, a\}$ avec les tables d'addition et de multiplication suivantes

+	0	ε	a
0	0	ε	a
ε	ε	a	0
a	a	0	ε

x	ε	a
ε	ε	a
a	a	ε

isomorphe à $(\mathbb{Z}/3\mathbb{Z}, +)$

Corps à 4 éléments : $F_4 = \{0, e, a, b\}$.

+	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

isomorphe à $((\mathbb{Z}/2\mathbb{Z})^2, +)$

x	e	a	b
e	e	a	b
a	a	b	e
b	b	e	e

isomorphe à $(\mathbb{Z}/3\mathbb{Z}, +)$.

En effet la caractéristique de F_4 divise l'ordre de F_4 donc 4 et est un nombre premier. C'est donc 2.

Nous construirons ce corps comme corps de rupture (associé à un polynôme irréductible ...)

Il n'existe pas de corps fini à 6 éléments.

Tout corps fini est de cardinalité p avec p premier et sa cardinalité est une puissance de p . Comme 6 n'est pas une puissance de 2 ou de 3, il n'existe pas de corps à 6 éléments.

EXERCICE 8 :

Soient A un anneau intègre unitaire et K un corps commutatif. Soit $f: A \rightarrow K$ un homomorphisme injectif d'anneau unitaire. Montrer que f se prolonge de manière unique en un homomorphisme de corps $f^*: K_A \rightarrow K$ où K_A est le corps des fractions de A .

$$\text{On a } K_A \ni \frac{a}{b} = \left\{ (c, d) \in A \times A^*, ad - bc = 0 \right\}$$

$$\text{Prenons } f^*: K_A \longrightarrow K$$

$$\frac{a}{b} \longmapsto f(a) f(b)^{-1}$$

Pour que f^* prolonge f on doit avoir $f^*\left(\frac{a}{1}\right) = f(a)$ ce qui est bien le cas puisque $f(a) f(1)^{-1} = f(a)$ (1 est l'élément neutre pour la multiplication).

Montrons que f^* ainsi défini est bien un homomorphisme de corps.

Tout d'abord f^* est bien définie

$$\text{si } \frac{a'}{b'} = \frac{a}{b}$$

$b \neq 0 \neq b'$ et $a'b = ab'$, et $f(b) \neq 0 \neq f(b')$ puisque f est injective donc $f(b)$ et $f(b')$ sont inversibles

$$\text{On a } f^*\left(\frac{a'}{b'}\right) = f(a') f(b')^{-1}$$

$$\text{Or } f(a'b) = f(ab') \text{ donc } f(a') f(b) = f(a) f(b') \\ \text{et } f(a') f(b')^{-1} = f(a) f(b)^{-1}.$$

$$\text{Ainsi } f^*\left(\frac{a'}{b'}\right) = f(a) f(b)^{-1} = f^*\left(\frac{a}{b}\right).$$

L'application f^* est bien un homomorphisme de corps :

$$f^*\left(\frac{a}{b} + \frac{c}{d}\right) = f^*\left(\frac{ad+cb}{bd}\right) = f(ad+cb) f(bd)^{-1} \\ = (f(a)f(d) + f(c)f(b)) f(b)^{-1} f(d)^{-1} \\ = f(a) f(b)^{-1} + f(c) f(d)^{-1} = f^*\left(\frac{a}{b}\right) + f^*\left(\frac{c}{d}\right)$$

$$f^*\left(\frac{a}{b} \times \frac{c}{d}\right) = f^*\left(\frac{ac}{bd}\right) = f(ac) f(bd)^{-1} = f(a) f(c) f(b)^{-1} f(d)^{-1} \\ = f^*\left(\frac{a}{b}\right) \times f^*\left(\frac{c}{d}\right).$$

$$f^*\left(\frac{0}{b}\right) = f(0) f(b)^{-1} = 0$$

$$f^*\left(\frac{1}{1}\right) = f(1) = 1$$

Montrons que f^* est l'unique homomorphisme de corps qui prolonge f .

Supposons que g est un autre homomorphisme de corps qui prolonge f

$$g\left(\frac{a}{1}\right) = f(a) = f^*\left(\frac{a}{1}\right) \text{ pour tout } a \in A.$$

$$\text{On a } g\left(\frac{1}{1}\right) = g\left(\frac{b}{b}\right) = g\left(\frac{b}{1}\right) g\left(\frac{1}{b}\right) = g\left(\frac{b}{1}\right) \times g\left(\left(\frac{b}{1}\right)^{-1}\right)$$

$$\underset{1}{1} \quad \text{donc } g\left(\frac{1}{b}\right) = g\left(\left(\frac{b}{1}\right)^{-1}\right) = g\left(\frac{b}{1}\right)^{-1} = f(b)^{-1}$$

$$g\left(\frac{a}{b}\right) = g\left(\frac{a}{1} \times \frac{1}{b}\right) = g\left(\frac{a}{1}\right) g\left(\frac{1}{b}\right) = f(a) f(b)^{-1} = f^*\left(\frac{a}{b}\right)$$

pour tout $(a, b) \in (A, A^*)$.

$$\text{donc } g = f^*.$$

EXERCICE 9 : Soit K un corps fini. Montrer que l'homomorphisme de Frobenius est un automorphisme.

Déterminer cet automorphisme lorsque $K = \mathbb{Z}/p\mathbb{Z}$, p étant premier.

Comme K est un corps fini il est de caractéristique $p \neq 0$ avec p premier. Soit $f: K \rightarrow K$ l'homomorphisme de Frobenius.

$$x \mapsto x^p$$

Frobenius. Alors

$$f(x+y) = (x+y)^p = x^p + C_p^1 x^{p-1} y + C_p^2 x^{p-2} y^2 + \dots + C_p^{p-1} x y^{p-1} + y^p$$

Mais pour tout $0 < k < p$ on a $p \mid C_p^k$.

en effet $k C_p^k = k \frac{p!}{k!(p-k)!} = \frac{p!}{(k-1)!(p-k)!} = p \times \frac{(p-1)!}{(k-1)!(p-1-(k-1))!}$

$$= p C_{p-1}^{k-1}$$

Donc p divise $k C_p^k$ et puisque p ne divise pas k , d'après le lemme d'Eulide p divise C_p^k .

Ainsi $f(x+y) = x^p + y^p = f(x) + f(y)$.

On a aussi $f(xy) = (xy)^p = x^p y^p = f(x) f(y)$.

et $f(1) = 1$

Donc f est un homomorphisme de corps qui est non nul donc injectif. Puisque $|K| < +\infty$ il est aussi surjectif donc f est un automorphisme (on va de K dans lui-même).

Prenons maintenant $K = \mathbb{Z}/p\mathbb{Z}$ (avec p premier). C'est un corps de caractéristique p .

$$f: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$$

$$x \mapsto x^p$$

$$1 \mapsto 1^p = 1$$

donc f est l'identité.