Chapitre 2
Structures algébriques

Nous avons vu que beaucoup de règles des opérations sur les nombres réels sont aussi valables pour les matrices, voir les lemmes 1.12 et 1.19. Mais en même temps nous avons vu que le passage des nombres aux matrices créée des différences importantes, notamment la perte de la commutativité de la multiplication. Dans ce chapitre nous allons discuter des structures algébriques qui non seulement capturent les diffrences entre les nombres et les matrices mais aussi couvrent beaucoup d'autres objets (fonctions, polynômes, division euclidienne, ...). Vous avez déjà vu une partie de ce chapitre dans le cours de Géométrie I.

2.1 Groupes

Définition 2.1 *Un* ***groupe*** *[group] est un ensemble G muni d'une loi de composition*

$$\begin{array}{rccc} \star: & G\times G & \to & G \\ & (a,b) & \mapsto & a\star b \end{array}$$

satisfaisant les axiomes suivants :

1. *La loi $\star$ est associative, c-à-d*
$$a\star(b\star c)=(a\star b)\star c \quad \forall a,b,c\in G.$$
2. *Il existe un élément $e\in G$ (appelé* ***élément neutre*** *ou* ***identité*** *[identity]) tel que*
$$a=e\star a=a\star e \quad \forall a\in G.$$
3. *Pour tout $a\in G$ il existe un élément $a^{-1}\in G$ (appelé* ***l'inverse*** *de a) tel que*
$$a^{-1}\star a=a\star a^{-1}=e.$$

Définition 2.2 *Un groupe $(G,\star)$ est dit* ***abélien*** *ou* ***commutatif*** *si*

$$a\star b=b\star a \quad \forall a,b\in G.$$

Lemme 2.3 *Soit $(G,\star)$ un groupe. Alors :*

1. *l'élément neutre e est unique,*
2. *l'inverse de $a\in G$ est unique,*
3. *$(a^{-1})^{-1}=a$ pour tout $a\in G$,*
4. *$(a\star b)^{-1}=b^{-1}\star a^{-1}$ pour tous $a,b\in G$.*

DÉMONSTRATION. Voir les exercices de Géométrie I. ■

2.1.1 Exemples des groupes

Les nombres. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\{+1,-1\},\cdot),(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},\cdot)$ sont des groupes abéliens.

Le plus petit groupe. $G=\{e\}$ avec $e\star e=e$.

Les matrices. Soit K un corps, alors $(M_{m\times n}(K),+)$ est un groupe abélien. En effet, la matrice nulle $0_{m\times n}$ est l'élément neutre. Les axiomes des définitions 2.1 et 2.2 découlent du lemme 1.12.

$(M_{n\times n}(K),\cdot)$ n'est pas un groupe si $n\geq 2$, car il existe des matrices $n\times n$ non nulle, non inversibles. Mais, l'ensemble des matrices inversibles $n\times n$ muni du produit matriciel forme un groupe noté $GL_n(K)$ et appelé **groupe général linéaire**. C'est une conséquence du résultat suivant plus général.

Lemme 2.4 *Soit $(H,\star)$ un **monoïde**, c-à-d la stabilité ainsi que les axiomes 1 et 2 de la définition 2.1 sont satisfaits. Alors, l'énsemble*

$$H^*=\{a\in H\,|\,il\ existe\ a^{-1}\in H\ avec\ a^{-1}\star a=a\star a^{-1}=e\}$$

muni de la loi de composition $\star$ est un groupe.

DÉMONSTRATION. Il faut vérifier que H^* est stable. Tout d'abord $H^*\neq\emptyset$, car $e\in H^*$. Or, soient $a,b\in H^*$ avec les inverses a^{-1},b^{-1}. On a

$$(b^{-1}\star a^{-1})\star(a\star b)=b^{-1}\star(a^{-1}\star a)\star b=b^{-1}\star b=e$$

et, de façon similaire, $(a\star b)\star(b^{-1}\star a^{-1})=e$. Alors, $a\star b\in H^*$. La validité des axiomes 1 et 2 dans H^* vient de leur validité dans H. ■

$(M_{n\times n}(K),\cdot)$ est un monoïde : l'associativité découle de (1.10) et l'élément neutre est la matrice identité I_n.

Applications. Soit E un ensemble non vide, on considère

$$\mathsf{App}(E):\{f:E\to E\,|\,f\text{ est une application de }E\text{ vers }E\}.$$

On définit pour $f,g\in\mathsf{App}(E)$ une loi de composition $f\circ g$ comme suit :

$$(f\circ g)(x)=f(g(x))\quad\forall x\in E.$$

On a alors que $(\mathsf{App}(E),\circ)$ est un monoïde. L'application identité $\mathsf{id}(x)=x$ pour tout $x\in E$ est l'élément neutre :

$$(\mathsf{id}\circ f)(x)=\mathsf{id}(f(x))=f(x)=f(\mathsf{id}(x))=(f\circ\mathsf{id})(x),$$

donc $\mathsf{id}\circ f=f\circ\mathsf{id}=f$.

D'après le lemme 2.4 $(\mathsf{App}(E)^*,\circ)$ est un groupe. Ce groupe est donné par

$$\mathsf{App}(E)^*=\{f:E\to E\,|\,f\text{ bijective}\}.$$

En effet : si $f\in\mathsf{App}(E)$ est inversible alors il existe $g\in\mathsf{App}(E)$ telle que $g\circ f=f\circ g=\mathsf{id}$, ceci implique que f est bijective. Réciproquement : si $f\in\mathsf{App}(E)$ est bijective, alors la réciproque de l'application f est

$$f^{-1}:E\to E,\quad y\mapsto f^{-1}(y)=x\text{ tel que }f(x)=y.$$

On a $f^{-1}\circ f = f\circ f^{-1} = \mathrm{id}$, donc f est inversible.

Si E est un ensemble fini, le groupe $\mathrm{App}(E)^*$ est appelé **groupe symétrique**, dénoté $S(E)$. Pour $E=\{1,2,\ldots,n\}$ on dénote $S(E)$ par S_n et $(S_n,\circ)$ est appelé le **groupe des permutations**. Les éléments de S_n s'appellent des permutations. On remarque que S_n n'est pas un groupe abélien.

La table suivante simplifie le traitement des permutations :

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}, \quad \pi \in S_n. \tag{2.1}$$

La composition $\pi\circ\sigma$ de $\pi,\sigma\in S_n$ prend la forme

$$\begin{pmatrix} 1 & \cdots & n \\ \pi(1) & \cdots & \pi(n) \end{pmatrix} \circ \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & \cdots & n \\ \pi(\sigma(1)) & \cdots & \pi(\sigma(n)) \end{pmatrix}.$$

L'inverse ou la réciproque π^{-1} est l'application $\pi(i)\mapsto i$ pour $i=1,\ldots,n$. On obtient la table correspondante en échangeant les deux lignes,

$$\begin{pmatrix} \pi(1) & \cdots & \pi(n) \\ 1 & \cdots & n \end{pmatrix},$$

et en réordonnant la première (et son image dans la deuxième) par ordre croissant.

Exemple 2.5 Soient

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix},$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

L'inverse de σ :

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

La composition $\pi\circ\sigma$:

$$\pi\circ\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \pi(1) & \pi(4) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Sous MATLAB on traite les permutations comme des vecteurs :

```
>> pi    = [ 4 2 3 1 ];
>> sigma = [ 1 4 2 3 ];
```

Par `pi(sigma)` on obtient le vecteur `pi(sigma(1))`, `pi(sigma(2))`, ..., qui constitue la composition de π et de σ.

```
>> pi(sigma)
ans =
     4   1   2   3
```

L'inverse σ^{-1} satisfait $\sigma^{-1}(\sigma(1)) = 1$, $\sigma^{-1}(\sigma(2)) = 2$, ... Cette relation permet d'obtenir l'inverse sous MATLAB :

```
>> r = [];
>> r(sigma) = 1:4,
r =
     1   3   4   2
```

Groupes finis. Voir Géométrie I.

2.1.2 Sous-groupes

Définition 2.6 *Soit $(G,\star)$ un groupe et $H\subseteq G$. Alors $(H,\star)$ est un sous-groupe de G si*

1. *H est non vide,*
2. *si $a,b\in H$ alors $a\star b\in H$ (H est stable par $\star$),*
3. *$a^{-1}\in H$ pour tout $a\in H$.*

Lemme 2.7 *Si $(H,\star)$ est un sous-groupe de $(G,*)$ alors $(H,*)$ est un groupe.*

DÉMONSTRATION. Exercice. ■

Soit $(G,\star)$ un groupe et soit e son élément neutre. Alors, $(\{e\},\star)$ et $(G,\star)$ sont des sous-groupes de $(G,\star)$. Les sous-groupes entre les deux extrêmes sont plus intéressants.

Groupe orthogonal. On considère les **matrices de rotation**

$$SO(2) := \left\{ G(\phi) = \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} \;\middle|\; \phi \in [0,2\pi[\right\}.$$

Alors, $SO(2)$ est un sous-groupe de $GL_2(\mathbb{R})$ (exercices).

Matrices 2×2 particulières. On considère

$$M_2 := \left\{ A(a,b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a,b \in \mathbb{R} \right\}.$$

Alors, $(M_2,+)$ est un sous-groupe de $(M_{2,2}(\mathbb{R}),+)$ et $(M_2 \setminus \{A(0,0)\},\cdot)$ un sous-groupe de $GL_2(\mathbb{R})$ (exercices).

Matrices triangulaires. On considère l'ensemble des matrices triangulaires supérieures à éléments diagonaux non nuls :

$$\widetilde{\mathsf{triu}}(n) = \left\{ U = \begin{pmatrix} u_{11} & \dots & u_{1n} \\ & \ddots & \vdots \\ 0 & & u_{nn} \end{pmatrix} \;\middle|\; u_{11} \neq 0, \dots, u_{nn} \neq 0 \right\}.$$

Lemme 2.8 *Soient $R,S \in \widetilde{\mathsf{triu}}(n)$. Alors, le produit $T = RS$ est encore dans $\widetilde{\mathsf{triu}}(n)$.*

DÉMONSTRATION. Étant donné que les matrices R,S sont triangulaires supérieures, on a $r_{ik} = 0$ si $i > k$ et $s_{kj} = 0$ si $k > j$. Si $i > j$,

$$t_{ij} = \sum_{k=1}^{n} r_{ik}s_{kj} = t_{ij} = \sum_{k=1}^{i-1} \underbrace{r_{ik}}_{=0} s_{kj} + \sum_{k=i}^{n} r_{ik} \underbrace{s_{kj}}_{=0} = 0.$$

Alors, T est triangulaire supérieure. En outre,

$$t_{ii} = \sum_{k=1}^{i-1} \underbrace{r_{ik}}_{=0} s_{ki} + r_{ii}s_{ii} + \sum_{k=i+1}^{n} r_{ik} \underbrace{s_{ki}}_{=0} = r_{ii}s_{ii} \neq 0$$

pour $i = 1,\dots,n$. ■

Lemme 2.9 *Soit $U \in \widetilde{\mathsf{triu}}(n)$. Alors, U est inversible et $U^{-1} \in \widetilde{\mathsf{triu}}(n)$.*

DÉMONSTRATION. Par récurrence sur n. Si $n = 1$ l'assertion est triviale. On suppose que l'assertion est vraie pour $n-1$. En partitionnant

$$U = \begin{pmatrix} U_{11} & u_n \\ 0 & u_{nn} \end{pmatrix},$$

on a $U_{11} \in \widetilde{\mathsf{triu}}(n-1)$ et $u_{nn} \neq 0$. Par hypothèse de récurrence, U_{11} est inversible. En définissant

$$U^{-1} = \begin{pmatrix} U_{11}^{-1} & -U_{11}^{-1}u_n u_{nn}^{-1} \\ 0 & u_{nn}^{-1} \end{pmatrix},$$

on vérifie sans peine que $U^{-1}U = UU^{-1} = I_n$. Alors, U est inversible et $U^{-1} \in \widetilde{\text{triu}}(n)$. ■

Les lemmes 2.8 et 2.9 montrant que $\widetilde{\text{triu}}(n)$ est un sous-groupe de $GL_n(K)$. Idem pour des matrices triangulaires inférieures à éléments diagonaux non nuls (exercices).

2.1.3 Morphismes, isomorphismes de groupes

Définition 2.10 *Soient $(G,\star)$ et $(H,\circ)$ deux groupes. Un **morphisme de groupes** [group homomorphism] est une application $f : G \to H$ telle que*

$$f(a \star b) = f(a) \circ f(b) \quad \forall a,b \in G.$$

*Si de plus f est bijective, on dit que f est un **isomorphisme de groupes** [group isomorphism].*

Lemme 2.11 *Soit $f : G \to H$ un morphisme du groupe $(G,\star)$ dans le groupe $(H,\circ)$. Alors,*

(i) $f(e_G) = e_H$, où e_G et e_H sont les éléments neutres de G et H respectivement

(ii) $f(a^{-1}) = \big(f(a)\big)^{-1}$ pour tout $a \in G$.

DÉMONSTRATION. (i) En appliquant $f(e_G)^{-1}$ aux deux côtés de l'équation $f(e_G) = f(e_G \star e_G) = f(e_G) \circ f(e_G)$ on obtient

$$e_H = f(e_G)^{-1} \circ f(e_G) = f(e_G)^{-1} \circ f(e_G) \circ f(e_G) = e_H \circ f(e_G) = f(e_G).$$

(ii) $f(a^{-1}) \circ f(a) = f(a^{-1} \star a) = f(e_G) = f(a \star a^{-1}) = f(a) \circ f(a^{-1})$. ■

On dit que les groupes G et H sont isomorphes s'il existe un isomorphisme de G dans H.

2.2 Anneaux

Contrairement aux groupes, les anneaux comportent deux lois de composition. Ceci permet de décrire des interactions entre les deux lois de composition. La distributivité du produit matriciel par rapport à l'addition matricielle (voir le lemme 1.19) est un bon exemple.

Définition 2.12 *Un **anneau** [ring] $(A,+,\cdot)$ est un ensemble muni de deux lois de composition $+$ et $\cdot$:*

$$\begin{array}{rccc} + : & A \times A & \to & A \\ & (a,b) & \mapsto & a+b \end{array} \qquad \begin{array}{rccc} \cdot : & A \times A & \to & A \\ & (a,b) & \mapsto & a \cdot b \end{array} \tag{2.2}$$

satisfaisant les axiomes suivants

(1) $a+b = b+a, \quad \forall a,b \in A.$ *(commutativité+)*

(2) $a+(b+c) = (a+b)+c, \quad \forall a,b,c \in A.$ *(associativité+)*

(3) il existe $0 \in A$ tel que $0+a = a$ pour tout $a \in A$. *(élément neutre+)*

(4) pour tout $a \in A$ il existe $-a \in K$ tel que $a+(-a) = 0$. *(inverse+)*

(5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a,b,c \in A.$ *(associativité·)*

(6) il existe $1 \in A$ tel que $1 \cdot a = a \cdot 1 = a$ pour tout $a \in A$. *(élément neutre·)*

(7) $(a+b) \cdot c = (a \cdot c) + (b \cdot c), \quad \forall a,b,c \in A.$ *(distributivité I)*

(8) $a \cdot (b+c) = (a \cdot b) + (a \cdot c), \quad \forall a,b,c \in A.$ *(distributivité II)*

En d'autres termes, $(A,+)$ est un groupe commutatif par (1)–(4) et $(A,\cdot)$ est un monoïde par (5)–(6). Cachée dans (2.2), la stabilité des lois de composition est une propriété essentielle d'un anneau.

Remarque 2.13 *On dit parfois de l'anneau ci-dessous que c'est un* ***anneau unitaire****. On peut aussi définir des anneaux sans l'identité* 1*, l'élément neutre de* $\cdot$.

Définition 2.14 *Un anneau* $(A,+,\cdot)$ *dans lequel la loi* $\cdot$ *est commutative est appelé* ***anneau commutatif*** *[commutative ring].*

Exemples:

- $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, où $+$ et $\cdot$ sont les opérations usuelles, sont des anneaux commutatifs.
- Soit $n\mathbb{Z}=\{nz : z\in\mathbb{Z}\}$ pour $n\in\mathbb{N}$, $n\geq 1$. Alors, $(n\mathbb{Z},+,\cdot)$ n'est pas un anneau pour $n>2$, car il n'existe pas de 1.
- Soit K un anneau commutatif. Alors $(M_{n\times n}(K),+,\cdot)$ avec l'addition matricielle $+$ et le produit matriciel $\cdot$ est un anneau (non-commutatif). (Exercices)
  D'autre part $(GL_n(K),+,\cdot)$ n'est pas un anneau. Par exemple, il n'existe pas de 0 dans $GL_n(K)$.
- On définit sur $\mathbb{R}\cup\{\infty\}$ les opérations

$$a\oplus b=\min\{a,b\},\quad a\odot b=a+b.$$

  $\big(\mathbb{R}\cup\{\infty\},\oplus,\odot\big\}$ n'est pas un anneau. (Exercises: Quels axiomes ne sont pas satisfaits?)
- Soit E un ensemble non vide et $(A,+,\cdot)$ un anneau. On définit

$$\mathsf{App}(E,A):=\big\{f\,|\,f \text{ est une application de } E \text{ vers } A\big\}$$

  et les opérations

$$(f+g)(x):=f(x)+g(x),\qquad (f\cdot g)(x):=f(x)g(x).$$

  Alors, $(\mathsf{App}(E,A),+,\cdot)$ est un anneau (non commutatif).
- Soit $(A,+,\cdot)$ un anneau. Un **polynôme** à coefficients dans A est une expression formelle

$$p=a_0\cdot t^0+a_1\cdot t^1+a_2\cdot t^2+\cdots+a_n\cdot t^n,\quad a_0,a_1,\ldots,a_n\in A. \tag{2.3}$$

  On écrit souvent $a_0\cdot t^0=a_0$ et $a_1\cdot t^1=a_1\cdot t$. Le **degré d'un polynôme** $\deg(p)$ est le plus grand entier j tel que $a_j\neq 0$. Si tous les coefficients a_i sont nuls on définit le degré par $-\infty$. On note l'ensemble des polynômes à coefficients dans A par $A[t]$.
  Attention ! Il es important de noter qu'à ce stade, l'expression (2.3) est formelle, t occupe la place d'un objet indéfini. De même, la puissance t^j ainsi que le signe $+$ sont formels.
  Soient $p,q\in A[t]$,

$$p=a_0+a_1\cdot t+\cdots+a_m\cdot t^m,\quad q=b_0+b_1\cdot t+\cdots+b_n\cdot t^n.$$

  On définit les opérations

$$\begin{aligned} p+q&:=(a_0+b_0)+(a_1+b_1)\cdot t+\cdots+(a_{\max\{m,n\}}+b_{\max\{m,n\}})\cdot t^{\max\{m,n\}}\\ p\cdot q&:=c_0+c_1\cdot t+\cdots+c_{m+n}\cdot t^{m+n},\qquad c_k:=\sum_{i+j=k}a_ib_j. \end{aligned}$$

Lemme 2.15 *L'ensemble* $A[t]$ *avec les opérations* $+$ *et* $\cdot$ *comme définies ci-dessus est un anneau. Si* A *est un anneau commutatif, alors* $A[t]$ *est aussi un anneau commutatif.*

DÉMONSTRATION. Exercices. ■

Lemme 2.16 *Soit $(A,+,\cdot)$ un anneau. Alors,*

(i) $0\cdot a = a\cdot 0 = 0$ *pour tout* $a \in A$,

(ii) $(-a)b = a(-b) = -(ab)$ *pour tous* $a,b \in A$,

(iii) $(-a)(-b) = ab$ *pour tous* $a,b \in A$.

DÉMONSTRATION.

(i) Par l'axiome de distributivité I,

$$0\cdot a = 0\cdot a + 0 = 0\cdot a + 0\cdot a + (-(0\cdot a)) = (0+0)\cdot a + (-(0\cdot a)) = 0\cdot a + (-(0\cdot a)) = 0.$$

De même on montre que $a\cdot 0 = 0$.

(ii) Par les axiomes de distributivité I+II et la partie (i),

$$ab + (-a)b = (a+(-a))b = 0\cdot b = 0$$

et

$$ab + a(-b) = a(b+(-b)) = a\cdot 0 = 0.$$

(iii) $(-a)(-b) = -(a(-b) = -(-(ab)) = ab$.

■

Le lemme 2.16 permet d'écrire $-ab$ sans ambiguité.

Définition 2.17 *Soient $(A,+,\cdot)$ et $(B,\oplus,\odot)$ deux anneaux. Un* ***morphisme d'anneaux*** *[ring homomorphism] est une application $f : A \to B$ telle que*

$$f(a+b) = f(a)\oplus f(b), \qquad f(a\cdot b) = f(a)\odot f(b), \qquad \forall a,b \in A,$$

et

$$f(1_A) = 1_B.$$

Si de plus f est bijective, on dit que f est un ***isomorphisme d'anneaux*** *et que les anneaux $(A,+,\cdot)$ et $(B,\oplus,\odot)$ sont isomorphes. On note $(A,+,\cdot) \cong (B,\oplus,\odot)$.*

Définition 2.18 *Soit $(A,+,\cdot)$ un anneau et $U \subseteq A$. On dit que $(U,+,\cdot)$ est un* ***sous-anneau*** *[subring] de A si*

(i) $(U,+)$ *est un sous-groupe de* $(A,+)$,

(ii) si $a,b \in U$ *alors* $a\cdot b \in U$,

(iii) L'élément neutre multiplicatif (1) *de A appartient à U.*

Par exemple, $(M_2,+,\cdot)$ (la définition de M_2 trouvée sur la page 24) est un sous-anneau de $(M_{2\times 2}(\mathbb{R}),+,\cdot)$.

Lemme 2.19 *$(A,+,\cdot)$ un anneau et $U \subseteq A$. Alors, les assertions suivantes sont équivalentes:*

(i) $(U,+,\cdot)$ *est un sous-anneau de* $(A,+,\cdot)$

(ii) $1 \in U$ *et pour tout* $a,b \in U$, *on a* $a-b \in U$ *et* $a\cdot b \in U$.

DÉMONSTRATION. (i) $\Rightarrow$ (ii) découle de la définition d'un sous-anneau.

(ii) $\Rightarrow$ (i) Comme $1 \in U$, U est non vide et comme $1-1=0$, on a que $0 \in U$. Si $b \in U$ alors $-b = 0-b \in U$. Si $a,b \in U$ alors $a+b = a-(-b) \in U$. Donc $(U,+)$ est un sous-groupe de $(A,+)$. Si $a,b \in U$ alors $a\cdot b \in U$ d'après (ii) et donc $(U,+,\cdot)$ est bien un sous-anneau de $(A,+,\cdot)$. ■

2.3 Matrices à coefficients dans un anneau

On peut généraliser la définition d'une matrice en permettant des coefficients dans un anneau.

Théorème 2.20 *Soit $(A,+,\cdot)$ un anneau. Alors, $M_{n\times n}(A)$ est un anneau.*

DÉMONSTRATION. Les axiomes (1), (2), (5), (7), (8) d'anneau découlent des généralisations du lemme 1.12 et du lemme 1.19. Soient 0_A et 1_A les éléments neutres de A par rapport à $+$ et $\cdot$, respectivement. Alors la matrice nulle $0_{n\times n}$ et la matrice identité I_n, définies par

$$0_{n\times n} = \begin{pmatrix} 0_A & \cdots & 0_A \\ \vdots & & \vdots \\ 0_A & \cdots & 0_A \end{pmatrix}, \quad I_n = \mathrm{diag}\,(1_A, 1_A, \ldots, 1_A),$$

sont les éléments neutres de $M_{n\times n}(A)$. ∎

Exemples:

- Les coefficients de $P \in M_{n\times n}(A[t])$ sont des polynômes. Par exemple,

$$P(t) = \begin{pmatrix} t^2+2 & t+1 \\ 3t+1 & 4t^2+t+2 \end{pmatrix} \in M_{2\times 2}(A[t])$$

  On peut également écrire

$$P(t) = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} t^2 + \begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix} t + \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

  et regarder $P(t)$ comme un élément de $\big(M_{2\times 2}(A)\big)[t]$.
  En général, soit $(A,+,\cdot)$ un anneau et $n \geq 1$. Alors l'anneau $M_{n\times n}(A[t])$, muni de l'addition/multiplication matricielle, et l'anneau $\big(M_{n\times n}(A)\big)[t]$, muni de l'addition/multiplication polynomiale, sont isomorphes. (Démonstration: Voir les exercises.)
- Les coefficients de $B \in M_{m\times n}(\mathbb{Z})$ sont des nombres entiers. Par exemple,

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}).$$

  On remarque que A est inversible vu comme un élément de $M_{2\times 2}(\mathbb{R})$:

$$A^{-1} = \frac{1}{2}\begin{pmatrix} -4 & 2 \\ 3 & -1 \end{pmatrix} \in M_{2\times 2}(\mathbb{R}).$$

  Au contraire, A est singulaire comme un élément de $M_{2\times 2}(\mathbb{Z})$. L'existence d'une matrice $X \in M_{2\times 2}(\mathbb{Z})$ avec $AX = XA = I_n$ contrarie l'unicité d'inverse dans $M_{2\times 2}(\mathbb{R})$.
- $M_{m\times m}(M_{n\times n}(A))$ est un exemple des matrices à coefficients dans un anneau non-commutatif. $M_{n\times n}(M_{n\times n}(A))$ et $M_{mn\times mn}(A)$ sont isomorphes (multiplication de matrices par blocs).

Après ce chapitre, nous ne traiterons pas des matrices à coefficients dans un anneau non-commutatif (sauf dans la démonstration du théorème de Cayley-Hamilton au chapitre 7). Quelques concepts avancés (rang, déterminant, ...) n'ont pas des définitions raisonables si A est non-commutatif.

2.4 Corps

Un corps (commutatif) est un anneau commutatif dans lequel $0 \neq 1$ et tout élément non nul est inversible (par rapport à $\cdot$).

Définition 2.21 *Un* **corps** *[field]* $(K,+,\cdot)$ *est un anneau commutatif tel que:*

(i) $K \neq \{0\}$

(ii) pour tuot $a \in K \setminus \{0\}$ *il existe* $a^{-1} \in K$ *tel que* $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

On remarque que $(K,+,\cdot)$ est un corps si et seulement si $(K,+)$ et $(K \setminus \{0\},\cdot)$ sont des groupes abéliens et $(a+b)\cdot c = a\cdot c + b\cdot c$ pour tous $a,b,c \in K$.

Une liste de tous les axiomes d'un corps $(K,+,\cdot)$:

$a+b \in K, \quad a\cdot b \in K \quad \forall a,b \in K.$	(stabilité)
$a+b = b+a, \quad \forall a,b \in K.$	(commutativité+)
$a+(b+c) = (a+b)+c, \quad \forall a,b,c \in K.$	(associativité+)
il existe $0 \in K$ tel que $0+a = a$ pour tout $a \in K$.	(élément neutre+)
pour tout $a \in K$ il existe $-a \in K$ tel que $a+(-a) = 0$.	(inverse+)
$a\cdot b = b\cdot a, \quad \forall a,b \in K.$	(commutativité$\cdot$)
$a\cdot(b\cdot c) = (a\cdot b)\cdot c, \quad \forall a,b,c \in K.$	(associativité$\cdot$)
il existe $1 \in K$ tel que $1\cdot a = a\cdot 1 = a$ pour tout $a \in K$.	(élément neutre$\cdot$)
pour tout $a \in K \setminus \{0\}$ il existe $a^{-1} \in K$ tel que $a\cdot a^{-1} = 1$.	(inverse$\cdot$)
$(a+b)\cdot c = (a\cdot c)+(b\cdot c), \quad \forall a,b,c \in K.$	(distributivité I)
$a\cdot(b+c) = (a\cdot b)+(a\cdot c), \quad \forall a,b,c \in K.$	(distributivité II)

En fait, le commutativité de $\cdot$ implique que les deux lois de distributivité I et II sont équivalentes.

Exemples :

- $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, où $+$ et $\cdot$ sont les opérations usuelles, sont des corps.
- $(\mathbb{Z},+,\cdot)$ n'est pas un corps parce qu'il n'y a pas d'inverse multiplicatif en general.
- L'ensemble M_2 de la page 24 muni de la somme et le produit matriciel est un corps (exercices).

Dans les deux sections suivantes on va voir deux autres exemples de corps.

Un morphisme (isomorphisme) de corps est simplement un morphisme (isomorphisme) d'anneaux sous-jacents.

2.5 Le corps des nombres complexes

Un **nombre complexe** est une paire ordonnée (couple) (x,y) où $x,y \in \mathbb{R}$. En définissant l'**unité imaginaire** *[imaginary unit]* i on écrit

$$x + \mathrm{i}y$$

au lieu de (x,y). L'ensemble des nombres complexes se note

$$\mathbb{C} = \{x+\mathrm{i}y : \ x,y \in \mathbb{R}\}.$$

Quelques conventions : Soit $z = x+\mathrm{i}y \in \mathbb{C}$.

- On note $x = \mathsf{Re}(z)$ et on dit que x est la **partie réelle** *[real part]* de z.
- On note $y = \mathsf{Im}(z)$ et on dit que y est la **partie imaginaire** *[imaginary part]* de z.
- Si $y = 0$ il est usuel d'identifier le nombre complexe z avec le nombre réel x. Cela justifie l'inclusion $\mathbb{R} \subset \mathbb{C}$.

– Si $x = 0$ on dit que z est **imaginaire pur** ou **totalement imaginaire** [*purely imaginary*].

On définit une loi $+$ (addition des nombres complexes) et une loi $\cdot$ (multiplication des nombres complexes) sur $\mathbb{C}$:

$$\begin{aligned} +: &\quad \mathbb{C}\times\mathbb{C}\to\mathbb{C}, \quad (x_1+y_1\mathrm{i})+(x_2+y_2\mathrm{i}) := (x_1+x_2)+(y_1+y_2)\mathrm{i}, \\ \cdot: &\quad \mathbb{C}\times\mathbb{C}\to\mathbb{C}, \quad (x_1+y_1\mathrm{i})\cdot(x_2+y_2\mathrm{i}) := (x_1x_2-y_1y_2)+(x_1y_2+y_1x_2)\mathrm{i}. \end{aligned}$$

On constate que $\mathrm{i}^2 = \mathrm{i}\cdot\mathrm{i} = -1$. En effet, cela suffit pour retrouver la loi de multiplication :

$$\begin{aligned} (x_1+\mathrm{i}y_1)\cdot(x_2+\mathrm{i}y_2) &= x_1x_2+\mathrm{i}y_1x_2+\mathrm{i}x_1y_2+\mathrm{i}^2y_1y_2 \\ &= x_1x_2+\mathrm{i}y_1x_2+\mathrm{i}x_1y_2-y_1y_2 \\ &= (x_1x_2-y_1y_2)+\mathrm{i}(x_1y_2+y_1x_2). \end{aligned}$$

Exemple 2.22

On a

$$(1+\mathrm{i})+(-2+\mathrm{i}) = -1+2\mathrm{i}$$

et

$$(1+\mathrm{i})(-2+\mathrm{i}) = -3-\mathrm{i}.$$

MATLAB

Sous MATLAB l'unité imaginaire est `i` (ou `j`). Mais il est recommandé d'utiliser `1i` au lieu de `i`, qui peut être une autre variable.

```
>> (1+1i) + (-2+1i),
ans =
  -1.0000 + 2.0000i
>> (1+1i) * (-2+1i),
ans =
  -3.0000 - 1.0000i
```

Héritant des propriétés de $(\mathbb{R},+)$, $(\mathbb{C},+)$ est un groupe abélien. L'élément neutre est $0 = 0+0\mathrm{i}$ et l'inverse additif de $z = x+\mathrm{i}y \in \mathbb{C}$ est $-z := -x-\mathrm{i}y$. On définit la soustraction des nombres complexes par

$$z_1 - z_2 := z_1 + (-z_2) = (x_1-x_2)+\mathrm{i}(y_1-y_2).$$

C'est laborieux de vérifier directement les propriétés de la multiplication. Au lieu de cela, on utilise un morphisme de corps. À cette fin, soit

$$\varphi : \mathbb{C}\to M_2, \quad \varphi : x+\mathrm{i}y \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}. \tag{2.4}$$

Voir la page 24 pour la définition de M_2. Évidemment, φ est bijective et, ainsi, φ est un isomorphisme du groupe $(\mathbb{C},+)$ dans $(M_2,+)$. En outre,

$$\begin{aligned} \varphi(x_1+\mathrm{i}y_1)\varphi(x_2+\mathrm{i}y_2) &= \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1x_2-y_1y_2 & x_1y_2+y_1x_2 \\ -y_1x_2-x_1y_2 & -y_1y_2+x_1x_2 \end{pmatrix} = \varphi\big((x_1+y_1\mathrm{i})(x_2+y_2\mathrm{i})\big). \end{aligned}$$

Comme $(M_2\setminus\{0_{2\times2}\},\cdot)$ est un groupe, $(\mathbb{C}\setminus\{0\},\cdot)$ est un groupe. L'élément neutre est $1 = \varphi^{-1}(I_2) = 1+0\mathrm{i}$. On obtient l'inverse multiplicatif dans $(\mathbb{C}\setminus\{0\},\cdot)$ par l'inverse matriciel :

$$\begin{aligned} z^{-1} = \varphi^{-1}(\varphi(z)^{-1}) &= \varphi^{-1}\left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}^{-1}\right) \\ &= \varphi^{-1}\left(\frac{1}{x^2+y^2}\begin{pmatrix} x & -y \\ y & x \end{pmatrix}\right) = \frac{x}{x^2+y^2} - \mathrm{i}\frac{y}{x^2+y^2}. \end{aligned}$$

En utilisant l'isomorphisme φ, $(\mathbb{C},+,\cdot)$ hérite des lois de distributivité de $(M_2,+,\cdot)$. En outre, la multiplication matricielle est commutative dans M_2 et, ainsi, la multiplication complexe est commutative. En résumé, on a montré le résultat suivant.

Théorème 2.23 *L'ensemble $\mathbb{C}$ muni des opérations $+$ et $\cdot$ définies ci-dessus est un corps.*

Définition 2.24 *Le conjugué d'un nombre complexe $z = x+\mathrm{i}y$ est le nombre complexe $\overline{z}$ défini par $\overline{z} := x-\mathrm{i}y$.*

Le conjugué d'un nombre complexe correspond à la transposée d'une matrice :

$$\varphi(\overline{z}) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}^{\mathsf{T}} = \varphi(z)^{\mathsf{T}}. \tag{2.5}$$

Lemme 2.25 *Soient $z_1,z_2,z \in \mathbb{C}$. Alors,*

(i) $\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$
(ii) $\overline{z_1\cdot z_2} = \overline{z_1}\cdot\overline{z_2}$
(iii) $\overline{\overline{z}} = z$
(iv) $\mathsf{Re}(z) = \frac{1}{2}(z+\overline{z})$
(v) $\mathsf{Im}(z) = \frac{1}{2\mathrm{i}}(z-\overline{z})$.

DÉMONSTRATION. Ces propriétés sont des exercices faciles. En effet, (i)–(iii) découlent des propriétés de la transposée (voir le lemme 1.26). Par exemple

$$\varphi(\overline{z_1\cdot z_2}) = \varphi(z_1z_2)^{\mathsf{T}} = \varphi(z_2)^{\mathsf{T}}\varphi(z_1)^{\mathsf{T}} = \varphi(z_1)^{\mathsf{T}}\varphi(z_2)^{\mathsf{T}} = \varphi(\overline{z_1})\varphi(\overline{z_2}) = \varphi(\overline{z_1}\cdot\overline{z_2}),$$

ce qui montre (ii). ∎

Les parties (i)–(iii) du lemme 2.25 impliquent que la conjugaison est un isomorphisme du corps $(\mathbb{C},+,\cdot)$ dans lui-même.[2]

Définition 2.26 *Le **module** [absolute value, modulus, magnitude] d'un nombre complexe $z = x+\mathrm{i}y$ est le nombre réel positif $|z|$ défini par $|z| := \sqrt{x^2+y^2}$.*

Lemme 2.27 *Soient $z_1,z_2,z \in \mathbb{C}$. Alors,*

(i) $z\overline{z} = |z|^2$
(ii) $z^{-1} = \frac{\overline{z}}{|z|^2}$ $\quad (z\neq 0)$
(iii) $\overline{z^{-1}} = \overline{z}^{-1}$ $\quad (z\neq 0)$
(iv) $|z_1\cdot z_2| = |z_1|\cdot|z_2|$
(v) $|z_1+z_2| \leq |z_1|+|z_2|$ *avec égalité si et seulement si il existe $\alpha \geq 0$ tel que $z_1 = \alpha z_2$ ou $z_2 = \alpha z_1$.*

DÉMONSTRATION. (i). $z\overline{z} = (x+\mathrm{i}y)(x-\mathrm{i}y) = x^2+y^2+\mathrm{i}(xy-yx) = x^2+y^2 = |z|^2$.
(ii) découle de (i) et (iii) découle de (ii).
(iv). En utilisant le lemme 2.25 et la commutativité de la multiplication complexe on obtient

$$|z_1\cdot z_2|^2 = z_1\cdot z_2\cdot\overline{z_1\cdot z_2} = z_1\cdot z_2\cdot\overline{z_1}\cdot\overline{z_2} = z_1\cdot\overline{z_1}\cdot z_2\cdot\overline{z_2} = |z_1|^2\cdot|z_2|^2.$$

(v). L'inégalité découle de

$$\begin{aligned} |z_1+z_2|^2 &= (z_1+z_2)\overline{(z_1+z_2)} = (z_1+z_2)(\overline{z_1}+\overline{z_2}) \\ &= |z_1|^2+z_2\overline{z_1}+z_1\overline{z_2}+|z_2|^2 = |z_1|^2+2\,\mathsf{Re}(z_1\overline{z_2})+|z_2|^2 \\ &\leq |z_1|^2+2\,|z_1||\overline{z_2}|+|z_2|^2 = |z_1|^2+2\,|z_1||z_2|+|z_2|^2 = (|z_1|+|z_2|)^2. \end{aligned}$$

2. Un isomorphisme d'une structure algébrique dans elle-même est dit **automorphisme**.

On a utilisé le fait que le module est toujours supérieur à la partie reélle. L'inégalité ci-dessus devient une égalité si $\mathrm{Re}(z_1\overline{z_2}) = |z_1\overline{z_2}|$ c-à-d si $\beta = z_1\overline{z_2}$ est reél positif. Si $z_2 = 0$ on a bien $z_2 = \alpha z_1$ avec $\alpha = 0$. Si $z_2 \neq 0$, alors

$$z_1\overline{z_2}z_2 = \beta z_2 \quad \Rightarrow \quad z_1 = \frac{\beta z_2}{|z_2|^2} = \alpha z_2 \text{ avec } \alpha = \frac{\beta}{|z_2|^2} \geq 0.$$

La réciproque est évidente. ■

La division d'un nombre complexe z_1 par un nombre complexe $z_2 \neq 0$ est définie par $z_1/z_2 := z_1 z_2^{-1}$. D'aprés le lemme 2.25 (ii), on a

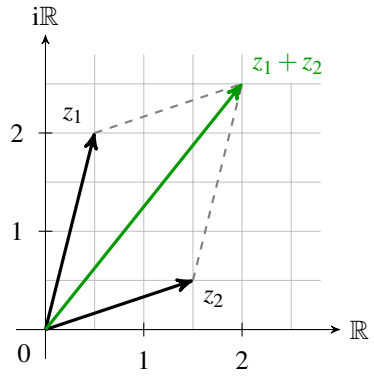
$$\frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{|z_2|^2}.$$

Par exemple,

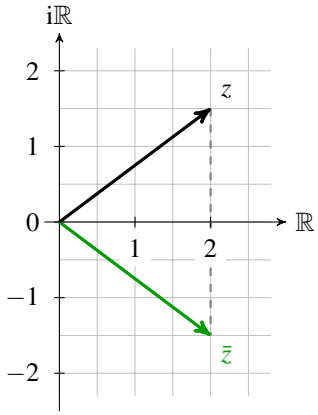
$$\frac{2+3\mathrm{i}}{1+\mathrm{i}} = \frac{(2+3\mathrm{i})(1-\mathrm{i})}{1+1} = \frac{5+\mathrm{i}}{2} = \frac{5}{2} + \frac{1}{2}\mathrm{i}.$$

2.5.1 Plan complexe et forme polaire

Par définition, les nombres complexes $\mathbb{C}$ sont des couples de nombres réels. Pour cette raison, tout nombre complexe correspond uniquement à un vecteur dans la plan (qui s'appele **plan complexe** [*complex plane*]). La somme des nombres complexes correspond à la somme des vecteurs et la conjugaison correspond à la réflexion par rapport à l'axe réel, voir figure 2.1.



l'addition des deux nombres complexes



le conjugué

FIG. 2.1 – L'addition et le conjugué dans la plan complexe.

Soit $z = x + \mathrm{i}y \in \mathbb{C} \setminus \{0\}$. En notant $r = \sqrt{x^2+y^2} > 0$ la longueur et $\theta = \arctan\frac{y}{x} \in]-\pi,\pi]$ l'angle du vecteur (x,y) dans la plan complexe, on peut écrire

$$(x,y) = (r\cos\theta, r\sin\theta).$$

Ainsi on a

$$z = x + \mathrm{i}y = r\cos\theta + \mathrm{i}r\sin\theta = r(\cos\theta + \mathrm{i}\sin\theta),$$

où θ est défini à $2k\pi$ près avec $k \in \mathbb{Z}$. On l'appelle la **forme polaire** [*polar form*] de z. $\theta = \arg$ est l'argument de z. La **fonction exponentielle complexe** [*complex exponential*] permet de faire une représentation plus compacte.

Définition 2.28 *Pour $z = x + \mathrm{i}y \in \mathbb{C}$ on définie*

$$e^z = \exp(z) := e^x(\cos y + \mathrm{i}\sin y) = e^{\mathsf{Re}z}(\cos(\mathsf{Im}z) + \mathrm{i}\sin(\mathsf{Im}z))$$

où e^x est la fonction exponentielle réelle usuelle.

Propriétés de l'exponentielle:

1. $|e^z| = e^x = e^{\mathsf{Re}z}$
2. $\arg(e^z) = \mathsf{Im}z$ (à $2k\pi$ près avec $k \in \mathbb{Z}$)
3. si $\mathsf{Im}z = 0$ on a $e^z = e^{\mathsf{Re}z}$
4. $e^{z+2k\pi\mathrm{i}} = e^x\big(\cos(y+2k\pi) + \mathrm{i}\sin(y+2k\pi)\big)$ pour tout $k \in \mathbb{Z}$
5. $e^{w+z} = e^w \cdot e^z$ pour tous $w,z \in \mathbb{C}$

La **formule d'Euler** s'écrit, pour $\theta \in \mathbb{R}$,

$$e^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta.$$

En particulier pour $\theta = \pi$ on obtient **l'identité d'Euler** (« l'étalon-or de la beauté mathématique »)

$$e^{\mathrm{i}\pi} + 1 = 0.$$

Par les identités trigonométriques, la forme polaire permet de multiplier facilement deux nombres complexes :

$$\begin{aligned} z_1 z_2 &= \rho_1(\cos\varphi_1 + \mathrm{i}\sin\varphi_1)\cdot\rho_2(\cos\varphi_2 + \mathrm{i}\sin\varphi_2) \\ &= \rho_1\rho_2\big(\cos(\varphi_1+\varphi_2) + \mathrm{i}\sin(\varphi_1+\varphi_2)\big). \end{aligned} \tag{2.6}$$

Alors, le produit $z_1 z_2$ représente géométriquement une multiplication de la longueur de z_1 par ρ_2 et une rotation anti-horaire de z_1 d'angle φ_2.

Lemme 2.29 (Formule de Moivre) *Pour tous $r > 0$, $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$ on a*

$$\big(r(\cos\theta + \mathrm{i}\sin\theta)\big)^n = r^n\big(\cos(n\theta) + \mathrm{i}\sin(n\theta)\big).$$

DÉMONSTRATION. Par récurrence utilisant (2.6). Voir exercices. ■

2.5.2 Matrices à coefficients complexes

Dans cette section, on considère $M_{m\times n}(\mathbb{C})$, l'ensemble des matrices $m \times n$ complexes. Le conjuguée d'une matrice $A \in M_{m\times n}(\mathbb{C})$ est la matrice (notée $\overline{A}$) formée des éléments de A conjugués :

$$\overline{A} \in M_{m\times n}(\mathbb{C}) \quad \text{avec} \quad (\overline{A})_{ij} := \overline{a_{ij}}, \quad i = 1,\dots,m,\ j = 1,\dots,n.$$

Exemple 2.30 Soient

$$A = \begin{pmatrix} 1+2\mathrm{i} & 1-\mathrm{i} \\ 3 & -\mathrm{i} \\ 2-\mathrm{i} & 2+\mathrm{i} \end{pmatrix},$$

$$B = \begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ -1-\mathrm{i} & 1+\mathrm{i} \end{pmatrix}.$$

Alors,

$$\overline{A} = \begin{pmatrix} 1-2\mathrm{i} & 1+\mathrm{i} \\ 3 & \mathrm{i} \\ 2+\mathrm{i} & 2-\mathrm{i} \end{pmatrix},$$

$$AB = \begin{pmatrix} -3+3\mathrm{i} & 5+\mathrm{i} \\ 2+4\mathrm{i} & 4-4\mathrm{i} \\ 2-2\mathrm{i} & 2 \end{pmatrix}.$$

MATLAB

```
>> A = [1+2i 1-1i;
        3     -1i;
        2-1i 2+1i];
>> B = [1+1i 1-1i;
       -1-1i 1+1i];
>> conj(A),
ans =
   1 - 2i   1 + 1i
   3 - 0i  -0 + 1i
   2 + 1i   2 - 1i
>> A*B,
ans =
  -3 + 3i   5 + 1i
   2 + 4i   4 - 4i
   2 - 2i   2 + 0i
```

Définition 2.31 *La* ***matrice adjointe*** A^* *(aussi appelée* ***matrice transposée conjuguée*** *[conjugate transpose, Hermitian transpose]) d'une matrice* $A \in M_{m\times n}(\mathbb{C})$ *est la matrice transposée de la matrice conjuguée de* A *:*

$$A^* \in M_{n\times m}(\mathbb{C}) \quad avec \quad (\overline{A})_{ij} := \overline{a_{ji}}, \quad i = 1,\ldots,n,\ j = 1,\ldots,m.$$

Dans le cas particulier où les coefficients de A sont réels, on a $A^* = A^T$.

Exemple 2.32

Soit A comme dans l'exemple 2.30. Alors,

$$A^* = \begin{pmatrix} 1-2\mathrm{i} & 3 & 2+\mathrm{i} \\ 1+\mathrm{i} & \mathrm{i} & 2-\mathrm{i} \end{pmatrix},$$

$$A^{\mathsf{T}} = \begin{pmatrix} 1+2\mathrm{i} & 3 & 2-\mathrm{i} \\ 1-\mathrm{i} & -\mathrm{i} & 2+\mathrm{i} \end{pmatrix}.$$

MATLAB

Étant donné une matrice à coefficients complexes, `A'` retourne la matrice adjointe et `A.'` retourne la matrice transposée.

```
>> A'
ans =
   1 - 2i   3 - 0i   2 + 1i
   1 + 1i  -0 + 1i   2 - 1i
>> A.'
ans =
   1 + 2i   3 + 0i   2 - 1i
   1 - 1i  -0 - 1i   2 + 1i
```

D'après la définition 2.31, on a

$$A^* = (\overline{A})^{\mathsf{T}} = \overline{A^{\mathsf{T}}}. \tag{2.7}$$

Lemme 2.33 *(i)*

$$\boxed{(A^*)^* = A} \qquad \forall A \in M_{m\times n}(\mathbb{C}).$$

(ii)

$$\boxed{(\alpha A)^* = \overline{\alpha} A^*} \qquad \forall A \in M_{m\times n}(\mathbb{C}), \alpha \in \mathbb{C}.$$

(iii)

$$\boxed{(A+B)^* = A^* + B^*} \qquad \forall A,B \in M_{m\times n}(\mathbb{C})$$

(iv)

$$\boxed{(AB)^* = B^* A^*} \qquad \forall A \in M_{m\times n}(\mathbb{C}), B \in M_{n\times p}(\mathbb{C}).$$

DÉMONSTRATION. Exercices. Indication: utiliser le lemme 1.26 et (2.7). ■

Définition 2.34 *On dit qu'une matrice* $A \in M_{n\times n}(\mathbb{C})$ *est* ***hermitienne*** *[Hermitian matrix] si*

$$A^* = A \quad c\text{-}\grave{a}\text{-}d \quad a_{ij} = \overline{a_{ji}} \quad \forall i,j = 1,\ldots,n.$$

Par exemple,

$$A = \begin{pmatrix} 1 & 2+3\mathrm{i} & 4+5\mathrm{i} \\ 2-3\mathrm{i} & 6 & 7+8\mathrm{i} \\ 4-5\mathrm{i} & 7-8\mathrm{i} & 9 \end{pmatrix}, \quad B = \begin{pmatrix} 1+\mathrm{i} & 2+3\mathrm{i} & 4+5\mathrm{i} \\ 2+3\mathrm{i} & 6+2\mathrm{i} & 7+8\mathrm{i} \\ 4+5\mathrm{i} & 7+8\mathrm{i} & 9-3\mathrm{i} \end{pmatrix}.$$

La matrice A est hermitienne. La matrice B au contraire est une matrice (complexe) symétrique mais elle n'est pas hermitienne. Les éléments diagonaux d'une matrice hermitienne sont réels.

2.6 Corps finis

En Géométrie vous avez déjà vu $\mathbb{Z}/p\mathbb{Z}$ pour un nombre entier p. Dans cette section nous rappelons cette structure algébrique.

Soit $p \geq 2$ un nombre entier et $\mathbb{N}_{<p} = \{0,1,2,\ldots,p-1\}$. On définit deux lois de compositions $\oplus$ et $\odot$ sur $\mathbb{N}_{<p}$ par

$$a \oplus b = \text{reste dans la division euclidienne de } a+b \text{ par } p,$$
$$a \odot b = \text{reste dans la division euclidienne de } a \cdot b \text{ par } p.$$

Héritant de la structure de $\mathbb{Z}$, $(\mathbb{N}_{<p},\oplus)$ et $(\mathbb{N}_{<p},\odot)$ sont des monoïdes.

Exemple 2.35 Les tables de Cayley pour $p = 2,3,4$:

$\mathbb{N}_{<2}$:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

$\mathbb{N}_{<3}$:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{N}_{<4}$:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

La commutativité des $\oplus$ et $\odot$ signifie que les tables ci-dessus sont symétriques. L'inversibilité d'un élément signifie que la ligne (ou la colonne) correspondante contient 1. En effet, par la « règle Sudoku », un monoïde fini est un groupe si et seulement si toute ligne et toute colonne contient une fois et une fois seulement chaque élément du monoïde. Alors, $(\mathbb{N}_{<2},\oplus)$, $(\mathbb{N}_{<2}\setminus\{0\},\odot)$, $(\mathbb{N}_{<3},\oplus)$, $(\mathbb{N}_{<3}\setminus\{0\},\odot)$, $(\mathbb{N}_{<4},\oplus)$ sont des groupes (abéliens). Au contraire, $(\mathbb{N}_{<4}\setminus\{0\},\odot)$ n'est pas un groupe, par exemple l'élément 2 n'est pas inversible. ♦

Lemme 2.36 *$a \in \mathbb{N}_{<p}$ tel que $a \neq 0$ est inversible (par rapport à $\cdot$) si et seulement si a et p sont premiers entre eux.*

DÉMONSTRATION. L'inversibilité de a dit qu'il existe $1 \leq b \leq p-1$, $q \in \mathbb{Z}$ tels que

$$ab + pq = 1. \tag{2.8}$$

Le plus grand diviseur commun (PGCD) de a,p divise $ab+pq$. Par (2.8), le PGCD doit être 1, c-à-d a et p sont premiers entre eux.

Réciproquement, on suppose que le PGCD de a,p soit 1. Alors, la division euclidienne permet de trouver $1 \leq b \leq p-1$, $q \in \mathbb{Z}$ satisfaisant (2.8). ■

Théorème 2.37 *Soit $p \geq 2$ un nombre entier. Alors :*

(i) $(\mathbb{N}_{<p},\oplus)$ *est un groupe abélien.*

(ii) $(\mathbb{N}_{<p},\odot)$ *est un monoïde commutatif.*

(iii) $(\mathbb{N}_{<p}\setminus\{0\},\odot)$ *est un groupe abélien si et seulement si p est un nombre premier.*

(iv) $(\mathbb{N}_{<p},\oplus,\odot)$ *est un anneau commutatif.*

(v) $(\mathbb{N}_{<p},\oplus,\odot)$ *est un corps si et seulement si p est un nombre premier.*

DÉMONSTRATION. Les parties (i) et (ii) sont des exercices.

Pour la partie (iii) il reste à montrer que tout élément de $\mathbb{N}_{<p} \setminus \{0\}$ est inversible si et seulement si p est un nombre premier. On suppose que p est un nombre premier. Alors, tous les nombres entre 1 et $p-1$ sont premiers avec p. Par le lemme 2.36, ils sont inversibles et, ainsi, le monoïde $\mathbb{N}_{<p} \setminus \{0\}$ devient un groupe. Réciproquement, on suppose que p est divisible par un nombre q avec $2 \leq q \leq p-1$. Par le lemme 2.36, q n'est pas inversible et, ainsi, $\mathbb{N}_{<p} \setminus \{0\}$ n'est pas un groupe.

La partie (iv) est un excercice. La partie (v) découle des parties (iii) et (iv). ■

Si p est premier on écrit souvent $\mathbb{F}_p$ en lieu de $(\mathbb{N}_{<p}, \oplus, \odot)$.

Le produit matriciel $C = AB$ de deux matrices $A \in M_{m\times n}(\mathbb{F}_p)$, $B \in M_{n\times p}(\mathbb{F}_p)$ est défini comme d'habitude. Pour calculer à la main ou sur un ordinateur, il peut être plus pratique de faire d'abord les additions et les multiplications usuelles; puis de faire la division euclidienne par p.

Exemple 2.38

Soient $A \in \mathbb{F}_5^{3\times 2}$, $B \in \mathbb{F}_5^{2\times 2}$ définies par

$$A = \begin{pmatrix} 2 & 3 \\ 4 & 1 \\ 2 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}.$$

Alors,

$$C = AB = \begin{pmatrix} 0 & 1 \\ 0 & 2 \\ 1 & 4 \end{pmatrix}.$$

MATLAB

MATLAB n'a pas de fonctions pour matrices à coefficients dans un corps finis. Malgré cela, le produit matriciel est facile à realiser :

```
>> A = [ 2 3; 4 1; 2 4];
>> B = [ 1 1; 1 3 ];
>> mod( A*B, 5 ),
ans =
   0   1
   0   2
   1   4
```

2.7 Polynômes à coefficients dans un corps

Si K est un corps en particulier $(K, +, \cdot)$ est un anneau commutatif et on sait d'après le lemme 2.15 que l'ensemble des polynômes à coefficients dans $K[t]$ muni de l'addition et de la multiplication des polynômes est un anneau commutatif.

Définition 2.39 *Soit K un corps, sous-anneau d'un anneau A. Soit $p \in K[t]$ avec $p(t) = a_0 + a_1 t + \cdots + a_n t^n$. **L'évaluation de p** en $s \in A$ notée $p(s)$ est*

$$a_0 + a_1 \cdot s + \cdots + a_n \cdot s^n, \quad \text{où} \quad s^j := \underbrace{s \cdot s \cdots s}_{j \text{ fois}}.$$

Exemple 2.40

Soit $K = \mathbb{R}$, $A = \mathbb{C}$, $p(t) = t^2 + 1 \in \mathbb{R}[t]$.

$$\begin{aligned} p(\mathrm{i}) &= \mathrm{i}^2 + 1 = -1 + 1 = 0 \\ p(\mathrm{i}+1) &= (\mathrm{i}+1)^2 + 1 \\ &= \mathrm{i}^2 + 2\mathrm{i} + 1 + 1 = 2\mathrm{i} + 1 \end{aligned}$$

MATLAB

Sous MATLAB un polynôme $a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + a_n t^n$ est representé par le vecteur $(a_n, a_{n-1}, \ldots, a_1, a_0)$. La commande polyval permet d'évaluer un polynôme :

```
>> polyval([1 0 1],1i)
ans =
     0
>> polyval([1 0 1],1i+1)
ans =
   1.0000 + 2.0000i
```

Théorème 2.41 (division euclidienne des polynômes) *Soient $p, q \in K[t]$ avec $q \neq 0$. Alors, il existe un unique couple de polynômes $g, r \in K[t]$ tels que*

$$p = gq + r \qquad \text{avec} \qquad \deg r < \deg q.$$

DÉMONSTRATION. **Existence.** Par récurrence sur $n = \deg p$. Si $n < \deg q$ alors $g = 0$ et $r = p$ conviennent. Supposons le résultat montré pour tout polynôme de degré strictement inférieur à n et $n \geq m := \deg q$. On pose

$$p(t) = a_0 + a_1 t + \cdots + a_n t^n, \qquad q(t) = b_0 + b_1 t + \cdots b_m t^m.$$

Posons $f(t) = p(t) - a_n/b_m \cdot t^{n-m} q(t)$, alors $\deg f < n$. Par hypothèse de récurrence, on a

$$f = g_1 q + r \qquad \text{avec} \qquad \deg r_1 < \deg q.$$

Alors

$$p(t) = g_1(t)q(t) + r + \frac{a_n}{b_m} \cdot t^{n-m} q(t) = \underbrace{\big(g_1(t) + \frac{a_n}{b_m} \cdot t^{n-m}\big)}_{=:g(t)} q(t) + r,$$

où g,r possèdent les propriétés demandées.

Unicité. Si $p = g_1 q + r_1 = g_2 q + r_2$ alors

$$(g_1 - g_2)q = r_2 - r_1 \qquad \text{avec} \qquad \deg(r_2 - r_1) < \deg q.$$

Si $g_1 - g_2 \neq 0$

$$\deg((g_1 - g_2)q) = \deg(g_1 - g_2) + \deg q \geq \deg q,$$

ce qui est absurde. Donc $g_1 = g_2$ et par suite $r_1 = r_2$. ■

Définition 2.42 *Un élément $c \in K$ s'appelle une* ***racine*** *[root, zero] de $p \in K[t]$ si $p(c) = 0$.*

Corollaire 2.43 *Soit $p \in K[t]$ et $c \in K$. Alors c est une racine de p si et seulement si $t - c$ divise p (sans reste), c-à-d $p(t) = g(t)(t - c)$ pour un certain $g \in K[t]$.*

DÉMONSTRATION. L'assertion découle du théorème 2.41 en posant $q(t) = t - c$. ■

Vocabulaire: Soient p,$q \in K[t]$ avec $q \neq 0$. On dit que

- q **divise** p, q est un **diviseur** de p
- p est **divisible** par q
- p est un **multiple** de q

si le reste de la division de p par q est nul.

Définition 2.44 *Un polynôme $p \in K[t]$ est dit* ***irréductible*** *(sur K) si*

(i) $\deg p \geq 1$

(ii) les seuls diviseurs de p sont les polynômes de degré 0 (les polynômes constants) et $c \cdot p(t)$ avec $c \in K \setminus \{0\}$.

Exemples :

1. tout polynôme de degré 1 est irréductible
2. $t^2 + 1 \in \mathbb{R}[t]$ est irréductible (sur $\mathbb{R}$)
3. $t^2 + 1 \in \mathbb{C}[t]$ est réductible : $t^2 + 1 = (t + \mathrm{i})(t - \mathrm{i})$
4. $at^2 + bt + c \in \mathbb{R}[t]$ est irréductible si et seulement si $b^2 - 4ac < 0$.

Théorème 2.45 *Tout polynôme $p \in K[t]$ de degré ≥ 1 peut s'écrire de manière unique (à permutation des facteurs près)*

$$p = \alpha\, g_1 g_2 \cdots g_r \qquad \text{où} \qquad \alpha \in K \tag{2.9}$$

et g_i, $i = 1, \ldots, r$, sont des polynômes irréductibles unitaires (c-à-d que le coefficient dominant vaut 1).

DÉMONSTRATION. Sans perte de généralité, on peut supposer que le coefficient dominant de p vaille 1.

Existence. Si p est irréductible on obtient directement (2.9). Sinon on peut écrire $p = p_1p_2$, où p_1,p_2 sont des polynômes de degré strictement inférieur à $\deg p$. Ainsi, on obtient (2.9) par la récurrence.

Unicité. Soit $p = g_1g_2\cdots g_r = h_1h_2\cdots h_s$, où h_i, $i = 1,\ldots,m$, sont des polynômes irréductibles unitaires. Comme h_1 est irréductible, h_1 divise un de g_i. Mais, comme g_i est aussi irréductible, $h_1 = g_i$. Soit σ une permutation avec $\sigma(1) = i$. Alors,

$$\prod_{\substack{i=1\\ i\neq\sigma(1)}}^{r} g_i = h_2h_3\cdots h_s.$$

En continuant de cette manière, on obtient $r = s$ et l'existence d'une permutation σ telle que $h_i = g_{\sigma(i)}$, $i = 1,\ldots,r$. ■

On dit qu'un polynôme p de degré ≥ 1 est **scindé** si tous les facteurs irréductibles (dans la décomposition du théorème 2.45) sont de degré 1 :

$$p(t) = \alpha(t-c_1)(t-c_2)\cdots(t-c_n), \qquad \alpha,c_1,\ldots,c_n \in K.$$

Théorème 2.46 (Théorème fondamental de l'algèbre) *Tout polynôme à coefficients dans $\mathbb{C}$ est scindé.*

DÉMONSTRATION. 2ème année. ■