Chapitre 8

Structures algébriques usuelles : rappels et compléments

Dans tout ce chapitre, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

Révisions MP2I

Revoir les chapitres 13, 14, 15, et 19.

1 Rappels sur les groupes et les anneaux

1.1 Structure de groupe

Définition 1. On dit qu'un ensemble $(G, *)$ est un *groupe* lorsque :
- $*$ est une loi de composition interne associative sur G
- $(G, *)$ possède un élément neutre (nécessairement unique) e : $\forall x \in G,\ e * x = x * e = x$
- Tout élément $x \in G$ possède un symétrique $y \in G$ (nécessairement unique) pour $*$: $x * y = y * x = e$.

Si $*$ est commutative, on dit que $(G, *)$ est un groupe *commutatif* ou *abélien*

Remarques :
- Si la loi $*$ est clairement identifiée, le groupe $(G, *)$ est noté plus simplement G.
- Les symboles classiques utilisés pour la loi d'un groupe sont $\times, +, \circ, *, \cdot$, qui peuvent se référer à des opérations précises sur certains ensembles (multiplication ou addition de nombres, composition).
- $\times, \circ, *, \cdot$ sont des notations dites "multiplicatives". Dans ce cas :
  — l'élément neutre peut être noté 1_G ou simplement 1 (ou encore I ou Id pour la loi de composition des fonctions $\circ$)
  — Le symétrique de x est noté x^{-1} et appelé *inverse*.
  — Le n-ième itéré de x, avec $n \in \mathbb{N}$ est noté x^n ($x^0 = 1_G$ par convention)
  — on a a tendance à ne pas écrire du tout le symbole d'opération : xy au lieu de $x * y$.
- $+$ est une notation dite "additive". Dans ce cas :
  — l'élément neutre est plutôt noté 0_G ou simplement 0.
  — Le symétrique de x est noté $-x$ et appelé *opposé*
  — Le n-ième itéré de x, avec $n \in \mathbb{N}$ est noté $n \cdot x$ ou nx ($0 \cdot x = 0_G$ par convention)
  — La loi doit être commutative (ne jamais utiliser $+$ comme loi pour un groupe non commutatif)

Proposition 1. *Étant donnés deux groupes $(G_1, *_1)$ et $(G_2, *_2)$ d'éléments neutres e_1 et e_2, la* loi produit $*$ *définie sur $G_1 \times G_2$ par :*

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$$

confère à $G_1 \times G_2$ une structure de groupe, avec pour élément neutre (e_1, e_2). $G_1 \times G_2$ est appelé groupe produit.

Remarque : Cette construction se généralise par récurrence pour définir le groupe produit d'une famille finie de groupes. On l'utilise surtout pour donner à G^n une structure de groupe lorsque G est un groupe : $\mathbb{Z}^n$ par exemple est un groupe abélien pour la loi $+$.

1.2 Sous-groupes et morphismes de groupes

Définition 2. Soit $(G, *)$ un groupe d'élément neutre e. On dit qu'une partie H de G est un sous-groupe de G lorsque :
- $e \in H$
- H est stable pour $*$: pour tout $x, y \in H$, on a $x * y \in H$
- H est stable par symétrisation : pour tout $x \in H$, on a $x^{-1} \in H$.

Remarque : Il suffit de montrer que $H \neq \emptyset$ et que pour tout $x, y \in H$, $x * y^{-1} \in H$.

Proposition 2. *Si H est un sous-groupe de $(G, *)$ d'élément neutre e, alors la loi induite par $*$ sur H (notée encore $*$) est une loi de composition interne et $(H, *)$ est un groupe d'élément neutre e.*

On rappelle que pour pour $\alpha \in \mathbb{R}$, $\alpha\mathbb{Z}$ désigne $\{\alpha k, k \in \mathbb{Z}\}$.

Proposition 3. *Une partie H de $\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$ si, et seulement si, il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Exercice 1. Soit H un sous-groupe de $(\mathbb{R}, +)$. Montrer que l'une **ou** l'autre des deux situations suivantes se présente :
- H est dense dans $\mathbb{R}$
- Il existe $\alpha \geqslant 0$ tel que $H = \alpha\mathbb{Z}$.

Définition 3. Soient $(G, *)$ et $(G', *')$ deux groupes d'éléments neutre e et e'. On appelle *morphisme de groupes* de G dans G', toute application f de G dans G' qui vérifie :

$$\forall (x, y) \in G^2, \quad f(x * y) = f(x) *' f(y).$$

Remarques :
- On a alors nécessairement $f(e) = e'$ et $f(x^{-1}) = \big(f(x)\big)^{-1}$ pour tout $x \in G$.
- Si f est bijective, l'application réciproque f^{-1} est aussi un morphisme et f est appelé *isomorphisme* : On dit alors que G et G' sont *isomorphes* ce qu'on peut noter $G \simeq G'$.
- Si $(G, *) = (G', *')$, f est appelé *endomorphisme*. Si de plus f est bijective, f est appelé *automorphisme*.

Proposition 4. *Soit $(G, *)$ et $(G', *')$ deux groupes d'éléments neutre e et e', et soit $f : G \to G'$ un morphisme.*
- *Si H est un sous-goupe de G, $f(H)$ est un sous-groupe de G'. En particulier $f(G)$ est un sous-groupe de G' appelé* image *de f et noté* $\mathrm{Im}(f)$. *On a $\mathrm{Im}(f) = G'$ si, et seulement si, f est surjectif.*
- *Si H' est un sous-groupe de G', $f^{-1}(H')$ est un sous-groupe de G. En particulier $f^{-1}(\{e'\})$ est un sous-groupe de G appelé* noyau *de f et noté* $\mathrm{Ker}(f)$. *On a $\mathrm{Ker}(f) = \{e\}$ si, et seulement si, f est injectif.*

1.3 Structure d'anneau

Définition 4. Soit A un ensemble muni de deux lois de composition internes $+$ et $\times$. On dit que $(A, +, \times)$ est un *anneau* lorsque :
- $(A, +)$ est un groupe commutatif,
- $\times$ est associative.
- A possède un élément neutre 1_A pour $\times$.
- $\times$ est distributive par rapport à $+$.

On dit que l'anneau est commutatif si $\times$ est commutative.

Remarques :
- Si $1_A = 0_A$, on a $A = \{0_A\}$, appelé anneau *nul* ou *trivial*. On évitera de se placer dans ce cas.
- On note généralement $x \cdot y$ ou encore xy au lieu de $x \times y$.
- Un élément $a \in A$ est dit *inversible* lorsqu'il est symétrisable pour la loi $\times$. On note alors a^{-1} son inverse.
- On montre que 0_A est *absorbant* ($0_A \times a = a \times 0_A = 0_A$ pour tout $a \in A$), en particulier jamais inversible.
- On note $n \cdot a$ ou na avec $n \in \mathbb{Z}$ pour l'itération additive et a^n avec $n \in \mathbb{N}$ (ou $n \in \mathbb{Z}$ si a est inversible) l'itération multiplicative.

Proposition 5. *Étant donnés deux anneaux A_1 et A_2, On peut munir l'ensemble produit $A_1 \times A_2$ de deux lois + et × :*

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \qquad et \qquad (x_1, x_2) \times (y_1, y_2) = (x_1 \times y_1, x_2 \times y_2)$$

Cela confère à $A_1 \times A_2$ une structure d'anneau, avec pour éléments neutres additifs et multiplicatifs $(0, 0)$ *et* $(1, 1)$. *$A_1 \times A_2$ est appelé* anneau produit.

Remarque : Cette construction se généralise par récurrence pour définir l'anneau produit d'une famille finie d'anneaux.

1.4 Sous-anneaux et morphismes d'anneaux

Définition 5. On appelle *sous-anneau* d'un anneau $(A, +, \times)$ un sous-groupe de $(A, +)$ qui est stable par $\times$ et qui contient 1_A. Muni des lois induites, un sous-anneau est un anneau.

Définition 6. Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. On dit que $f : A \to B$ est un *morphisme d'anneau* si :

1. $\forall (x, y) \in A^2, \quad f(x + y) = f(x) + f(y)$,
2. $\forall (x, y) \in A^2, \quad f(x \times y) = f(x) \times f(y)$
3. $f(1_A) = 1_B$.

Remarques :
- Un morphisme d'anneaux est en particulier un morphisme de groupes pour les lois +. En particulier on a nécessairement $f(0_A) = 0_B$ et $f(-x) = -f(x)$ pour tout $x \in A$.
- Si $a \in A$ est inversible, alors $f(a)$ est inversible et $f(a^{-1}) = \big(f(a)\big)^{-1}$.
- Les terminologies *endomorphisme*, *isomorphismes*, *automorphisme* s'adaptent au cas des anneaux.
- L'image d'un sous-anneau par f, en particulier l'image $\mathrm{Im}(f)$ de A, est un sous-anneau de B.
- Le noyau de f, en revanche, n'est jamais un sous-anneau de A, sauf si B est l'anneau nul (pourquoi ?).

Exercice 2. Déterminer les endomorphismes de $\mathbb{Z}$:

a) En tant que groupe pour +

b) En tant qu'anneau pour + et ×.

1.5 Anneau intègre et corps, groupe des inversibles

Définition 7. On dit qu'un anneau A est *intègre* lorsqu'il est non nul, commutatif, et qu'il vérifie :

$$\forall a, b \in A, \quad ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Remarques :
- Dans un anneau intègre, on a ainsi les règles de simplifications suivantes, pour tout $a, x, y \in A$ avec $a \neq 0$:
$$ax = ay \Rightarrow x = y \qquad \text{et} \qquad xa = ya \Rightarrow x = y$$
On dit que tout $a \in A$ non nul est *régulier*
- Si a est inversible, a est régulier. La réciproque est fausse.

Exemples :
- $\mathbb{Z}$ est un anneau intègre, mais seuls 1 et -1 sont inversibles.
- $\mathbb{K}[X]$ est un anneau intègre (si P et Q sont non nuls, PQ est non nul de degré $\deg(P) + \deg(Q)$) mais seuls les polynômes constants non nuls sont inversibles.
- l'anneau $\mathcal{M}_n(\mathbb{K})$ n'est pas intègre pour $n \geqslant 2$ ($E_{1,2}^2$ est la matrice nulle, par exemple, et de toute façon, ce n'est pas un anneau commutatif).

Exercice 3. Montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si, et seulement si, elle est régulière dans $\mathcal{M}_n(\mathbb{K})$.

Proposition 6. *L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la loi ×.*

Définition 8. L'ensemble $A^\times$ s'appelle *groupe des inversibles*, ou encore *groupe des unités* de A. On peut le noter aussi $U(A)$.

Exemples :
- $\mathbb{Z}^\times = \{-1, 1\}$, à ne pas confondre avec $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$.
- $\mathbb{K}[X]^\times = \mathbb{K}_0[X] \simeq \mathbb{K}^*$.
- $\mathcal{M}_n(\mathbb{K})^\times = GL_n(\mathbb{K})$.

Définition 9. Un anneau A est un *corps* lorsque c'est un anneau non nul, commutatif, et dans lequel tout élément non nul est inversible. On a alors $A^\times = A^* = A\backslash\{0\}$.

Exemples :
- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ (*corps des fractions* de l'anneau intègre $\mathbb{Z}$)
- L'ensemble des *fractions rationnelles* $\mathbb{K}(X)$: c'est le *corps des fractions* de l'anneau intègre $\mathbb{K}[X]$.

1.6 Structure de $\mathbb{Z}/n\mathbb{Z}$

Définition 10. Soit $n \in \mathbb{N}$. On dit que a est *congru à b modulo n* lorsque $a - b \in n\mathbb{Z}$. On note alors $a \equiv b \quad [n]$.

Proposition 7. *La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Définition 11. Pour $n \in \mathbb{N}$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n.

Pour $k \in \mathbb{Z}$, on note $\overline{k}$ (ou $\dot{k}$) la classe de k pour cette relation.

Proposition 8. *Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n, et on a :*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Remarque : Cela ne fonctionne pas pour $n = 0$ puisque $\mathbb{Z}/0\mathbb{Z} = \{\{k\}, k \in \mathbb{Z}\}$ qui est infini.
À "l'opposé" de cette situation, on a $\mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\}$ de cardinal 1.

Proposition 9. *La relation de congruence modulo n sur $\mathbb{Z}$ est compatible avec sa structure d'anneau :*
- *Si $a_1 \equiv b_1$ et $a_2 \equiv b_2$, $a_1 + a_2 \equiv b_1 + b_2$*
- *Si $a \equiv b$, $-a \equiv -b$.*
- *si $a_1 \equiv b_1$ et $a_2 \equiv b_2$, alors $a_1 a_2 \equiv b_1 b_2$*

Le résulat précédent permet de définir une addition et une multiplication sur $\mathbb{Z}/n\mathbb{Z}$.

Définition 12. Soit $n \in \mathbb{N}$. Pour tout $u, v \in \mathbb{Z}/n\mathbb{Z}$:

$$u + v = \overline{a + b}, \quad \text{où} \quad u = \overline{a} \text{ et } v = \overline{b},$$

$$uv = \overline{ab}, \quad \text{où} \quad u = \overline{a} \text{ et } v = \overline{b},$$

ce qui ne dépend pas des représentants a et b choisis dans $\mathbb{Z}$.

Proposition 10. *Muni de l'addition définie ci-dessus, $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif d'élément neutre $\overline{0}$.*

L'application $\phi : k \mapsto \overline{k}$ est un morphisme de surjectif de groupes, de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, appelé surjection canonique*, et de noyau $n\mathbb{Z}$.*

Exemples :
- Pour $n = 0$, ϕ est un isomorphisme : $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$.
- Pour $n = 1$, on a $\operatorname{Ker}(\phi) = \mathbb{Z}$ et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$ est le groupe trivial à un seul élément.
- Pour $n = 2$, on a $\operatorname{Ker}(\phi) = 2\mathbb{Z}$ (ensemble des entiers pairs) et $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$: il s'agit de l'unique groupe à 2 éléments, à isomorphisme près.

Exercice 4. Soit $f : \mathbb{Z} \to \mathbb{Q}^*$ défini par $f(k) = (-1)^k$.

a) Montrer que f définit un morphisme de groupes de $(\mathbb{Z}, +)$ vers $(\mathbb{Q}^*, \times)$

b) Déterminer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

c) Montrer que $\mathrm{Im}(f) \simeq \mathbb{Z}/2\mathbb{Z}$.

Proposition 11. *Muni de l'addition et de la multiplication précedemment définies, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif d'éléments neutres $\overline{0}$ et $\overline{1}$.*

L'application $\phi : k \mapsto \overline{k}$ est un morphisme surjectif d'anneaux, de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, appelé surjection canonique*, et de noyau $n\mathbb{Z}$.*

Remarques :
- Pour $n = 0$, ϕ est un isomorphisme : $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$.
- Pour $n = 1$, on a $\overline{0} = \overline{1}$ et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$ est donc l'anneau nul.

2 Compléments sur les groupes

2.1 Sous-groupe engendré par une partie

Soit $(G, \cdot)$ un groupe.

Proposition 12. *Toute intersection de sous-groupes de G est un sous-groupe de G.*

Définition 13. Soit $A \subset G$.
- on appelle *sous-groupe engendré* par A l'intersection de tous les sous-groupes de G contenant A. On le note $\langle A \rangle$.
- On dit que A est une *partie génératrice* de G lorsque $\langle A \rangle = G$.

Remarques :
- Le sous-groupe engendré par A est le plus petit (au sens de la relation d'inclusion) sous-groupe contenant A. Pour montrer que H est le sous-groupe engendré par A, il suffit donc de montrer que :
  — H est un sous-groupe contenant A.
  — Si H' est un autre sous-groupe contenant A, alors $H \subset H'$.
- Si A est un singleton $\{a\}$, on peut aussi parler du sous-groupe engendré par a (et on dit alors que a est un *générateur*), qu'on note plus simplement $\langle a \rangle$. Si A est une paire $\{a, b\}$, avec $a \neq b$, on peut parler du sous-groupe engendré par a et b, qu'on note $\langle a, b \rangle$.

Exemples :
- Le sous-groupe engendré par e est le sous-groupe trivial $\{e\}$.
- Dans le groupe $(\mathbb{Z}, +)$, si $n \in \mathbb{N}^*$, alors $\langle n \rangle = n\mathbb{Z}$.
- En particulier, 1 est un générateur de $\mathbb{Z}$.
- L'ensemble $\mathcal{T}$ des transpositions de $[\![1, n]\!]$ est une partie génératrice du groupe symétrique S_n.
- L'ensemble des matrices de $\mathcal{M}_n(\mathbb{K})$ associées à des opérations élémentaires (dilatation, transvection, permutation) est une partie génératrice de $GL_n(\mathbb{K})$.
- L'ensemble des réflexions d'un espace euclidien E est une partie génératrice du groupe orthogonal $O(E)$ (voir chapitre ultérieur).

2.2 Groupes engendrés par un élément

Dans ce qui suit, on considère toujours un groupe $(G, \cdot)$ d'élément neutre e, en notant sans symbole la loi du groupe.

Proposition 13. *Si $a \in G$, le sous-groupe de G engendré par a est :*

$$\langle a \rangle = \{a^k, k \in \mathbb{Z}\} \quad \textit{ou} \quad \langle a \rangle = \{k\,a, k \in \mathbb{Z}\} \quad \textit{(en notation additive)}$$

Définition 14.
- On dit que G est un groupe *monogène* lorsqu'il est engendré par un seul élément : il existe $a \in G$ tel que $G = \langle a \rangle$.
- On dit que G est un groupe *cyclique* lorsqu'il est monogène et fini.

Tout élément a qui engendre G est appelé un *générateur*.

Exemples :
- $(\mathbb{Z},+)$ est monogène infini, engendré par 1 ou par -1.
- Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par $\overline{1}$.

En fait les exemples de $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$) encapsulent toutes les situations possibles de groupes monogènes, à isomorphisme près :

Proposition 14. *Supposons G monogène. Alors :*
- *Si G est infini, $G \simeq \mathbb{Z}$.*
- *Si G est fini de cardinal n, $G \simeq \mathbb{Z}/n\mathbb{Z}$.*

Exercice 5. Soit $n \in \mathbb{N}^*$. Montrer que l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un groupe cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Remarques :
- $\mathbb{U}_n$ est le noyau du morphisme de groupes $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ défini par $\varphi(z) = z^n$.
- Rappelons que $\mathbb{U}_n$ est aussi un sous-groupe de $\mathbb{U}$, lui-même sous-groupe de $(\mathbb{C}^*, \times)$, comme noyau du morphisme de groupes $z \mapsto |z|$.

2.3 Ordre d'un élément d'un groupe

Définition 15. Soit $a \in G$. Si le sous-groupe $\langle a \rangle$ est fini, on appelle *ordre* de a le cardinal de $\langle a \rangle$. On dit sinon que a est d'ordre infini.

Remarque : Lorsque a est d'ordre fini $d \geqslant 1$, d est le plus petit entier $n > 0$ tel que $a^n = e$ (élément neutre).

Proposition 15. *Si a est d'ordre fini d alors pour tout $n \in \mathbb{Z}$, $a^n = e \Leftrightarrow d|n$.*

Proposition 16. *Si G est un groupe fini, alors tout élément de G est d'ordre fini, et son ordre divise* $\mathrm{card}(G)$.

Remarque : Un théorème plus général (Lagrange) montre que si G est fini, le cardinal de n'importe quel sous-groupe divise le cardinal de G.

Exercice 6.

a) Déterminer l'ordre de $(\overline{1}, \overline{1})$ dans le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, et en déduire qu'il s'agit d'un groupe cyclique.

b) Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (appelé groupe de Klein) n'est pas cyclique.

c) montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si, et seulement si, m et n sont premiers entre eux.

3 Complément sur les anneaux

3.1 Idéal d'un anneau commutatif

Dans toute la suite, A est un anneau commutatif. On a vu que le noyau d'un morphisme d'anneaux $f : A \to B$ n'est pas un sous-anneau de A car il ne contient pas 1_A. Il a cependant une structure intéressante que nous découvrons ici.

Définition 16. Une partie I de A est appelé un *idéal* lorsque :
- $(I,+)$ est un sous-groupe de $(A,+)$
- Pour tout $a \in I$ et tout $x \in A$, $ax \in I$.

Remarque : les deux points important à noter par rapport à un sous-anneau sont
- le fait que $1_A \notin I$ en général.
- la stabilité multiplicative lors du produit d'un élément a de I par n'importe quel élement x de A (et pas seulement de I).

Il suffit en pratique de vérifier que I n'est pas vide, est stable pour l'addition, et vérifie de plus $ax \in I$ pour tout $(a,x) \in I \times A$.

Exercice 7. Soit I un idéal de A. Montrer que $I = A$ si, et seulement si, $I \cap A^\times \neq \varnothing$.

Proposition 17. *Le noyau d'un morphisme $f : A \to B$ d'anneaux est un idéal de A.*

3.2 Idéal engendré par un élément

Proposition 18. *Soit $a \in A$. L'ensemble $aA = \{ax, x \in A\}$ est un idéal de A. On dit que c'est l'*idéal engendré *par a.*

Un idéal engendré ainsi par un seul élément est appelé un idéal principal.

Définition 17. On dit qu'un idéal I est *principal* lorqu'il est engendré par un seul élément, *i.e* lorsqu'il existe $a \in A$ tel que $I = aA$.

On a déjà vu que tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$. Ce sont donc également des idéaux de l'anneau $(\mathbb{Z}, +, \times)$. Il s'avère même que ce sont les seuls :

Proposition 19. *Si I est un idéal de $\mathbb{Z}$, il existe un unique $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.*

Remarques :
- $-n$ est aussi un générateur de $n\mathbb{Z}$, mais il n'y en a pas d'autres.
- Tous les idéaux de $\mathbb{Z}$ sont donc principaux : on dit que $\mathbb{Z}$ est un anneau *principal*.

Si $\mathbb{K}$ est un corps, une situation similaire se présente dans l'anneau $\mathbb{K}[X]$ des polynômes en X

Proposition 20. *Si I est un idéal de $\mathbb{K}[X]$, il existe un unique $P \in \mathbb{K}[X]$ unitaire tel que $I = P\mathbb{K}[X]$.*

Remarques :
- Pour tout $\lambda \in \mathbb{K}^*$, λP est aussi un générateur.
- Tous les idéaux de $\mathbb{K}[X]$ sont donc principaux : tout comme $\mathbb{Z}$, $\mathbb{K}[X]$ est un anneau principal.

3.3 Compléments sur $\mathbb{Z}/n\mathbb{Z}$

Proposition 21. *Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$.*
- *$\overline{k}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, k est premier avec n.*
- *$\overline{k}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ si, et seulement si, k est premier avec n.*

Remarques :
- Les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ correspondent donc précisément aux générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Pour trouver en pratique l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$, on doit chercher une relation de Bézout $uk + vn = 1$: les nombres u et v s'obtiennent grâce à l'algorithme d'Euclide étendu (voir cours MP2I).

Corollaire 1. *$\mathbb{Z}/p\mathbb{Z}$ est un corps si, et seulement si, p est premier. On note alors ce corps $\mathbb{F}_p$.*

Exercice 8. Déterminer les inverses des éléments non nuls du corps $\mathbb{F}_{17}$.

3.4 Divisibilité dans un anneau intègre

Dans ce paragraphe, on suppose que A est intègre, donc commutatif et sans diviseur de 0 (un produit de deux éléments non nuls n'est pas nul). Cette propriété, vérifiée notamment par $\mathbb{Z}$ et $\mathbb{K}[X]$, va permettre de généraliser différents aspects liés à la relation de divisibilité présente dans ces deux anneaux, et de dégager notamment la notion d'élément *irréductible*.

Définition 18. Étant donnés a et b non nuls dans A, on dit que a *divise* b et on note $a \mid b$ lorsqu'il existe $c \in A$ tel que $b = ac$.

Proposition 22. *Soient $a, b \in A \backslash \{0\}$. Alors $a \mid b$ si, et seulement si, $bA \subset aA$.*

Remarque : La relation «divise» est réflexive et transitive, mais pas symétrique. Ce n'est donc pas une relation d'ordre, mais seulement de *préordre*. Le fait que A est intègre va conduire à ce que ce défaut de symétrie soit complétement encapsulée par le groupe $A^\times$ des inversibles.

Proposition 23. *Les trois assertions suivantes sont équivalentes :*

(i) $a \mid b$ *et* $b \mid a$.

(ii) $aA = bA$

(iii) Il existe $u \in A^\times$ *tel que* $b = ua$

Dans ces conditions, on dit que a *et* b *sont* associés.

Exemples :
- dans l'anneau $\mathbb{Z}$, a et b sont associés si, et seulement si, $a = \pm b$.
- dans l'anneau $\mathbb{K}[X]$, P et Q sont associés si, et seulement si, il existe $\lambda \in \mathbb{K}^*$, tel que $P = \lambda Q$.

La définition suivante généralise la notion de nombre premier.

Définition 19. Un élément $p \in A$ non nul est dit *irréductible* lorsque :
- $p \notin A^\times$
- Pour tout $a, b \in A$, $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Autrement dit, un élément irréductible n'est pas inversible et ses seuls diviseurs sont ses associés ou les inversibles.

Exemples :
- dans l'anneau $\mathbb{Z}$ on retrouve au signe près la notion de nombre premier : $p \in \mathbb{Z}$ est irréductible si, et seulement si, $|p|$ est un nombre premier.
- dans l'anneau $\mathbb{K}[X]$ on retrouve la notion de polynôme irréductible : P est irréductible si, et seulement si, $\deg(P) \geqslant 1$ et $P = AB \Rightarrow A$ ou B constant.

3.5 Décomposition en facteurs irréductibles

Grâce à la division euclidienne, les éléments irréductibles de $\mathbb{Z}$ et $\mathbb{K}[X]$ constituent des briques fondamentales permettant de reconstruire tous les éléments de ces anneaux.

Théorème 1. ***(de décomposition en facteurs premiers dans*** $\mathbb{Z}$***)***

Soit $n \in \mathbb{Z}$ *avec* $|n| \geqslant 2$. *Il existe alors* $k \in \mathbb{N}^*$, $p_1, \ldots, p_k \in \mathbb{N}$ *premiers et deux à deux distincts, et* $m_1, \ldots, m_k \in \mathbb{N}^*$ *tels que*

$$n = \pm p_1^{m_1} \cdots p_k^{m_k}$$

Cette décomposition est unique à l'ordre des facteurs près.

Remarque : En notant $p = p_i$ pour un certain $i \in [\![1, k]\!]$, m_i est la *valuation* p-adique de n, et peut se noter $\nu_p(n)$.

Exemple : $-6600 = -2^3 \times 3 \times 5^2 \times 11$ et $\nu_5(-6600) = 2$.

Théorème 2. ***(de décomposition en facteurs irréductibles dans*** $\mathbb{K}[X]$***)***

Soit $P \in \mathbb{K}[X]$ *avec* $\deg(P) \geqslant 1$. *Il existe alors* $a \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, $P_1, \ldots, P_k \in \mathbb{K}[X]$ *unitaires irréductibles deux à deux distincts et* $m_1, \ldots, m_k \in \mathbb{N}^*$ *tels que*

$$P = aP_1^{m_1} \cdots P_k^{m_k}$$

Cette décomposition est unique à l'ordre des facteurs près.

Remarques :
- Il peut être important de bien préciser dans quel anneau de polynôme on considère l'irréductibilité, autrement dit de quel corps $\mathbb{K}$ on parle. Par exemple $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{R}[X]$.
- Tout polynôme de degré 1 est irréductible.
- Si P est irréductible dans $\mathbb{K}[X]$, P n'admet aucune racine dans $\mathbb{K}$, mais attention, la réciproque est fausse ($X^4 + 1$ n'a aucune racine réelle mais n'est pas irréductible sur $\mathbb{R}$)

Le cas de $\mathbb{C}[X]$ est fondamental : seuls les polynômes de degré 1 sont irréductible, de sorte que tout polynôme est scindé. C'est une conséquence immédiate du théorème fondamental de l'algèbre :

Théorème 3. ***(de d'Alembert-Gauss)***
Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine.

Corollaire 2.
- *Les éléments irrédutibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 ;*
- *Tout polynôme $P \in \mathbb{C}[X]$ est scindé : il existe $a \in \mathbb{K}^*$, $k \in \mathbb{N}^*$, $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ deux à deux distincts et $n_1, \ldots, n_k \in \mathbb{N}^*$ tels que*
$$P = a(X - \lambda_1)^{m_1} \cdots (X - \lambda_k)^{m_k}$$
Cette décomposition est unique à l'ordre des facteurs près.

Remarque : Dans ce contexte, m_i est la *multiplicité* de la racine λ_i, pour tout $i \in [\![1, k]\!]$.

Exercice 9.

a) Montrer que tout polynôme $P \in \mathbb{R}[X]$ de degré impair admet au moins une racine réelle.

b) En déduire que les polynômes irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 à discriminant strictement négatif.

c) Expliciter le théorème de decomposition en facteurs irréductibles dans $\mathbb{R}[X]$.

Exercice 10. Déterminer la décomposition de $X^4 - X^2 - 2$ en facteurs irréductibles dans $\mathbb{K}[X]$ suivant que $\mathbb{K}$ est le corps $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, et $\mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q}$.

4 Algèbres

4.1 Définition

Définition 20. On appelle $\mathbb{K}$-*algèbre*, ou *algèbre* sur $\mathbb{K}$, tout quadruplet $(A, +, \times, \cdot)$ tel que :

(i) $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

(ii) $(A, +, \times)$ est un anneau.

(iii) $\forall \lambda \in \mathbb{K},\ \forall (a, b) \in A^2,\ (\lambda \cdot a) \times b = a \times (\lambda \cdot b) = \lambda \cdot (a \times b)$

On dit de plus que l'algèbre $(A, +, \times, \cdot)$, ou plus simplement A, est
- commutative si l'anneau sous-jacent $(A, +, \times)$ est commutatif
- intègre si l'anneau sous-jacent $(A, +, \times)$ est intègre.
- de dimension finie si l'espace vectoriel sous-jacent $(A, +, \cdot)$ est de dimension finie. La dimension de A est alors la dimension de cet espace vectoriel.

Remarques :
- En pratique la notation pour les lois multiplicatives $\times$ (interne) et $\cdot$ (externe) est omise.
- Si $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel, les conditions (ii) et (iii) signifient que $(a, b) \mapsto a \times b$ est une application $\mathbb{K}$-bilinéaire de $A \times A$ dans A définissant une l.c.i. associative et admettant un élément neutre 1_A différent de 0_A.

Exemples :
- $\mathbb{K}[X]$ est une algèbre intègre.
- Si E est un $\mathbb{K}$-espace vectoriel, $\big(\mathcal{L}(E), +, \circ, \cdot\big)$ est une $\mathbb{K}$-algèbre non intègre en général.
- $\mathcal{M}_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre non intègre si $n \geqslant 2$.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{K}'$, $\mathbb{K}'$ est une $\mathbb{K}$-algèbre.
- Si X est un ensemble quelconque, $\mathcal{F}(X, \mathbb{K})$ est une $\mathbb{K}$-algèbre commutative mais non intègre pour les lois usuelles $+$ et $\times$ déduites de celles de $\mathbb{K}$. La loi externe $(\lambda, f) \mapsto \lambda f$ se confond avec la loi interne $\times$ en interprétant λ comme une fonction constante.

4.2 Sous-algèbre et morphisme d'algèbre

Définition 21. Soit A une $\mathbb{K}$-algèbre. On appelle sous-algèbre de A toute partie de A qui est à la fois un sous-espace vectoriel et un sous-anneau de A.

Définition 22. Soient A et B deux algèbres sur le même corps $\mathbb{K}$. On dit que $f : A \to B$ est un morphisme d'algèbres lorsque f est à la fois un morphisme d'anneaux et une application linéaire :
- $\forall (x, y) \in A^2,\ \forall \lambda \in \mathbb{K},\ f(x + \lambda y) = f(x) + \lambda f(y)$
- $\forall (x, y) \in A^2\ f(xy) = f(x)f(y)$
- $f(1_A) = 1_B$.

Proposition 24. *Si $f : A \to B$ est un morphisme d'algèbres, alors :*
- $\mathrm{Im}(f)$ *est une sous-algèbre de* B
- $\mathrm{Ker}(f)$ *est à la fois un idéal et un sous-espace vectoriel de* A.

Exemple : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n muni d'une base $\mathcal{B}$. L'application $u \mapsto \underset{\mathcal{B}}{\mathrm{Mat}}(u)$ est un isomorphisme d'algèbres de $\mathcal{L}(E)$ sur $\mathcal{M}_n(\mathbb{K})$. En particulier si $E = \mathbb{K}^n$ et $\mathcal{B}$ est la base canonique, cet isomorphisme est dit *canonique* : il est tellement naturel qu'on peut procéder à l'identification $\mathcal{L}(\mathbb{K}^n) = \mathcal{M}_n(\mathbb{K})$.

La proposition suivante permet de définir l'idéal annulateur d'une matrice, ainsi que la notion de polynôme minimal, un outil essentiel pour la réduction (voir chapitre suivant).

Proposition 25. *Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{K})$. Il existe un unique morphisme d'algèbres $\Phi : \mathbb{K}[X] \to \mathcal{L}(E)$ vérifiant $\Phi(X) = u$.*

Remarques :
- Le noyau de Φ est un idéal de $\mathbb{K}[X]$ appelé *idéal annulateur* de u. Il est engendré par un polynôme unitaire appelé *polynôme minimal* de A et noté μ_A.
- L'image de Φ est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$ de dimension finie $\deg(\mu_A)$. Elle est appelée *algèbre des polynômes en A*, et notée $\mathbb{K}[A]$.