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 $a \in A^*$ pour tout $b \in A$.

Soit $\mathbb{K}$ un corps. Quelque soit $a \neq 0$ dans $\mathbb{K}$ et quel que soit b dans $\mathbb{K}$ 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 droite.
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.

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 $\mathbb{H} = \left\{ \begin{pmatrix} \alpha & -\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}, \ \alpha, \beta \in \mathbb{C} \right\}$.

C'est un corps puisque c'est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$ (avec l'addition et la multiplication des matrices) et $\mathbb{H}^*$ est un gr (multiplicatif
Il est appelé corps des quaternions.

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

$$A = a\mathbb{1} + bI + cJ + dK \quad \text{avec } a, b, c, d \in \mathbb{R}$$

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

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

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

$$= a\mathbb{1} + bI + cJ + dK. \qquad a,b,c,d \in \mathbb{R}.$$

De plus cette décomposition est unique puisque si

$$A = a\mathbb{1} + bI + cJ + dK = a'\mathbb{1} + b'I + c'J + d'K$$

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

$1, I, J, K$.

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

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

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

3. Soit $A = a1 + bI + cJ + dK$ un élément de $\mathbb{H}$.
On pose $\overline{A} = a1 - bI - cJ - dK$. Démontrer quelques propriétés de l'application $A \longmapsto \overline{A}$ appelée conjugaison.

L'application conjugaison est une involution :

$\left(\overline{\overline{A}}\right) = A$.

Mais ce n'est pas un morphisme de corps.
On a bien $\quad \overline{A+B} = \overline{A} + \overline{B}$
mais $\quad \overline{AB} \neq \overline{A}.\overline{B}$
En effet si $A = a1 + bI + cJ + dK$ et $B = a'1 + b'I + c'J + d'$
$AB = (aa' - bb' - cc' - dd')1 + (ab' + ba' + cd' - dc')I$
$\quad + (ac' - bd' + ca' + db')J + (ad' + bc' - cb' + da')K$
donc $\quad \overline{AB} = (aa' - bb' - cc' - dd')1 + (-ab' - ba' - cd' + dc')I$
$\quad + (-ac' + bd' - ca' - db')J + (-ad' - bc' + cb' - da')K$

et $\overline{A}\,\overline{B} = (a1 - bI - cJ - dK)(a'1 - b'I - c'J - d'K)$
$\quad = (aa' - bb' - cc' - dd')1 + (-ba' + cd' - dc' - ab')I$

v

$$\overline{B}.\overline{A} = (a'1 - b'I - c'J - d'K)(a1 - bI - cJ - dK)$$
$$= (aa' - bb' - cc' - dd')1 + (-a'b - b'a + c'd - d'c)I$$
$$(-a'c - b'd - c'a + d'b)J + (-a'd + b'c - c'b - d'a)K$$
$$\overline{B}\,\overline{A} = \overline{AB}$$

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

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

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

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

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

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

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

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 $\sqrt{(A+B)(\overline{A+B})} \leqslant \sqrt{A\overline{A}} + \sqrt{B\overline{B}}$

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 $\mathbb{Q}$

On a $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}\ ,\ a,b\in\mathbb{Q}\}$.
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 $\mathbb{R}$ contena
$0 = 0+0\sqrt{2}$ 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

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

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 $\frac{1}{a_0+b_0\sqrt{2}} \in$
Or $\frac{1}{a_0+b_0\sqrt{2}} = \frac{a_0-b_0\sqrt{2}}{a_0^2-2b_0^2} = \underbrace{\frac{a_0}{a_0^2-2b_0^2}}_{\in\mathbb{Q}} + \underbrace{\frac{-b_0}{a_0^2-2b_0^2}}_{\in\mathbb{Q}}\sqrt{2}$ donc cet inverse est bien dans $\mathbb{Q}(\sqrt{2})$.

Rappelons que $\sqrt{2}$ est irrationnel i.e $\sqrt{2}\neq\frac{p}{q}$ $(p,q)\in\mathbb{Z}\times$
donc $a_0^2-2b_0^2$ est toujours différent de 0 pour $(a_0,b_0)\neq($

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

Ainsi: $0\in\mathbb{Q}(\sqrt{2})$, $-(a_0+b_0\sqrt{2})\in\mathbb{Q}(\sqrt{2})$ $\exists\,(a_0+b_0\sqrt{2})+(a_1+b_1\sqrt{2})$
$\Rightarrow$ $(\mathbb{Q}(\sqrt{2}),+)$ sous-groupe de $(\mathbb{R},+)$
$1\in\mathbb{Q}(\sqrt{2})$, $(a_0+b_0\sqrt{2})\times(a_1+b_1\sqrt{2})\in\mathbb{Q}(\sqrt{2})$ et $(a_0+b_0\sqrt{2})^{-1}\in\mathbb{Q}($
si $a_0+b_0\sqrt{2}\neq$
$\Rightarrow$ $(\mathbb{Q}^*(\sqrt{2}),\times)$ est un sous groupe de $(\mathbb{R}^*,\times$

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

un homomorphisme non nul de corps.

1. Montrer que f est injectif.
2. On suppose maintenant que $\mathbb{K}_1 = \mathbb{K}_2$ et que ce corps soit fini. Montrer alors que f est bijectif.

1. On sait que $\operatorname{Ker} f$ est un ideal de $\mathbb{K}_1$. Or les seuls idéaux d'un corps sont $\{0\}$ et lui-même. Donc $\operatorname{Ker} f = \mathbb{K}_1$ ou $\operatorname{Ker} f = \{0\}$. Si $\operatorname{Ker} f = \mathbb{K}_1$ alors $f \equiv 0$ ce qui est contraire à l'hypothèse de départ. Ainsi $\operatorname{Ker} f = \{0\}$ et f est injectiv

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'élement neutre pour l'addition et de l'élément neutre pour la multiplication.

+	0	ε
0	0	ε
ε	ε	0

×	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

×	ε	a
ε	ε	a
a	a	ε

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

+	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 $\left((\mathbb{Z}/2\mathbb{Z})^2, +\right)$

×	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 $\mathbb{K}$ un corps commutatif. Soit $f : A \to \mathbb{K}$ un homomorphisme injectif d'anneau unitaire. Montrer que f se prolonge de manière unique en un homomorphisme de corps $f^* : \mathbb{K}_A \to \mathbb{K}$ où $\mathbb{K}_A$ est le corps des fractions de A.

On a $\quad \mathbb{K}_A \ni \dfrac{a}{b} = \left\{ (c,d) \in A \times A^*, \ ad - bc = 0 \right\}$

Prenons

$$f^* : \mathbb{K}_A \longrightarrow \mathbb{K}$$
$$\frac{a}{b} \longmapsto f(a)\, f(b)^{-1}$$

Pour que f^* prolonge f on doit avoir $f^*\left(\dfrac{a}{1}\right) = f(a)$ 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 homorphisme de
corps

si $\dfrac{a'}{b'} = \dfrac{a}{b}$ $b \neq 0 \neq b'$ et $a'b = ab'$, et $f(b) \neq 0$, puisque f est injective donc $f(b)$ et $f(b')$ sont inver

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

Or $f(a'b) = f(ab')$ donc $f(a')f(b) = f(a)f(b')$

et $f(a')\,f(b')^{-1} = f(a)\,f(b)^{-1}$.

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

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

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

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

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

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

Supposons que g est un autre homomorphisme de corps qui prolonge f $g\left(\frac{a}{1}\right) = f(a) = f^*\left(\frac{a}{1}\right)$ pour tout $a \in A$.

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

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

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

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

donc $g \equiv f^*$.

sme de Frobenius est un automorphisme.
Déterminer cet automorphisme lorsque $\mathbb{K} = \mathbb{Z}/_{p\mathbb{Z}}$, p étant premier

Comme $\mathbb{K}$ est un corps fini il est de caractéristique $p \neq 0$ avec p premier. Soit $f : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & x^p \end{array}$ l'homomorphisme de Frobenius. Alors

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

Mais pour tout $0 < k < p$ on a $p \mid C_p^k$.
en effet
$$k\, C_p^k = k \frac{p!}{k!(n-k)!} = \frac{p!}{(k-1)!\,(n-k)!} = p \times \frac{(p-1)!}{(k-1)!(n-1\cdot}$$
$$= p\, C_{p-1}^{k-1}$$

Donc p divise $k\, C_p^k$ et puisque p ne divise pas k, d'après le lemme d'Euclide 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 $|\mathbb{K}| < +\infty$ il est aussi surjectif donc f est un automorphisme (on va de $\mathbb{K}$ dans lui-mê

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

$$f : \begin{array}{ccc} \mathbb{Z}/_{p\mathbb{Z}} & \longrightarrow & \mathbb{Z}/_{p\mathbb{Z}} \\ x & \longmapsto & x^p \\ 1 & \longmapsto & 1^p = 1 \end{array}$$

donc f est l'identité.