Algèbre et Géométrie 3

Licence de mathématiques S3

2017-2018

Chapitre 1

Structures algébriques.

1.1 Notion de Groupe.

Définition et premiers exemples

Définition 1.1.1. *Soit E un ensemble. Une* ***loi de composition interne (LCI)*** *est une application*

$$* : E \times E \to E.$$

Pour $x, y \in E$, on note $x * y$ l'élément de E obtenu par application de $*$ au couple (x, y).

Définition 1.1.2. *Un* ***groupe*** *est un couple $(G, *)$ où G est un ensemble non vide muni d'une loi de composition interne $* : G \times G \to E$, qui vérifie :*

GR1*. $*$ est associative : $\forall (x, y, z) \in G^3, (x * y) * z = x * (y * z)$,*

GR2*. Il existe un élément neutre : $\exists e \in G$ tel que $\forall x \in G, x * e = e * x = x$,*

GR3*. Tout élément a un inverse : $\forall x \in G, \exists y \in G$ tel que $x * y = y * x = e$.*

Proposition 1.1.1.

- *Tout groupe a un unique élément neutre.*
- *Tout élément x d'un groupe a un unique inverse.*

Démonstration. □

Exemple 1.1.1.

- $(\mathbb{C}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +)$ *sont des groupes.* $(\mathbb{N}, +)$ *n'est pas un groupe.*
- $(\mathbb{C}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{Q}^*, \cdot)$ *sont des groupes.*

Exemple 1.1.2. *Les nombres complexes de valeur absolue 1 forment un groupe avec LCI multiplication.*

Exemple 1.1.3.
- *L'ensemble {1,-1} est un groupe avec LCI multiplication.*
- *L'ensemble {1,i,-1,-i} est un groupe avec LCI multiplication.*

Exemple 1.1.4. *Soit V un sous-espace vectoriel de $\mathbb{R}^n$. Alors $(V,+)$ est un groupe.*

Définition 1.1.3. *Un groupe $(G,*)$ est dit **commutatif** (ou **abélien**) si*

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

Exemple 1.1.5.
- *Les groupes $(\mathbb{C},+),(\mathbb{R},+),(\mathbb{Q},+),(\mathbb{Z},+),(\mathbb{C}^*,\cdot),(\mathbb{R}^*,\cdot),(\mathbb{Q}^*,\cdot)$ sont abeliens.*
- *Soit $G = GL(2,\mathbb{R})$ l'ensemble des matrices 2×2 invertibles, à coéfficients dans $\mathbb{R}$. G muni de LCI multiplication est un groupe non-abelien (comment est-ce qu'on justifie ca ?).*

Notations. Si $(G,*)$ est un groupe, nous allons noter xy l'élément $x*y$ e l'élément neutre, et x^{-1} l'inverse de x.

Souvent, au lieu d'écrire $(G,*)$, nous allons écrire tout simplement G.

Définition 1.1.4 (Produit direct)**.** *Soit G, G' deux groupes. On définit*

$$G \times G' = \{(x,x') | x \in G, x' \in G'\}.$$

On définit la loi de composition

$$* : (G \times G') \times (G \times G') \to G \times G'$$

par

$$(x,x') * (y,y') = (xy, x'y').$$

*On montre facilement que $G \times G'$ muni de cette LCI est un groupe. On appelle $G \times G'$ **le produit direct** de G et G'.*

D'après la définition, un groupe G a au moins un élément. Le groupe $G = \{e\}$ est **trivial**. Si G a un nombre fini d'éléments, on dit que G est un **groupe fini** ou un **groupe d'ordre fini**, et le nombre d'éléments dans un groupe fini G est appellé **l'ordre** de G. Si G n'est pas fini, on dit que G est un **groupe infini**. Par exemple, les groupes dans Exemple 1.1.3 sont finis, d'ordre 2 et 4.

Exemple 1.1.6 (Groupe symétrique d'un ensemble E)**.** *Soit E un ensemble non vide. On considère l'ensemble*

$$S_E = \{f : E \to E \text{ bijection }\}.$$

On muni S_E de l'operation $\circ$ de composition des applications : $(f \circ g)(x) = f(g(x))$.

Proposition 1.1.2. *$(S_E, \circ)$ est un groupe, appelé groupe symétrique de E.*

Démonstration. Exercice □

Les éléments du groupe symétrique S_E sont appelés permutations (de E). Lorsque E est fini, on représente souvent une telle permutation σ par un tableau dont la première ligne est les éléments de E, et la deuxième leur image par σ. Par exemple, si $E = \{1, 2, 3, 4, 5\}$, on écrit pour un $\sigma \in E$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) \end{pmatrix}.$$

Exercice 1.1.1. *Soit*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}, \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Calculer $\sigma \circ \sigma', \sigma^{-1}$ et σ'^{-1}.

Si $E = \{1, 2, 3, \ldots, n\}$, on note S_n le groupe symétrique.

Proposition 1.1.3. *S_n est fini d'ordre $n!$*

Démonstration. □

Règles de calcul dans les groupes

Soit G un groupe. Pour $x_1, x_2, \ldots, x_n$ des éléments dans G, on définit leur produit par récurrence :

$$x_1 x_2 x_3 \ldots x_n = (x_1 x_2 x_3 \ldots x_{n-1}) x_n.$$

En utilisant l'associativité de la LCI, on peut montrer qu'on obtient le même élément indépendement de comment on met des parenthèses autour d'éléments. Par exemple, si $n = 4$, nous avons

$$(x_1 x_2)(x_3 x_4) = ((x_1 x_2) x_3) x_4$$

et aussi

$$(x_1x_2)(x_3x_4) = x_1(x_2(x_3x_4)).$$

Si G est abelien, on peut montrer par récurrence que le produit $x_1x_2 \dots x_n$ est independent de l'ordre dont on écrit les éléments. Soit G un groupe et $x \in G$. Pour n un entier strictement positif, on définit

$$x^n = \underbrace{xx \dots x}_{n \text{ fois}}.$$

Pour $n = 0$, on définit $x^0 = e$, où e est l'élément neutre de G. Si $n = -m$ où $m > 0$ un entier on définit

$$x^{-m} = (x^{-1})^m.$$

Proposition 1.1.4. *Soit G un groupe. Alors $\forall (m, n) \in \mathbb{Z}^2$, $\forall g \in G$,*

$$g^m \cdot g^n = g^{m+n},$$
$$(g^m)^n = g^{mn},$$
$$(g^n)^{-1} = (g^{-1})^n$$

Démonstration. En exercice. Il faut noter que l'inverse de l'inverse est l'élément lui-même. □

Proposition 1.1.5. *Soit G un groupe. Pour tous x, y, a dans G,*

(a) $(ax = ay) \Rightarrow (x = y)$ *et* $(xa = ya) \Rightarrow (xa = ya)$,
(b) $(xy = e) \Rightarrow (x = y^{-1})$,
(c) $(xy)^{-1} = y^{-1}x^{-1}$.

Démonstration.

(a) Si $ax = ay$ alors $a^{-1}ax = a^{-1}ay$ donc $ex = ey$ d'où $x = y$.
(b) Si $xy = e$ alors $xyy^{-1} = y^{-1}$ donc $x = y^{-1}$.

□

Sous-groupes

Définition 1.1.5. *Soit G un groupe et H une partie de G. On dit que H est un* ***sous-groupe*** *de G et on écrit $H < G$ si :*

1. *H contient l'élément neutre de G ;*
2. *Si $x, y \in H$, alors $xy \in H$ et $x^{-1} \in H$.*

Proposition 1.1.6. *Un sous-groupe H d'un groupe G muni de la LCI restreinte à H est un groupe.*

Exemple 1.1.7. *Soit G un groupe. Les ensembles $H = G$ et $H = \{e\}$ sont toujours des sous-groupes de G.*

Exemple 1.1.8. *$(\mathbb{Q}, +)$ et $(\mathbb{Z}, +)$ sont des sous-groupes de $(\mathbb{R}, +)$. Le groupe $(\mathbb{R}_+^*, \cdot)$ est un sous-groupe de $(\mathbb{R}^*, \cdot)$.*

Théorème 1.1.1. *Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles*

$$n\mathbb{Z} = \{nx |\ x \in Z\},$$

où $n \in \mathbb{N}$.

Démonstration. Montrons d'abord que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Nous avons $0 = n0 \in n\mathbb{Z}$. Pour na et nb dans $n\mathbb{Z}$, la somme est $na + nb = n(a + b) \in \mathbb{Z}$. Finalement pour $na \in n\mathbb{Z}$, $-na = n(-a) \in n\mathbb{Z}$.

Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si H est trivial, i.e. $H = \{0\}$, on écrit $H = 0\mathbb{Z}$. Si H n'est pas trivial, montrons qu'il existe $n > 0$ entier tel que $H = n\mathbb{Z}$. Comme $H \neq \{0\}$, il contient un élément non nul, et quitte à considerer son opposé, il existe ainsi un élément non nul et positif dans H. Posons

$$n = \min\{y | y \in H \cap N^*\}.$$

Vérifions que $H = n\mathbb{Z}$, en procédant par double inclusion :

- $\forall q \in \mathbb{Z}, qn = nq \in H$, donc $n\mathbb{Z} \subset H$.
- Soit $x \in H$, faisons la division euclidienne de x par n : $x = nq + r$ avec $0 \leq r < n$. Nous avons $r = x - nq \in H$, donc $r = 0$ par définition de n. D'où $n|x$, et ainsi $H \subset n\mathbb{Z}$.

□

Soit G un groupe. Nous allons décrire maintenant une façon d'obtenir des sous-groupes de G. Soit S un sous-ensemble non vide de G. On pose

$$H = \{x_1 x_2 \dots x_n |\ \forall i, 1 \leq i \leq n,\ x_i \in S \text{ ou } x_i^{-1} \in S,\ n \in \mathbb{N}^*\}.$$

Montrons que H est un sous-groupe de G. Si $x \in S$, alors $e = xx^{-1} \in H$. Pour $x, y \in H$, on écrit $x = x_1 x_2 \dots x_m$ et $y = y_1 y_2 \dots y_k$ où x_i ou x_i^{-1} et y_j ou y_j^{-1} sont dans S. Donc le produit $xy = x_1 \dots x_m y_1 \dots y_k$ est aussi dans H. L'inverse de x est (Exercice 6 du Feuille 1) $x^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1}$ et donc aussi est contenu dans H. H est donc un sous-group de G. Nous allons dire que H est le sous-groupe **engendré** par S, et que S est l'ensemble des générateurs de H. La notation est

$$H = \langle S \rangle.$$

Exemple 1.1.9. *Le groupe additif $\mathbb{Z}$ est cyclique : $Z = \langle 1 \rangle$. Pour $n \in \mathbb{N}$, le sous-groupe $H = n\mathbb{Z}$ est cyclique, il est engendré par n.*

Exemple 1.1.10. *Soit a, b deux éléments dans le groupe additif des entiers $\mathbb{Z}$. Soit $H = \langle a, b \rangle$ le sous-groupe de $\mathbb{Z}$ engendré par a et b. Notons que, comme H est abelien, tout élément x de H est de la forme $x = ar + br'$, $r, r' \in \mathbb{Z}$. D'après le Théorème 1.1.1, il existe $d \in \mathbb{Z}$ tel que $H = d\mathbb{Z}$. Montrons que $d = gcd(a, b)$. On démontre en deux étapes.*

1. *$d|a$ et $d|b$.*
   D'abord, comme $a \in H$ et $b \in H$, nous avons $a \in d\mathbb{Z}$ et $b \in d\mathbb{Z}$ d'où $d|a$ et $d|b$.
2. *($n|a$ et $n|b$) $\Rightarrow n|d$.*
   Soit $n \in \mathbb{Z}$ un diviseur de a et de b. Montrons que $n|d$. En effet, comme $d \in H$, on peut écrire $d = ar + br'$. On a aussi $a = nk$ et $b = nk'$. D'où $d = n(kr + k'r')$.

Donc $d = gcd(a, b)$.

Si G est un groupe et les éléments $x_1, x_2 \ldots, x_r$ forment un ensemble de générateurs de G, on écrit

$$G = \langle x_1, \ldots, x_n \rangle.$$

Groupes cycliques

Nous allons dire que G est **cyclique** ou **monogène** si il existe un élément $x \in G$ tel que

$$G = \langle x \rangle.$$

Exemple 1.1.11. *Soit $G = \mathbb{Q}^*$ un groupe multiplicatif, et $S = \{2\}$. Le sous-groupe de G engendré par S est $H = \{2^n | n \in \mathbb{Z}\}$. H est un groupe cyclique.*

Exemple 1.1.12. *Le groupe additif $\mathbb{Z}$ est cyclique, $\mathbb{Z} = \langle 1 \rangle$. En effet, tout nombre entier s'écrit comme $1 + 1 + \ldots + 1$ ou comme $-1 - 1 - \ldots - 1$. Le sous-groupe $n\mathbb{Z}$ est engendré par n, $n\mathbb{Z} = \langle n \rangle$.*

Soit G un groupe et $a \in G$. Si $a^n = e$ pour un $n \geq 1$, nous allons dire que a est **d'ordre fini**. Sinon, a est **d'ordre infini** et $\langle a \rangle$ sous-groupe cyclique infini. Si a est d'ordre fini, son ordre est le plus petit entier strictement positif m tel que $a^m = e$.

Proposition 1.1.7. *Soit x un élément d'ordre fini n dans un groupe G, et soit k un entier tel que $k = nq + r$, $0 \leq r < n$. Alors*

- $x^k = x^r$;
- $x^k = e \Leftrightarrow r = 0$;
- *Soit s pose* $d = gcd(k, n)$. *Alors l'ordre de* x^k *est* n/d.

Démonstration. Nous avons $x^k = x^{nq+r} = (x^n)^q x^r = ex^r = x^r$. Donc si $x^k = 1$ alors $x^r = 1$. Comme $0 \leq r < n$ et n est l'ordre de x, on conclut que $r = 0$. La démonstration de la dernière partie est un exercice du Feuille 2. □

Proposition 1.1.8. *Soit G un groupe, et $x \in G$ un élément d'ordre fini. Si x est d'ordre n, alors $H = \langle x \rangle$ est un sous-groupe cyclique d'ordre n.*

Démonstration. en exercice □

Morphismes de groupe

Définition 1.1.6. *Soient G et G' deux sous-groupes. Un* ***morphisme de groupe de*** *G* ***dans*** *G' est une application $\phi : G \to G'$ qui vérifie :*

$$\forall (x, y) \in G^2,\ \phi(xy) = \phi(x)\phi(y).$$

Le côté gauche de cette équation signifie :
d'abord multiplier x et y dans G, puis envoyer le produit xy dans G' en applicant ϕ,
et le côté droit signifie :
d'abord envoyer x et y dans G' en applicant ϕ, puis multiplier leur images dans G'.

Exemple 1.1.13. *Soit G un groupe abelien. L'application $\phi : G \to G$ définie par $\phi(x) = x^{-1}$ est un morphisme de groupe. Effectivement, $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$.*

Exemple 1.1.14. *L'application $\phi : \mathbb{C}^* \to \mathbb{R}_+^*$, définie par $\phi(z) = |z|$, est un morphisme de groupe de $(\mathbb{C}^*, \cdot)$ dans $(\mathbb{R}_+^*, \cdot)$. En effet,*

$$\phi(zz') = |zz'| = |z||z'| = \phi(z)\phi(z').$$

Exemple 1.1.15. *L'application $x \mapsto e^x$ est un morphisme de groupe du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{R}_+^*$. Comment on vérifie ça ?*

Voici quelques propriétés immédiates des morphismes de groupes.

Proposition 1.1.9. *Soit G, G' deux groupes et $\phi : G \to G'$ un morphisme de groupe. Alors*

1. *Si e e e' sont les éléments neutres de G et G' respectivement, alors*
$$\phi(e) = e'.$$
2. *Soit $x \in G$. Alors*
$$\phi(x^{-1}) = (\phi(x))^{-1}.$$
3. $\forall n \in \mathbb{Z}$, $\forall x \in G, \phi(x^n) = (\phi(x))^n$.
4. $\forall x_1, x_2, \dots x_n \in G$, $\phi(x_1 x_2 \dots x_n) = \phi(x_1)\phi(x_2)\dots\phi(x_n)$.

Démonstration.

1. Dénote $a = \phi(e) \in G'$. Alors $a = \phi(e) = \phi(ee) = \phi(e)\phi(e) = a^2$. Mais $a = a^2$ implique $a^{-1}a = a^{-1}a^2$, d'où $e' = a$.
2. Nous avons $e' = \phi(e) = \phi(x^{-1}x) = \phi(x^{-1})\phi(x)$. Donc on a montré
$$\phi(x^{-1})\phi(x) = e'.$$
Par la Proposition 1.1.5, $\phi(x^{-1}) = (\phi(x))^{-1}$.
3. par récurrence
4. par récurrence

□

Proposition 1.1.10. *Soitent $\phi : G \to G'$ et $\psi : G' \to G''$ morphismes de groupe. Alors la composée $\psi \circ \phi$ est un morphisme de groupe de G dans G''.*

Démonstration. Pour montrer que $\psi \circ \phi$ est un morphisme de groupe de G dans G'', il faut vérifier

$$\forall x, y \in G,\ (\psi \circ \phi)(xy) = (\psi \circ \phi)(x)\,(\psi \circ \phi)(y).$$

Soit $x, y \in G$. Nous avons

$$\begin{aligned}
&(\psi \circ \phi)(xy) = \\
&\psi(\phi(xy)) \overset{\phi \text{ morphisme}}{=} \psi(\phi(x)\phi(y)) \\
&\overset{\psi \text{ morphisme}}{=} \psi(\phi(x))\,\psi(\phi(y)) \\
&= (\psi \circ \phi)(x)\,(\psi \circ \phi)(y)
\end{aligned}$$

□

Définition 1.1.7. *Soit $\phi : G \to G'$ un morphisme de groupes, déléments neutres e et e', respectivement. Le **noyau** de ϕ est l'ensemble*

$$Ker(\phi) = \{x \in G | \, \phi(x) = e'\}.$$

Proposition 1.1.11. *Soit $\phi : G \to G'$ un morphisme de groupe. Alors*

(a) $Ker(\phi)$ est un sous-groupe de G.

(b) Soit $H < G$. L'image de H par ϕ, $\phi(H) = \{\phi(x) | \, x \in H\}$ est un sous-groupe de G'

(c) Soit $H' < G'$. L'image réciproque de H', $\phi^{-1}(H') = \{x \in G | \, \phi(x) \in H'\}$ est un sous-groupe de G.

Démonstration.

(a) Montrons que $Ker(\phi)$ est un sous-groupe de G. On sait déjà (Proposition 1.1.9) que $\phi(e) = e'$, donc $e \in Ker(\phi)$. Soit $x, y \in Ker(\phi)$. On a

$$\phi(xy) = \phi(x)\phi(y) = e'e' = e',$$

d'où $xy \in Ker(\phi)$. Si $x \in Ker(\phi)$, on a $\phi(x^{-1}) = (\phi(x))^{-1} = e'$, donc $x^{-1} \in Ker(\phi)$.

(b) Soit $H < G$. Montrons que $\phi(H)$ est un sous-groupe de G'. D'abord, comme H est une sous-groupe de G, $e \in H$. Donc $e' = \phi(e) \in \phi(H)$. Si $x', y' \in \phi(H)$, il existe x et y dans H tels que $\phi(x) = x'$ et $\phi(y) = y'$. Donc $\phi(xy) = \phi(x)\phi(y) = x'y'$, d'où $x'y' \in \phi(H)$. Finalement, montrons que $(x')^-1 \in \phi(H)$. Comme $\phi(x) = x'$, $\phi(x^{-1}) = (\phi(x))^{-1} = (x')^{-1}$ et donc $(x')^{-1} \in \phi(H)$.

(c) Exercice du Feuille TD 3.

□

Nous allons dire que le noyau $Ker(\phi)$ est trivial si $Ker(\phi) = \{e\}$.

Proposition 1.1.12. *Si le noyau d'un morphisme de groupe $\phi : G \to G'$ est trivial, alors ϕ est injective.*

Démonstration. On note e et e' les éléments neutres de G et G' respectivement. Si $\phi(x) = \phi(y)$, en multipliant à droite par $(\phi(x))^{-1}$ et on obtient $\phi(x)(\phi(x))^{-1} = \phi(x)(\phi(x))^{-1}$. Comme $(\phi(x))^{-1} = \phi(x^{-1})$, on a $\phi(x)\phi(x^{-1}) = \phi(y)\phi(x^{-1})$, et par la définition de morphisme on a $\phi(xx^{-1}) = \phi(yx^{-1})$, d'où $\phi(yx^{-1}) = \phi(xx^{-1}) = e'$. Donc $yx^{-1} \in Ker(\phi)$ et comme le noyau est trivial, $yx^{-1} = e$, d'où $y = x$. □

Définition 1.1.8. *Soit $\phi : G \to G'$ un morphisme de groupe. Nous allons dire que ϕ est un* ***isomorphisme de groupe*** *s'il existe un morphisme de groupe $\psi : G' \to G$ tel que $\phi \circ \psi = Id_{G'}$ et $\psi \circ \phi = Id_G$, où Id_G et $Id_{G'}$ sont les applications identité de G et G', respectivement.*

Nous allons écrire

$$G \approx G'$$

et dire que G est isomorphe à G' s'il existe un isomorphisme $\phi : G \to G'$.

Lemme 1.1.1. *Si $\phi : G \to G'$ est un isomorphisme de groupe, alors son inverse ϕ^{-1} est un isomorphisme $G' \to G$.*

Démonstration. En exercice □

Donc $G \approx G'$ est equivalent à $G' \approx G$.

Exemple 1.1.16. *L'application $x \mapsto e^x$ est un isomorphisme de groupe de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*)$.*

Exemple 1.1.17. *Soit G un groupe commutatif. L'application $\phi : x \mapsto x^{-1}$ est un isomorphisme de G dans G.*

Proposition 1.1.13. *Soit $\phi : G \to G'$ un morphisme de groupe. Si ϕ est bijective, alors ϕ est un isomorphisme.*

Démonstration. □

Théorème 1.1.2. *Soit $\phi : G \to G'$ un morphisme de groupes.*

1. *Si $Ker(\phi)$ est trivial, alors ϕ est un isomorphisme de G dans $\phi(G)$.*
2. *Si ϕ et $Ker(\phi)$ est trivial, alors ϕ est un isomorphisme.*

Démonstration.

1. Nous avons montré que ϕ est injective si $Ker(\phi)$ est trivial. Comme $\phi : G \to \phi(G)$ est surjective, d'apreès la Proposition 1.1.13, ϕ est isomorphisme de G dans $\phi(G)$.
2. Même raisonnement. $Ker(\phi) = \{e\}$, donc ϕ est injective. De plus, ϕ est surjective, donc c'est une bijection et par la Proposition 1.1.13

   $$\phi : G \to G'$$

   est un isomorphisme.

□

Nous allons maintenant démontrer que tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.

Théorème 1.1.3. *Soit G un groupe. Il existe un ensemble E tel que $G \approx H$ pour un sous-groupe $H < S_E$.*

Démonstration. Pour $a \in G$ arbitraire, on définit une application $T_a : G \to G$ par

$$x \mapsto ax.$$

Montrons que T_a est une bijection. En effet, si $T_a(x) = T_a(y)$, alors $ax = ay$ et en multipliant à gauche par a^{-1}, on voit que $x = y$ et que T_a est injective. Pour $y \in G$, soit $x = a^{-1}y$, alors $T_a(x) = aa^{-1}y = y$, d'où T_a est surjective. Donc T_a est une bijection de G dans G et donc $T_a \in S_G$. Montrons que l'application $a \mapsto T_a$ est un morphisme de groupe. On voit facilement que $T_{ab}(x) = abx = T_aT_b(x)$ pour tout $x \in G$. Ce morphisme est injective : Si $a \in Ker(\phi)$ alors $T_a = Id_G$, mais dans ce cas là $a = e$. Donc on a un morphisme de groupe $G \to S_G$ dont le noyau est trivial. Alors

$$G \approx \phi(G)$$

et $\phi(G) < S_G$. □

Si ϕ est un isomorphisme de groupe **de G dans G**, on dit que ϕ est un **automorphisme** de G. Par exemple, l'application identité $Id : G \to G$, $Id(x) = x$, est un automorphisme de groupe.

Un exemple très important d'un automorphisme de groupe est conjugaison.

Définition 1.1.9. *Soit G un groupe et $a \in G$. Soit $\phi_a : G \to G$ l'application définie par*

$$x \to axa^{-1}.$$

*Cette application est appelée **conjugaison par** a.*

Montrons que ϕ_a est un automorphisme de G. Pour $x, y \in G$, on a

$$\phi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$$

donc ϕ_a est un morphisme de groupe. Si $axa^{-1} = e$, on a $ax = a$ d'où $x = e$. Donc $Ker(\phi)$ est trivial. Soit $y \in G$, on a

$$y = a(a^{-1}ya)a^{-1} = \phi(a^{-1}ya).$$

Ca montre que ϕ est surjective. Par le Théorème 1.1.2, ϕ est isomorphisme $G \to G$ et donc, automorphisme.

Rappelons que $S(E)$ est le groupe de bijections de E.

Définition 1.1.10. *Soit G un groupe. Notons $Aut(G)$ l'ensemble d'automorphismes de G.*

Lemme 1.1.2. *$Aut(G)$ est un sous-groupe du groupe symétrique S_G, où la LCI est la composition des applications.*

Démonstration. □

Classe suivant un sous-groupe. Sous-groupes distingués

Nous aurons besoin d'une notation suivante. Soit G un groupe et S, S' deux sous-ensembles non-vides de G. S et S' ne sont pas forcement des sous-groupes de G. On définie le produit SS' par

$$SS' = \{xx' |\ x \in S, x' \in S'\}.$$

Voici quelques propriétés dont on aura besoin.

Lemme 1.1.3. • *Si H est un sous-groupe de G, alors $HH = H$;*

- *Si $H < G$ et S un sous-ensemble non-vide de H, alors $SH = H$;*
- *Si S_1, S_2, S_3 sont des sous-ensembles non-vides de G, alors*
  a) $(S_1S_2)S_3 = S_1(S_2S_3)$.
  b) $(S_1 \cup S_2)S_3 = S_1S_3 \cup S_2S_3$.

Démonstration. en exercice □

Définition 1.1.11. *Soit G un groupe et $H < G$ un sous-groupe. Soit a un élément de G. L'ensemble*

$$aH = \{ah |\ h \in H\}$$

est appellé la ***classe à gauche de*** *a* ***suivant*** *H.*

Remarque 1. *Les classes à gauche suivant un sous-groupe H sont les classes d'équivalence de la rélation*

$$x \sim y \text{ si } x = yh \text{ pour un } h \in H.$$

Vérifier que c'est bien une relation d'équivalence !

Le théorème suivant dit que deux classes à gauches suivant un sous-groupe sont égaux ou disjoints.

Théorème 1.1.4. *Soit G un groupe, $H < G$, et $a, b \in G$. Si $aH \neq bH$, alors $aH \cap bH = \emptyset$.*

Démonstration. Supposons que $aH \cap bH \neq= \emptyset$. Donc il existe un élément x tel que $x \in aH$ et $x \in bH$. Alors on peut écrire $x = ah_1$ et $x = bh_2$ où h_1 et h_2 sont dans H. Donc $ah_1 = bh_2$. Comme $H = h_1H$ et $H = h_2H$ (Lemme 1.1.3), on a $aH = ah_1H$ et $bH = bh_2H$. Mais $ah_1 = bh_2$ et donc $ah_1H = bh_2H$ d'où $aH = bH$. □

Soit G un groupe fini et $H < G$, alors tout élément $x \in G$ est contenu dans un unique (d'après le Théorème 1.1.4) classe à gauche suivant H, $x \in xH$. Ca implique qu'on a une **décomposition de G en classes à gauche suivant** H :

$$G = \cup_{i=1}^{r} a_i H$$

où les classes $a_1H, a_2H, \ldots, a_rH$ sont tous distincts. On dit aussi que tout elément $a_ih \in a_iH$ est un **représentant** de classe a_iH. Maintenant nous allons voir que si G est un groupe et H un sous-groupe fini, alors les classes à gauche suivant H ont le même nombre d'éléments.

Théorème 1.1.5. *Soit G un groupe, H un sous-groupe fini de G et $a \in G$. Le nombre d'éléments de aH est $|H|$.*

Démonstration. On considère $f : H \to aH$ définie par $f(x) = ax$. Il suffit de montrer que f est une bijection. En effet, si $ax = ay$, alors $a^{-1}ax = a^{-1}ay$ et donc $x = y$. Ca implique que f est injective. Soit $y \in aH$, alors $y = ah$ pour un $h \in H$. On a $f(h) = ah = y$, et donc f est surjective. Nous avons montré que f est un bijection entre H et aH, et donc les deux ensembles ont le méme nombre d'éléments. □

Notons G/H l'ensemble de classes à gauche suivant H. Le nombre déléments dans G/H est **l'indice de H dans G**. L'indice peut être fini ou infini. Mais si G est un groupe fini, alors l'indice de tout sous-groupe dans G est fini. On dénote l'indice de H dans G par $(G : H)$. L'ordre de G est l'indice du sous-groups trivial dans G.

Théorème 1.1.6. *Soit G un groupe fini et H un sous-groupe de G. Alors*

1. *$|G| = (G : H) \cdot |H|$;*
2. *(Théorème de Lagrange) L'ordre d'un sous-groupe divise l'ordre de G ;*
3. *Soit $a \in G$. L'ordre de a dans G divise l'ordre de G ;*

4. Si $K < H < G$, alors

$$(G : K) = (G : H)(H : K)$$

Démonstration. 1. Comme $G = \cup_{i=1}^{r} a_i H$ où $a_i H$ sont des classes à gauche suivant H tels que $a_i H \cap a_j H = \emptyset$ si $i \neq j$, on a $|G| = \sum_{i=1}^{r} |a_i H| = r|H|$. r est exactement le nombre de classes distincts, i.e. $r = (G : H)$.

2. Comme $(G : H)$ est un nombre naturel, $|H|$ divise $|G|$
3. L'ordre d'un élément $a \in G$ est l'ordre du sous-groupe cyclique $\langle a \rangle$.
4. Nous avons $|G| = (G : H)|H|$, $|H| = (H : K)|K|$ et $|G| = (G : K)|K|$ d'où
$$(G : K) = \frac{|G|}{|K|} = \frac{(G : H)|H|}{|K|} = (G : H)(H : K).$$

□

Exemple 1.1.18. *Soit G un groupe d'ordre $p > 1$ où p est un nombre premier, et soit $a \in G$ avec $a \neq e$. Alors G est cyclique et $G = \langle a \rangle$.*

Ce **n'est pas vrai** en général que si G est un groupe fini et d est un diviseur de $|G|$, alors il existe $H < G$ avec $|H| = d$. Trouver un contre-exemple ? Voici quelques converses partielles :

Théorème 1.1.7. *(Sylow) Soit G un groupe fini d'ordre $p^\alpha m$ où p est un nombre premier et m n'est pas un multiple de p. Alors il existe un sous-groupe $H < G$ avec $|H| = p^\alpha$.*

Démonstration. Nous allons admettre ce théorème. □

Théorème 1.1.8. *(Cauchy) Soit G un groupe fini et p un nombre premier tel que p divise $|G|$. Alors il existe un élément $x \in G$ d'ordre p. (Autrement dit, il existe un sous-groupe cyclique $H < G$ d'ordre p)*

Démonstration. On peut démontrer ce théorème un utilisant le théorème de Sylow. Comme p divise $|G|$, on écrit $|G| = p^\alpha m$, où $\alpha, m \in \mathbb{N}^*$ et p ne divise pas m. Par le Théorème de Sylow, il existe un sous-groupe $H < G$ d'ordre p^α. Si $x \in H$ un élément different de e, alors l'ordre de x divise p^α et donc $|x| = p^\beta$ avec $1 \leq \beta \leq \alpha$. Si $\beta = 1$, alors $|x| = p$ et on s'arrete là. Si $\beta \geq 2$, on a $K = \langle x \rangle$ un sous-groupe cyclique d'ordre p^β. Soit $y = x^{p^{\beta-1}}$. D'après un exercice de la feuille 2, y est d'ordre p.

□

Nous avons défini les classes à gauche suivant un sous-groupe. De la même façon on peut définir les classes à droite : si $H < G$ et $a \in G$ la classe à droite de a suivant H est l'ensemble

$$Ha = \{ha|\ h \in H\}.$$

Nous n'allons pas vraiment travailler avec les classe à droite.

Définition 1.1.12. *Soit G un groupe. On dit que H est un sous-groupe distingué si on a :*

$$\forall x \in G,\ xH = Hx.$$

Autrement dit, H est un sous-groupe distingué si $\forall x \in G$, $xHx^{-1} = H$.

$xH = Hx$ ou $H = xHx^{-1}$ signifie que pour tout $h \in H$, le conjugué de h par x appartient à H : $xhx^{-1}H$.

Exemple 1.1.19. *Si G est abélien, alors $xH = Hx$ pour tout sous-groupe H et $x \in G$. Donc tout sous-groupe dans un groupe abélien est distingué.*

Exemple 1.1.20. *$G = GL(2, \mathbb{R})$. Le sous-groupe U des matrices triangulaires supérieures n'est pas distingués dans G. Le sous-groupe $H = SL(2, \mathbb{R})$ est distingué dans G.*

Proposition 1.1.14. *Soit G un groupe et H un sous-groupe de G. Alors H est un sous-groupe distingué s'il existe un morphisme de groupe $\phi : G \to G'$ tel que $H = Ker(\phi)$.*

Démonstration. Soit $\phi : G \to G'$ un morphisme de groupe tel que $H = Ker(\phi)$, et $x \in G$. Alors pour tout $h \in H$, on a $\phi(xhx^{-1}) = \phi(x)\phi(h)\phi(x^{-1}) = e'$, et donc $xHx^{-1} \subset H$ pour tout $x \in G$. En particulier, $x^{-1}Hx \subset H$. En multipliant à gauche par x et à droite par x^{-1} on obtient l'inclusion $H \subset xHx^{-1}$. □

Nous avons montré que si H est le noyau d'un morphisme de G dans un groupe, alors H est un sous-groupe distingué. En fait c'est une condition nécessaire et nous allons maintenant montrer qu'un sous-groupe distingué est toujours le noyau d'un morphisme de groupe.

Théorème 1.1.9. *Soit G un groupe et H un sous-groupe distingué. Si aH et bH sont des classes à gauche suivant H, alors le produit $(aH)(bH) = \{ah_1bh_2|\ h_1, h_2 \in H\}$ est aussi une classe à gauche suivant H. L'ensemble G/H des classes à gauche suivant H, muni de cette loi de composition, est un groupe.*

Démonstration. Soit $a, b \in G$. Alors le produit $(aH)(bH) = a(Hb)H = a(bH)H = abH$. Ca montre que le produit de deux classes à gauche suivant H est une clase à gauche. La classe $eH = H$ est l'élément neutre :

$$aHeH = aHH = H.$$

Finalement, on a $(aH)(a^{-1}H) = a(Ha^{-1})H = a(a^{-1}H)H = eHH = H$, et donc $a^{-1}H$ est l'inverse de aH. Nous avons montré que G/H est un groupe. □

Le groupe G/H dans le théorème précedant est applelé le **le groupe quotient de G par H** ou G **modulo** H.

Exemple 1.1.21. *$G = \mathbb{R}$ un groupe additif, $H = \mathbb{Z}$. Le groupe quotient $\mathbb{R}/\mathbb{Z}$ est isomorphe au cercle $S^1 = \{z \in \mathbb{C} | \ |z| = 1\}$ (L'application $\phi : G/H \to S^1$ définie par $\phi : \phi(x) = e^{2\pi xi}$ est un isomorphisme).*

Exemple 1.1.22. *Si $G = GL(2, \mathbb{R})$ et $H = SL(2, \mathbb{R})$, le groupe quotient G/H est isomorphe à $\mathbb{R}^*$. (rappel : $det(AB) = det(A)det(B)$. $\phi : G/H \to \mathbb{R}^*$ défini par $\phi(AH) = det(A)$ est un isomorphisme)*

Corollaire 1.1.1. *Soit G un groupe et H un sous-groupe distingué. Soit G/H le groupe quotient de G par H et*

$$\phi : G \to G/H$$

définie par $\phi(x) = xH$. Alors ϕ est un morphisme de groupe et $Ker(\phi) = H$.

Démonstration. Soit $a, b \in G$, alors $\phi(ab) = abH = aHbH = \phi(a)\phi(b)$, donc ϕ est un morphisme de groupe. Montrons que $Ker(\phi) = H$. Si $x \in Ker(\phi)$, montrons que $x \in H$. On a $\phi(x) = H$. Ca signifie que $xH = H$. Alors $xh \in H$ pour tout $h \in H$. En particulier, $xe \in H$, d'où $x \in H$. On a aussi $H \subset Ker(\phi)$, parce que pour tout $h \in H$, $\phi(h) = hH = H$. Donc $H = Ker(\phi)$. □

On appel ϕ le morphisme canonique de G dans G/H. La Proposition 1.1.14 et le Corollaire 1.1.1 impliquent que $H < G$ est distingué si et seulement si il existe un morphisme ϕ de groupe de G dans un groupe G' tel que $H = Ker(\phi)$.

Proposition 1.1.15. *Soit $f : G \to G'$ un morphisme de groupe et $H = Ker(f)$. Soit $a' \in G'$ un élément de G' qui est dans l'image $f(G)$ et $a \in G$ tel que $f(a) = a'$. Alors*

$$f^{-1}(a') = \{x \in G | f(x) = a'\} = aH.$$

Démonstration. Si $b \in aH$ alors $b = ah$ et $f(b) = f(ah) = f(a)f(h) = a'e' = a'$, donc $aH \subset f^{-1}(a')$. Si $b \in f^{-1}(a')$, alors écrivons $b = aa^{-1}b$ et montrons que $a^{-1}b \in H$. $f(a^{-1}b) = f(a^{-1})f(b) = (f(a))^{-1}f(b) = (a')^{-1}a' = e'$. Alors $b \in aH$. □

Si $f : G \to G'$ est un morphisme de groupe et $H = Ker(\phi)$, on vient de montrer que $f(x) = f(y)$ si et seulement si x et y sont dans la même classe à gauche suivant H. En particulier, f est constant sur les classe à gauche. On peut alors noter $f(xH) = f(x)$.

Notons aussi $Imf = f(G)$.

Théorème 1.1.10. *(Premier Théorème d'Isomorphisme) Soit $f : G \to G'$ un morphisme de groupe. Soit $H = Ker(f)$. L'application $xH \mapsto f(xH)$ est un isomorphisme*

$$G/H \to Imf$$

entre G/H et l'image de f.

Démonstration. Notons $\bar{f}$ l'application de G/H dans G' définie par $\bar{f}(xH) = f(xH)$. D'après le Théorème 1.1.2, il faut vérifier

1. $\bar{f}$ est un morphisme de groupe ; En effet, $\bar{f}((aH)(bH)) = \bar{f}(abH) = f(abH) = f(ab) = f(a)f(b) = f(aH)f(bH) = \bar{f}(aH)\bar{f}(bH)$.
2. $\bar{f}$ est injectif ; Si $\bar{f}(aH) = \bar{f}(bH)$, alors $f(aH) = f(bH)$ et donc $f(a) = f(b)$, d'où $aH = bH$.
3. $Imf = Im\bar{f}$. en exercice

□

Groupes cycliques

Un des premiers exemples que nous avons consideré était le groupe additif des entiers $\mathbb{Z}$. C'est un groupe cyclique infini, $\mathbb{Z} = \langle 1 \rangle$. Comme $\mathbb{Z}$ est abélien, tout son sous-groupe est distingué et on peut considérer le groupe quotient correspondant. Les sous-groupes de $\mathbb{Z}$ sont $\{n\mathbb{Z} | \, n \in \mathbb{N}\}$.

Fixons $n \in \mathbb{N}^*$ et considérons $\mathbb{Z}/n\mathbb{Z}$. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont les classes à gauche $0 + \mathbb{Z}, 1 + \mathbb{Z}, 2 + \mathbb{Z}, \ldots$. Comme $x + n + \mathbb{Z} = x + \mathbb{Z}$, il y a exactement n éléments dans $\mathbb{Z}/n\mathbb{Z}$. On les notes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$, où $\bar{k}$ est la classe $k + \mathbb{Z}$. Comme $\overline{a+b} = \bar{a} + \bar{b}$ (vérifier !), on voit facilement que $\bar{k} = k \cdot \bar{1}$, et donc $\mathbb{Z}/n\mathbb{Z}$ est cyclique et $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$.

Si $n = 0$, le sous-groupe $0\mathbb{Z} = \{0\}$. Par définition, $x \in y + 0\mathbb{Z}$ si $-y + x \in 0\mathbb{Z}$. Donc x et y sont dans la même classe si et seulement si $x = y$. Donc le morphisme canonique $\phi : \mathbb{Z} \to \mathbb{Z}/0\mathbb{Z}$ est un isomorphisme.

Soit G un groupe cyclique et a un générateur. On considère une application

$$\phi : \mathbb{Z} \to G$$

définie par $\phi(k) = a^k$. C'est un morphisme surjectif. (Vérifier !) Le noyau de ϕ est un sous-groupe de $\mathbb{Z}$, donc il existe un unique $n \in \mathbb{N}$ tel que $Ker(\phi) = n\mathbb{Z}$. Par le Premier Théorème d'Isomorphisme, G est isomorphe à $Z/n\mathbb{Z}$.

Théorème 1.1.11. *Soit G_1 et G_2 deux groupes cycliques d'ordre d. Alors $G_1 \approx G_2$. Si $a_1 \in G_1$ et $a_2 \in G_2$ générateurs de G_1 et G_2, respectivement, alors il existe un unique isomorphisme $\phi : G_1 \to G_2$ tel que*

$$\phi(a_1) = a_2.$$

Démonstration. D'après la remarque précédant le théorème il existent ϕ_1 et ϕ_2 des isomorphismes de $\mathbb{Z}/d\mathbb{Z}$ dans G_1 et G_2, tels que

$$\phi_1(k + d\mathbb{Z}) = a_1^k \text{ et } \phi_2(k + d\mathbb{Z}) = a_2^k.$$

Alors $h = \phi_2 \circ \phi_1^{-1} : G_1 \to G_2$ est un isomorphisme tel que $h(a_1) = a_2$.

Si $g : G_1 \to G_2$ est un autre isomorphisme tel que $g(a_1) = a_2$, alors pour tout $k \in \mathbb{Z}$, $h(a_1^k) = g(a_1^k) = a_2^k$ et donc $h = g$.

□

Les générateurs ne sont pas en général uniques. La proposition suivante nous dit exactement quels éléments engendrent un groupe cyclique.

Proposition 1.1.16. *Soit G un groupe cyclique d'ordre n. Un élément $a \in G$ est un générateur de G, $G = \langle a \rangle$, si et seulement si $|a| = n$. Si $G = \langle a \rangle$, alors a^k engendre G ssi $pgcd(k, n) = 1$.*

Démonstration. Si $a \in G$ est d'ordre n, alors le groupe $H = \langle a \rangle$ est un sous-groupe de G, et $|H| = n$. Donc $G = H$, d'òu $G = \langle a \rangle$.

Si a est un gén'érateur de G, l'ordre de a est l'ordre de G, donc $|a| = n$.

Soit $k \in \mathbb{Z}^*$. On a vu en TD que l'ordre de a^k est $\frac{n}{pgcd(n,k)}$. Donc a^k engendre G si et seulement si $pgcd(n, k) = 1$. □

Groupes Symétriques

Soit $n \in \mathbb{N}^*$. On rappelle que S_n est l'ensemble des bijections de l'ensemble $\{1, 2, \ldots, n\}$ dans lui-même. Un élément σ de S_n est une **permutation** et on peut le représenter sous la forme

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

On a montré que S_n est un groupe avec LCI composition des applications, et que $|S_n| = n!$. Nous avons déjà vu que S_3 n'est pas abélien. En fait S_n n'est pas abélien pour tout $n \geq 3$.

Proposition 1.1.17. *Le groupe symétrique S_n n'est pas abélien si $n \geq 3$.*

Démonstration. Il suffit de trouver deux éléments qui ne commutent pas. Par exemple, soit

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 3 & 2 & \dots & n \end{pmatrix}.$$

Un calcule simple montre que $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$. □

Définition 1.1.13. *Une **transposition** est une permutation qui échange deux éléments distincts et qui laisse tous les autres éléments inchangés. Plus précisement, $\sigma \in S_n$ est une transposition si $\exists\, i, j$ tels que $i \neq j$, avec $\sigma(i) = j$, $\sigma(j) = i$ et $\sigma(k) = k$ pour tout $k \neq i, j$.*

On remarque que les transpositions sont d'ordre 2. Nous allons montrer que les transpositions engendrent S_n.

Proposition 1.1.18. *Tout élément $\sigma \in S_n$ est un produit des transpositions.*

Démonstration. Par récurrence. On vérifie facilement que l'enoncé est vrai pour $n = 2$. Supposons qu'il est vrai pour $n = k - 1$ est montrons le pour $n = k$. Soit $\sigma \in S_k$. Notons $m = \sigma(k)$. Soit σ_1 la permutation qui échange m et k et qui laisse les autres éléments inchangés. On pose $\sigma' = \sigma_1 \circ \sigma$, et on note tout de suite que $\sigma = \sigma_1 \circ \sigma'$. En suite on note que $\sigma'(k) = k$ et donc on peut considérer σ' comme une permutation dans S_{k-1}. Donc par l'hypothèse, σ' est un produit des transpositions, et comme $\sigma = \sigma_1 \circ \sigma'$, σ l'est aussi. □

Définition 1.1.14. *Soit k en entier t.q. $k \geq 2$. Un k-cycle (ou un cycle) est une permutation σ telle que il existe des éléments distincts $i_1, i_2, \dots, i_k$ tels que σ envoie i_1 sur i_2, i_2 sur i_3, etc., et enfin i_k sur i_1, et laisse tous les autres éléments inchangés. On dénote un tel cycle $(i_1 i_2 \dots i_k)$. L'ensemble $\{i_1, i_2, \dots, i_k\}$ est le **support** de $(i_1 i_2 \dots i_k)$.*

Par exemple $(1\,3\,4)$ dans S_5 est une permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}.$$

Les transpositions sont des 2-cycles.

Proposition 1.1.19. *Soit $k \geq 2$. Un k-cycle est d'ordre k.*

Deux cycles $(i_1 i_2 \dots i_k)$ et $(j_1 j_2 \dots j_l)$ sont à supports disjoints si $i_a \neq j_b$ pour tous $1 \leq a \leq k$ et $1 \leq b \leq l$.

Proposition 1.1.20. *Soit $\sigma \in S_n$, $\sigma \neq e$. Alors σ peut être écrit comme un produit des cycles à supports deux-a-deux disjoints.*

Proposition 1.1.21. *Deux cycles à support disjoint commutent.*

Démonstration. En exercice(voir Feuille TD 6). □

Signature d'une permutation Nous avons vu que toute permutation est un produit de transpositions. En général il y a plusieurs façons de factoriser une permutation en transpositions. Par exemple, $(123) = (23) \circ (13) = (13) \circ (12) = (23) \circ (12) \circ (13) \circ (23)$. Mais nous allons voir que le nombre de transpositions dans la factorisation est toujours pair ou toujours impair.

Soit $x_1, x_2, \dots, x_n$ des variables indépendentes. On définit un polynôme

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Par exemple, si $n = 4$, on a

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Si $\sigma \in S_n$, on définit

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Par exemple, si $n = 4$ et $\sigma = (1234)$, on obtient

$$\Delta = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = -\Delta.$$

Ce qu'il faut remarquer est que, si $i < j$ et donc $(x_i - x_j)$ est un facteur de Δ, alors soit $(x_i - x_j)$ soit $-(x_i - x_j)$ est dans $\sigma(\Delta)$. Justifions ça. En effet, σ est une bijection est on pose $i' := \sigma^{-1}(i)$ et $j' := \sigma^{-1}(j)$ Si $i' < j'$ alors $(x_{i'} - x_{j'})$ est un facteur de Δ, est donc $(x_i - x_j)$ est un facteur de $\sigma(\Delta)$. Si $j' < i'$, on a $(x_j - x_i) = -(x_i - x_j)$ un facteur de $\sigma(\Delta)$. Ca implique que $\sigma(\Delta)$ a les mêmes facteurs au signe près et donc

$$\sigma(\Delta) = \pm\Delta.$$

Nous avons presque démontré le théorème suivant

Théorème 1.1.12 (Signature d'une permutation)**.** *Soit $n \in N^*$. A tout élément $\sigma \in S_n$ on peut associer une signature* 1 *ou* -1*, notée $\epsilon(\sigma)$, telle que :*

(i) Si $\sigma \in S_n$ est un transposition, alors $\epsilon(\sigma) = -1$.

(ii) Si $\sigma, \sigma' \in S_n$ alors, $\epsilon(\sigma \circ \sigma') = \epsilon(\sigma)\epsilon(\sigma')$. Autrement dit, $\epsilon : S_n \to \{1,_1\}$ est un morphisme de groupe.

Démonstration. On pose

$$\epsilon(\sigma) = \begin{cases} 1 & \sigma(\Delta) = \Delta \\ -1 & \sigma(\Delta) = -\Delta \end{cases}$$

Comme $(\sigma \circ \sigma')(\Delta) = \sigma(\sigma'(\Delta))$, on voit que $\epsilon(\sigma \circ \sigma') = \epsilon(\sigma)\epsilon(\sigma')$. Si $\sigma \in S_n$ est une transposition, $\sigma = (k\, m)$, $(k < m)$, montrons que $\epsilon(\sigma) = -1$.

C'est techniquement difficile et pour commencer nous allons montrer que la signature de $\sigma = (1\, 2)$ est -1.

$$\sigma(\Delta) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \tag{1.1}$$

$$= \prod_{1 < j \le n} (x_{\sigma(1)} - x_{\sigma(j)}) \prod_{2 < j \le n} (x_{\sigma(2)} - x_{\sigma(j)}) \prod_{3 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) \tag{1.2}$$

$$= (x_2 - x_1) \prod_{3 \le j \le n} (x_2 - x_j) \prod_{2 < j \le n} (x_1 - x_j) \prod_{3 \le i < j \le n} (x_i - x_j) \tag{1.3}$$

$$= - \prod_{2 \le j \le n} (x_1 - x_j) \prod_{3 \le j \le n} (x_2 - x_j) \prod_{3 \le i < j \le n} (x_i - x_j) = -\Delta \tag{1.4}$$

d'où $\epsilon((1,2)) = -1$. En suite notons que pour tout $k \ge 2$, $(1\, k) = (2\, k)(1\, 2)(2\, k)$ et $(m\, k) = (1\, m)(1\, k)(1\, m)$, d'où

$$(m\, k) = (1\, m)(2\, k)(1\, 2)(2\, k)(1\, m).$$

La signature de $(m\, k)$ est

$$\epsilon(m\, k) = \epsilon(1\, m)\epsilon(2\, k)\epsilon(1\, 2)\epsilon(2\, k)\epsilon(1\, m) = \epsilon^2(1\, m)\epsilon^2(2\, m)\epsilon(1\, 2) = -1.$$

□

Exemple 1.1.23. *Soit $n \in \mathbb{N}^*$. Notons $A_n = Ker(\epsilon)$. A_n est l'ensemble des permutations de signature* 1*. C'est un sous-groupe de S_n, appelé* ***le groupe alterné.*** *C'est un sous-groupe distingué de S_n, parce que A_n est le noyau d'un morphisme. Combien d'éléments y-a-t-il dans A_n ? D'après le Premier Théorème d'Isomorphisme, le groupe quotient S_n/A_n est isomorphe à un groupe*

d'ordre 2, $S_n/A_n \approx \epsilon(S_n) = \{1, -1\}$*, et donc il y a exactement deux classes à gauche suivant* A_n*, i.e. l'indice de* A_n *dans* S_n *est* $(S_n : A_n) = 2$*. Comme* $|S_n| = (S_n : A_n)\,|A_n|$*, on a trouvé que* $|A_n| = n!/2$*.*

Nous allons maintenant montrer que le converse du Théorème de Lagrange est faux. Plus précisement, nous allons montrer que

$$(d \text{ un diviseur de } |G|) \not\Rightarrow (d \text{ et l'ordre d'un sous-groupe de } G).$$

Nous allons dire qu'un groupe G est **simple** si les seuls sous-groupes distingués de G sont G et $\{e\}$.

Proposition 1.1.22. *Pour tout* $n \geq 5$*, le groupe alterné* A_n *est simple.*

A_n pour $n \geq 5$ n'ont pas de sous-groupes d'ordre $|A_n|/2$. En effet, tout sous-groupe H de G d'indice 2 est distingué (Feuille 5). Mais A_n sont simples (pour $n \geq 5$), et donc n'ont pas de sous-groupes distingués autres que A_n et $\{Id\}$. Par exemple, il n'y a pas de sous-groupe d'ordre 30 dans A_5 (qui est d'ordre 60).

Actions de groupe.

Soit G un groupe et E un ensemble. Une **action** de G sur E est une application de $G \times E$ dans E, qui envoie un pair $(a, x) \in G \times E$ sur un élément de E noté $a \cdot x$, et qui satisfait les propriétés suivantes :

1. Si e est l'élément neutre de G, alors $e \cdot x = x$ pour tout $x \in E$.
2. Pour tous $a, b \in G$ et $x \in E$, nous avons

$$a \cdot (b \cdot x) = (ab) \cdot x.$$

On dit aussi que G **agit** sur E (ou que G opère sur E).

Une action $G \times E \to E$ définit un morphisme $G \to S_E$. En effet, $\forall a \in G$ l'action donne une application $\pi_a : E \to E$ définie par $\pi_a(x) = a \cdot x$. Montrons que π_a est une bijection. $\pi_{a^{-1}}$ est aussi une application $E \to E$.

$$\pi_{a^{-1}} \circ \pi_a(x) = \pi_{a^{-1}}(\pi_a(x)) = a^{-1} \cdot (a \cdot x) \overset{(2)}{=} (a^{-1} \circ a) \cdot x = e \cdot x \overset{(1)}{=} x,$$

et donc $\pi_{a^{-1}} \circ \pi_a = Id_E$. De la même façon on justifie $\pi_a \circ \pi_a = Id_E$. Donc π_a est une bijection.

Enfin, soit $a, b \in G$, on a

$$\pi_{ab}(x) = (ab) \cdot x \overset{(2)}{=} a \cdot (b \cdot x) = \pi_a(\pi_b(x)) = (\pi_a \circ \pi_b)(x)$$

ce qui montre que $a \mapsto \pi_a$ est un morphisme de groupe.

Réciproquement, un morphisme $G \underset{a\mapsto\pi_a}{\to} S_E$ définit une application

$$G \times E \underset{(a,x)\mapsto a\cdot x}{\to} E,$$

où $a \cdot x := \pi_a(x)$. Cette application satisfait les propriétés (1) et (2) et donc est une action de G sur E. (Vérifier !)

Conclusion : Pour tout groupe G et l'ensemble E, l'ensemble des actions de G sur E est en bijection avec l'ensemble des morphismes $G \to S_E$.

Voici quelques exemples :

Exemple 1.1.24. *Tout groupe G agit sur un ensemble arbitraire E par $(a, x) \mapsto x$. C'est à dire, $\pi_a = Id_E$ pour tout $a \in G$. Une telle action s'appelle **triviale**.*

Exemple 1.1.25. *$G = GL(2, \mathbb{R})$, $E = \mathbb{R}^2$. Une application $G \times \mathbb{R}^2 \to \mathbb{R}^2$ définie par*

$$(A, \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}) \mapsto A \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

est une action de G sur $\mathbb{R}^2$.

Exemple 1.1.26. *Un groupe G agit sur lui-même de deux manières fondamentales :*

1. *Translation : $G \times G \to G$, $(a, b) \mapsto ab$ est une action par des translations à gauche.*
2. *Conjugaison : $G \times G \to G$, $(a, b) \mapsto aba^{-1}$ est une action par conjugaison.*

Le **noyau** d'une action $G \times E \to E$ est $\{a \in G | a \cdot x = x, \forall x \in E\}$. C'est l'ensemble de tous les éléments de G qui sont envoyé sur Id_E par le morphisme $G \to S_E$. En particulier, **le noyau d'une action est un sous-groupe distingué de G.**

Soit $x \in E$. Notons $G_x = \{a \in G | \, a \cdot x = x\}$ l'ensemble de tous les éléments de G qui fixent x. On appelle G_x le **stabilisateur** de x dans G.

Lemme 1.1.4. *$G_x < G$.*

Démonstration. en exercice □

Exemple 1.1.27. *Le groupe symétrique $G = S_n$ agit naturellement sur l'ensemble $E = \{1, 2, \ldots, n\}$. On rappelle que G est d'ordre $n!$ Soit $k \in E$. Le stabilisateur de k dans G est*

$$G_x = \{\sigma \in G | \sigma(x) = x\}.$$

G_x est isomorphe à S_{n-1} (pourquoi ?) et donc $|G_x| = (n-1)!$. Alors l'indice de G_x dans G est n.

Définition 1.1.15. *Soit $G \times E \to E$ une action et $x \in E$. L'ensemble*

$$G(x) = \{a \cdot x \in E | a \in G\} \subset E$$

*est **l'orbite de** x.*

Exemple 1.1.28. *Soit G un groupe et on considère l'action de G sur lui-même par conjugaison. Soit $x \in G$. L'orbite de $x \in G$ est appelé la **classe de conjugaison**. Elle est composée de tous le éléments yxy^{-1} où $y \in G$.*

$$G(x) = \{yxy^{-1} \mid y \in G\}.$$

Soit G un groupe qui agit sur un ensemble E. **Fixons** $x \in E$. Si $a, b \in G$ tels que $a \cdot x = b \cdot x$, alors $b^{-1} \cdot (a \cdot x) = x$ et donc $(b^{-1}a) \cdot x = x$ d'où $b^{-1}a \in G_x$ où G_x est le stabilisateur de x dans G. Alors a et b sont dans la même classe à gauche suivant G, i.e. $aG_x = bG_x$.

Réciproquement, si $aG_x = bG_x \in G$, alors $b^{-1}a \in G_x$ d'où $a \cdot x = b \cdot x$. Soit $f : G \to E$ l'application définie par $f(a) = a \cdot x$, alors nous venons de montrer que $f(a) = f(b)$ si et seulement si $aG_x = bG_x$. Alors nous pouvons définir l'application $\bar{f} : G/G_x \to E$ par $\bar{f}(aG_x) = f(a \cdot x)$. Nous allons dire que $\bar{f}$ est **induit** par f.

Proposition 1.1.23. *Soit $G \times E \to E$ une action de G sur E, et soit $x \in E$.*

1. *L'application $f : G \to E$ définie par $f(a) = x \cdot a$ induit une bijection entre G/G_x et l'orbite $G(x)$ de x.*
2. *L'ordre (le nombre d'éléments) de l'orbite $G(x)$ est égal à l'indice $(G : G_x)$ de G_x dans G.*

Démonstration. □

Proposition 1.1.24. *Si $G(x) \neq G(y)$, alors $G(x) \cap G(y) = \emptyset$.*

Donc si G opère sur E, l'ensemble des orbites forme une partition de E. Soit E un ensemble fini et $G \times E \to E$ une action, et soit $G(x_1), G(x_2), \ldots, G(x_r)$ les orbites distincts. Alors d'après la Proposition 1.1.23,

$$|E| = \sum_{i=1}^{r} (G : G_{x_i})$$

Groupes diédraux et isométries du plan

Soit E un espace euclidien ($E = \mathbb{R}^n$) orienté (on a choisi une repère $(O, \bar{e}_1, \ldots, \bar{e}_n)$). La distance euclidienne $d : E \times E \to \mathbb{R}_+$ est définie par

$$d(\bar{x}, \bar{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \ldots + (x_n - y_n)^2}.$$

Définition 1.1.16. *Une isométrie de E est une bijection $\phi : E \to E$ telle que $\forall \bar{x}, \bar{y} \in E$, $d(\phi(\bar{x}), \phi(\bar{y})) = d(\bar{x}, \bar{y})$.*

Notons $Isom(E)$ l'ensemble des isométries de E.

Proposition 1.1.25. *$(Isom(E), \circ)$ est un groupe.*

Démonstration. Soit ϕ_1 et ϕ_2 deux isométries de E. Soit $\bar{x}, \bar{y} \in E$. Alors

$$d(\phi_1 \circ \phi_2(\bar{x}), \phi_1 \circ \phi_2(\bar{y})) = d(\phi_1(\phi_2(\bar{x})), \phi_1(\phi_2(\bar{y}))) = d(\phi_2(\bar{x}), \phi_2(\bar{y})) = d(\bar{x}, \bar{y}).$$

L'identité Id_E est l'élément neutre, car $Id_E \circ \phi = \phi \circ Id_E = \phi$.

L'associativité de la LCI se montre comme l'associativité de la composition des applications.

Soit $\phi \in Isom(E)$. Comme ϕ est une bijection, il existe une bijection $\phi^{-1} : E \to E$ telle que $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = Id_E$. Soit $\bar{x}, \bar{y} \in E$, et notons $\bar{x}' = \phi^{-1}(x)$ et $\bar{y}' = \phi^{-1}(y)$. Alors

$$d(\phi^{-1}(\bar{x}), \phi^{-1}(\bar{y})) = d(\bar{x}', \bar{y}') = d(\phi(\bar{x}'), \phi(\bar{y}')) = d(\bar{x}, \bar{y}),$$

d'où $\phi^{-1} \in Isom(E)$. On a montré que $Isom(E)$ est un groupe. □

On a vu (en L1) que les isométries du plan sont :
— les rotations
— les symètries axiales
— les translations
— les symétries glissés
On a vu aussi que $Isom(\mathbb{R}^2)$ est engendré par les symétries axiales. En plus, on a vu que dans le plan, un isométrie ϕ est determinée par l'image de trois points distincts.

On voudrait maintenant considérer quelques sous-groupes de $G = Isom(\mathbb{R}^2)$.

Notons que G agit (par isométries) sur $\mathbb{R}^2$. Soit $\bar{x}_0 \in \mathbb{R}^2$. Nous avons vu que le stabilisateur G_{x_0} de x_0 est un sous-groupe de G. Par exemple, G_O, le stabilisateur de l'origine consiste de toutes les rotations centrées en O et de toutes les symétries dont les axes passent par O.

Soit $n \geq 3$. Considérons $P_n \subset \mathbb{R}^2$ un polygone régulier d'ordre n, i.e. un polygone convexe avec n côtés, qui est équilatéral et équiangle. Nous allons demander que $(0,0)$ soit le centre de P_n. Considérons D_n l'ensemble des symétries de P_n. Une symétrie de P_n est une isométrie de $\mathbb{R}^2$ dans $\mathbb{R}^2$ qui préserve P_n.

Trouvons tous les éléments de D_n. Pour simplifier la présentation, notons les sommets de P_n par $1, 2, 3, \ldots n$. (Make picture here) Alors tout élément de D_n définit une permutation de l'ensemble $\{1, 2, \ldots, n\}$, et il est défini uniquement par cette permutation.

Par exemple, soit $s \in D_n$ la rotation d'angle $2\pi/n$ (sens direct) ; elle envoie z_1 sur z_2, z_2 sur z_3 etc. Alors la permutation correspondant est le n-cycle $(1\,2\,3\,4\ldots n)$. Inversement, étant donné une permutation $\sigma \in S_n$, il y au plus une symétrie s de P_n telle que $s(z_i) = z_{\sigma(i)}$.

Pour tout $1 \leq i \leq n$ Il existe une symétrie de P_n qui envoie z_1 sur z_i : (par exemple la rotation r de l'angle $2\pi(i-1)/n$ le fait). Le sommet z_2 doit être envoyé sur un des voisins de z_i : $z_{i+1(mod\, n)}$ ou $z_{i-1(mod\, n)}$. La rotation r l'envoie sur $z_{i+1(mod\, n)}$. Soit L_{z_i} la droite qui passe par l'origine et par z_i. La symétrie axiale s par rapport à L_{z_i} est une symétrie de P_n. (Pourquoi ?) Elle échange $z_{i+1(mod\, n)}$ et $z_{i-1(mod\, n)}$, et elle fixe z_i. Donc $s \circ r$ envoie le sommet z_1 sur z_i, et z_2 sur $z_{i-1(mod\, n)}$. Il y a $n \cdot 2$ positions où le pair ordonné (z_1, z_2) peut être envoyé par des symtries de P_n . Et si on spécifie l'image de z_1 et z_2, on connait l'image des autres sommets automatiquement. Donc il y a exactement $2n$ éléments dans D_n : n rotations de centre $(0,0)$ et d'angle $\frac{2\pi i}{n}$, et n symétries axiales. (Exemples ?)

D_n est un groupe muni de l'operation composition des applications. En effet, la composée de deux symétries de P_n est une symétrie, l'élément neutre est l'application identité, la composition des application est associative, l'inverse d'une symétrie est une symétrie. (Vérifier !).

Proposition 1.1.26. *Soit $n \geq 2$, et P_n un n-gone régulier avec des sommets $\{z_1, z_2, \ldots, z_n\}$, où z_1 est sur l'axe positif des x. Soit r une rotation d'angle $\theta = \frac{2\pi k}{n}$, et s la symétrie par rapport à l'axes des x. Alors*

$$D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, rs, r^2 s, \ldots r^{n-1} s\}.$$

Démonstration. Il suffit de montrer que tous ces éléments sont distincts. □

Fixons $n \geq 3$ et un polygone P_n comme avant avec les sommets $z_1, z_2, \ldots z_n$. Soit $E = \{1, 2, 3, \ldots, n\}$. Alors nous avons une application $D_n \times E \to E$ définie par

$$(\sigma, i) \mapsto j \quad \text{si } \sigma(z_i) = z_j.$$

Proposition 1.1.27. *L'application* $(\sigma, i) \mapsto j$ *si* $\sigma(z_i) = z_j$ *est une action de* D_n *sur* E.

Démonstration. Vérifions que c'est une action du groupe. Soit $e \in D_n$ l'élément neutre. Comme $e(z_i) = z_i$, on a $e \cdot i = i$ pour tout $1 \leq i \leq n$. Soit $\sigma, \sigma' \in D_n$. Fixons i et soit $z_j = \sigma'(z_i)$ et $z_k = \sigma(z_k)$. Alors $(\sigma\sigma')(z_i) = \sigma(\sigma'(z_i)) = \sigma(z_j) = z_k$, et donc $\sigma\sigma' \cdot i = k$ et $\sigma \cdot (\sigma' \cdot i) = \sigma \cdot j = k$. □

L'action définie un morphisme ϕ de D_n dans S_n. Comme ϕ est injectif, (Pourquoi ?) $D_n \approx \phi(D_n) < S_n$.

Exemple 1.1.29. *Pour* $n = 3$, *le groupe des symétries d'un triangle équilatère,* D_3 *contient* $2 \cdot 3 = 6$ *éléments. Comme* D_n *est isomorphe à un sous-groupe de* S_3, *et comme* $|S_3| = 6$, *les deux groupes sont isomorphes,* $D_3 \approx S_3$. *En général,* D_n *est beaucoup plus petit que* S_n.

1.2 Anneaux et Corps.

Définition et premières propriétés

Un **anneau** (A,+ est un ensemble muni de deux LCI, *l'addition* $(x, y) \mapsto x + y$ et la *multiplication* $(x, y) \mapsto xy$, qui satisfont les propriétés suivantes :

A1 $(A, +)$ est un groupe abélien.

A2 Pour tous $x, y, z \in A$, on a $x(y + z) = xy + xz$ et $(y + z)x = yx + zx$.

A3 Multiplication est associative : pour tous $x, y, z \in A$, on a $(xy)z = x(yz)$.

A4 Il existe un élément neutre pour multiplication : $\exists e \in A$ tel que $\forall x \in A$, on a $xe = ex = e$.

Proposition 1.2.1. *Soit* $(A, +, \cdot)$ *un anneau. Un élément neutre pour la multiplication est unique.*

On appèle souvant l'élément neutre pour la multiplication *l'élément unité*, et on le dénote souvent 1_A. L'élément neutre de $(A, +)$ sera souvent noté 0_A. Voici quelques premiers exemples d'anneaux.

Exemple 1.2.1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *sont des anneaux.*

Exemple 1.2.2. *Soit* $M(n, \mathbb{R})$ *l'ensemble des matrices carrées* $n \times n$ *à coéfficients réels* $(M(n, \mathbb{R}), +, \cdot)$ *est un anneau.*

Exemple 1.2.3. *Soit G un groupe abélien et notons sa LCI "+". Notons*

$$End(G) = \{\phi : G \to G \text{ morphisme de groupe }\}.$$

Si $\phi, \phi' \in End(G)$, on pose $(\phi+\phi')(x) = \phi(x)+\phi'(x)$. Ca définit une LCI sur $End(G)$ et $(End(G), +)$ est un groupe (Vérifier !). Comme G est abélien, on a $\phi(x)+\phi'(x) = \phi'(x)+\phi(x)$ et donc $\phi+\phi' = \phi'+\phi$. Alors $(End(G), +)$ est un groupe abélien.

Mais on peut aussi munir $End(G)$ de la LCI composition des applications : si $\phi, \phi' \in End(G)$, la composée $\phi \circ \phi'$ est aussi un morphisme de G dans G, et donc $\phi \circ \phi' \in End(G)$. En plus, l'identité Id_G est l'élément unité. Enfin, pour $\phi, \phi', \phi'' \in End(G)$, on vérifie

$$\phi \circ (\phi' + \phi'')(x) = \phi(\phi'(x) + \phi''(x)) = \phi(\phi'(x)) + \phi(\phi''(x)) = (\phi \circ \phi' + \phi \circ \phi'')(x)$$

et

$$((\phi' + \phi'') \circ \phi)(x) = (\phi' \circ \phi + \phi'' \circ \phi)(x).$$

Alors $(End(G), +, \circ)$ est un anneau.

Définition 1.2.1. *Un anneau $(A, +, \cdot)$ est **commutatif** si $\forall x, y \in R$ on a $xy = yx$.*

Voici quelque règles de calcul qui découlent de la définition d'un anneau.

Proposition 1.2.2. *Soit A un anneau. Notons 0 l'élément neutre de $(A, +)$ et e l'élément unité.*

1. *$0x = 0$ pour tout $x \in A$.*
2. *$(-e)x = -x$ pour tout $x \in A$.*
3. *$(-e)(-e) = e$.*
4. *$(-x)y = -xy$ pour tous $x, y \in A$.*
5. *$(-x)(-y) = xy$ pour tous $x, y \in A$.*
6. *$(x_1 + x_2 + \ldots + x_k)(y_1 + \ldots y_m) = x_1y_1 + \ldots x_ky_m$.*

Démonstration. On démontre les trois premiers et laisse le reste en exercice.

1. On a $0x + x = 0x + ex = (0 + e)x = ex = x$, et donc $0x = 0$.
2. On calcule $(-e)x + x = (-e)x + ex = (-e + e)x = 0x = 0$. Donc $(-e)x = -x$.
3. D'après la partie précédent, $(-e)(-e) = -(-e) = e$.

□

Exemple 1.2.4. *Un anneau* ***trivial*** *est un ensemble* $A = \{0_A\}$ *où* $0_A \cdot 0_A = 0_A$ *et* $0_A + 0_A = 0_A$. *(Vérifier que c'est bien un anneau).*

Soit $(A, +, \cdot)$ *un anneau, et on note* 0_A *l'élément neutre de* $(A, +)$ *et* 1_A *l'élément unité.*

Si $0_A = 1_A$, *alors pour tout* $x \in A$, $x = 1_A \cdot x = 0_A \cdot x = 0_A$. *Donc* $A = \{0_A\}$.

Définition 1.2.2. *Soit* $(A, +, \cdot)$ *un anneau. Un sous-ensemble* A' *de* A *est un sous-anneau de* A, *tel que*

1. $1_A \in A'$;
2. *si* $x, y \in A'$ *alors* $-x, x + y, xy$ *sont aussi dans* A'

On voit facilement que $(A', +, \cdot)$ est aussi un anneau.

Exemple 1.2.5. $(\mathbb{Z}, +, \cdot)$ *est un sous-anneau de* $(\mathbb{R}, +, \cdot)$ *(et aussi de* $(\mathbb{Q}, +, \cdot)$ *et de* $(\mathbb{C}, +, \cdot)$*).*

Définition 1.2.3. *Soit* $(A, +, \cdot)$ *un anneau, notons* 0_A *l'élément neutre du groupe* A'*). Si* $x, y \in A \setminus \{0_A\}$ *tels que* $xy = 0_A$, *on dit que* x *et* y *sont des* ***diviseurs de zéro****.*

Exemple 1.2.6. *Dans l'anneau* $(M(2, \mathbb{R}), +, \cdot)$, *il y a des diviseurs de zéro. Par exemple, le produit de*

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

est la matrice nulle.

Exemple 1.2.7. *Il n'y a pas de diviseurs de zéro dans* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$, *parce que* $xy = 0$ *implique* $x = 0$ *ou* $y = 0$ *pour les nombres complexes.*

Définition 1.2.4. *Un* ***anneau intègre*** *est un anneau* $(A, +, \cdot)$ *sans diviseurs de zéro et tel que* $1_A \neq 0_A$.

Exemple 1.2.8. *Les anneaux* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$ *sont intègres.* $(M(2, \mathbb{R}), +, \cdot)$ *n'est pas un anneau intègre*

Définition 1.2.5. *Un* ***anneau commutatif*** $(A, +, \cdot$ *tel que* $(A \setminus 0_A, \cdot)$ *est un groupe, est appelé* ***un corps****.*

Proposition 1.2.3. *Tout corps est un anneau intègre.*

Démonstration. Soit $(A, +, \cdot)$ un corps. Montrons que $1_A \neq 0_A$. C'est facile : comme $(A \setminus 0_A, \cdot)$ est un groupe, A n'est pas trivial et donc $0_A \neq 1_A$.

Supposons que maintenant que $xy = 0_A$ et que $x \neq 0_A$. Alors x admet un inverse $x^{-1} \in A \setminus \{0_A\}$. Alors $x^{-1}xy = x^{-1}0_A$ et donc $y = 0_A$. □

Exemple 1.2.9. $\mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$ *sont des corps.*

Pour un anneau A on dénote A^* l'ensemble des éléments $x \in A$ tels que il existe $y \in A$ avec $xy = yx = 1_A$. Autrement dit, A^* est l'ensemble des éléments qui admettent un inverse multiplicatif.

Idéaux

Définition 1.2.6. *Soit $(A, +, \cdot)$ un anneau. Une partie $I \subset A$ est un* ***idéal à gauche*** *de A si*

1. $0_A \in I$;
2. $\forall x, y \in I$, *on a* $x + y \in I$;
3. $\forall a \in A$ *et* $\forall x \in I$, *on a* $ax \in I$.

Remarque 2. *Soit I un idéal à gauche d'un anneau A. Alors si $x \in I$, on a aussi*

$$(-1_A)x = -x \in A$$

et donc $(I, +)$ est un sous-groupe de $(A, +)$. Ca implique on peut définir les idéaux à gauche comme des sous-groupes de $(A, +)$ stables par multiplication à gauche par les éléments de A.

De la même façon on définit un **idéal à droite** (on démand que $x \in I$ et $a \in A$ implique $xa \in I$), et un **idéal bilatère** (on démande que $x \in I$ et $a \in A$ implique $xa, ax \in I$).

Remarque 3. *Si A est commutatif, tous ces idéaux sont bilatères.*

Exemple 1.2.10. *Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z}$ est un idéal bilatère de $(\mathbb{Z}, +, \cdot)$. Tout idéal de $\mathbb{Z}$ est égal à $n\mathbb{Z}$ pour un $n \in \mathbb{N}$.*

Exemple 1.2.11. *Soit $A = \{f : [0, 1] \to \mathbb{R}$ fonction continue sur $[0, 1]\}$. Alors $(A, +, \cdot)$ est un anneau commutatif. L'ensemble $I = \{f \in A |\ f(1/2) = 0\}$ est un idéal (bilatère) de A.*

Exemple 1.2.12. *Soit $(A, +, \cdot)$ un anneau, et $a \in A$ un élément. L'ensemble*

$$I = \{xa \mid x \in A\}$$

est un idéal à gauche (Pourquoi ?). On l'appele ***idéal principal à gauche engendré*** *par a.*

Morphismes d'anneaux

Définition 1.2.7. *Soit A et A' deux anneaux. Une application $\phi : A \to A'$ est un* ***morphisme d'anneaux*** *si pour tous $x, y \in A$,*

1. $\phi(x+y) = \phi(x) + \phi(y)$,
2. $\phi(xy) = \phi(x)\phi(y)$.
3. $\phi(1_A) = 1_{A'}$

On remark que dans $\phi(x+y) = \phi(x) + \phi(y)$, $x+y$ est l'élément obtenu en applicant la loi $+$ de A aux élément x et y de A, tandis que $\phi(x) + \phi(y)$ est le résultat d'application de la loi $+$ de A' aux éléments $\phi(x)$ et $\phi(y)$. Pareil pour $\phi(xy) = \phi(x)\phi(y)$.

Définition 1.2.8. *Soit $\phi : A \to A'$ un morphisme d'anneaux. Le* ***noyau*** *de ϕ est l'ensemble*

$$Ker(\phi) = \{x \in A |\ \phi(x) = 0_{A'}\}.$$

Proposition 1.2.4. *Le noyau d'un morphisme d'anneaux $\phi : A \to A'$ est un idéal bilatère de A.*

Démonstration.

- Montrons que $0_A \in Ker(\phi)$. Pour tout $x \in A$, on a $\phi(x) = \phi(x + 0_A) = \phi(x) + \phi(0_A)$, et donc $\phi(0_A) = 0_{A'}$.
- Soit $x, y \in Ker(\phi)$. On a $\phi(x+y) = \phi(x) + \phi(y) = 0_{A'} + 0_{A'} = 0_{A'}$. Alors $x + y \in Ker(\phi)$.
- Soit $x \in Ker(\phi)$ et $a \in A$. $\phi(ax) = \phi(a)\phi(x) = \phi(a)0_{A'} = 0_{A'}$ d'où $ax \in Ker(\phi)$. De la même façon on montre que $xa \in Ker(\phi)$.

□

Exemple 1.2.13. *Soit $A = \{f : [0,1] \to \mathbb{R}, f$ continue$\}$. L'application $\phi : A \to \mathbb{R}$ définie par $\phi(f) = f(\frac{1}{2})$ est un morphisme d'anneaux.*

Comme pour les groupes, on définit un **isomorphisme d'anneaux**.

Définition 1.2.9. *On dit que un morphisme d'anneaux $\phi : A \to A'$ est un isomorphisme d'anneaux s'il existe un morphisme d'anneaux $\psi : A' \to A$ tel que $\phi \circ \psi = Id_{A'}$ et $\psi \circ \phi = Id_A$. Un automorphisme d'anneaux est un isomorphisme d'anneaux $A \to A$.*

On peut montrer (en exercice) que $\phi : A \to A'$ est un isomorphisme d'anneau si et seulement si ϕ est une bijection.

Anneaux quotients

Comme pour les groupes, il existe une notion de quotient sur les anneaux.

Soit A un anneau et I un idéal bilatère de A. Rappelons que I est un sous-groupe de $(A,+)$. Pour $x \in A$, soit $x+I$ la classe à gauche de x suivant I. Comme le groupe $(A,+)$ est commutatif, $x+I = I+x$, et nous allons dire classe de x suivant I.

Voici quelques propritétés utiles :

Lemme 1.2.1.

(a) $x+I = x'+I \leftrightarrow x \in x'+I \leftrightarrow x-x' \in I$;

(b) *Si* $x+I = x'+I$ *et* $z \in A$, *alors* $zx+I = zx'+I$ *et* $xz+I = x'z+I$;

(c) *Si* $x+I = x'+I$ *et* $y+I = y'+I$, *alors* $xy+I = x'y'+I$ *et* $x+y+I = x'+y'+I$;

Démonstration. (a) Si $x+I = x'+I$, alors pour tout $m \in I$ il existe $m' \in I$ tel que $x+m = x'+m'$. Ca implique que $x = x'+(m'-m)$. Comme $m'-m \in I$, on a $x \in x'+I$. Mais on a aussi $x-x' = m'-m \in I$, d'où $x-x' \in I$. Supposons maintenant que $x-x' \in I$. Notons $m' = x-x'$. Alors $x = x'+m'$. Comme $m \in I$, on a $x \in x'+I$. Les classes de x et x' ont l'intersection non-vide (les deux contiennent x), donc $x+I = x'+I$.

(b) Soit $x+I = x'+I$ et $z \in A$. Montrons que $zx+I = zx'+I$. On a $zx-zx' = z(x-x')$. Comme $x-x' \in I$, on a $z(x-x') \in I$ et dont $zx-zx' \in I$. D'après (a), $zx+I = zx'+I$. De la même façon on peut montrer que $xz+I = x'z+I$.

(c) Soit $x+I = x'+I$ et $y+I = y'+I$. Montrons que $xy+I = x'y'+I$. Ecrivons $x' = x+m$ et $y' = y+m'$ où $m, m' \in I$. Alors $x'y' = (x+m)(y+m') = xy+my+xm'+mm'$. Comme I est un idéal bilatère, on a $my+xm'+mm' \in I$. Ca montre que $xy-x'y' \in I$, donc d'après la partie (a) on a $xy+I = x'y'+I$. On laisse en exercice la démonstration de la dernière egalité.

□

Soit $A/I = \{x+I |\ x \in A\}$ l'ensembles des classes suivant I. Nous savons déjà que A/I est un groupe commutatif muni de LCI

$$(x+I)+(y+I) = (x+y)+I.$$

On définit la loi de multiplication par $(x+I)(y+I) = xy+I$. La propriété (c) du lemme precedent implique que cette opération est bien définie (ne depend

pas de choix de representants de $x + I$ et $y + I$). Nous allons maintenant vérifier que $(A/I, +, \cdot)$ est un anneau. La classe $1_A + I$ est l'élément neutre de multiplication :

$$(1_A + I)(x + I) = 1_A x + I = x + I.$$

Ensuite, la multiplication est associative :

$$((x+I)(y+I))(z+I) = (xy+I)(z+I) = xyz+I = (x+I)(yz+I) = (x+I)((y+I)(z+I)).$$

Enfin, on montre la distributivité :

$$(x+I)((y+I)+(z+I)) = (x+I)(y+z+I) = (xy+I)+(xz+I) = (x+I)(y+I)+(x+I)(z+I).$$

On appelle A/I **l'anneau quotient** de A par I.

Théorème 1.2.1. *Soit $\phi : A \to A'$ un morphisme d'anneaux, et soit $I = Ker(\phi)$ le noyau de ϕ. Pour tout classe $x + I$, $\phi(x + I)$ est un élément de A', et l'application ϕ' qui associe à tout $x + M$ l'élément $\phi(x + I)$ est un isomorphisme d'anneaux de A/I dans $\phi(A)$.*

Démonstration. Si $y \in x+I$, alors on peut écrire $y = x+m$ avec $m \in M$. Donc $\phi(y) = \phi(x+m) = \phi(x)+\phi(m) = \phi(x)$. Ca nous dit que ϕ est constante sur les classes suivant I, et donc $\phi(x + I)$ est l'élément $\phi(x)$ de A'. Donc nous avons l'application $\phi' : A/I \to \phi(A)$ qui envoie $x + I$ sur $\phi(x)$. C'est un morphisme, car

$$\phi'(x+I+y+I) = \phi'(x+y+I) = \phi(x+y) = \phi(x)+\phi(y) = \phi'(x+I)+\phi'(y+I)$$

et

$$\phi'((x + I)(y + I)) = \phi'(xy + I) = \phi(xy) = \phi(x)\phi(y) = \phi'(x + I)\phi'(y + I).$$

Enfin, $\phi'(1_A + I) = \phi(1_A) = 1_{A'}$ et donc ϕ' est un morphisme d'anneaux. Il nous reste à montrer que ϕ' est injectif. Si $\phi'(x + I) = \phi'(y + I)$, alors $\phi(x) = \phi(y)$ et donc $\phi(x - y) = 0_{A'}$ d'où $x + I = y + I$. □

Exemple 1.2.14. *Si $A = \mathbb{Z}$, les idéaux de A sont tous de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. Soit $I = n\mathbb{Z}$ ou $n \geq 1$. L'anneau quotient correspondant est $\mathbb{Z}/n\mathbb{Z}$. C'est un anneau fini, il contient n éléments. Comme $\mathbb{Z}$ est commutatif, $\mathbb{Z}/n\mathbb{Z}$ l'est aussi. Soit $\bar{x}$ un élément non-nul de $\in \mathbb{Z}/n\mathbb{Z}$. $\bar{x}$ admet un inverse multiplicatif si et seulement si il existe $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{x}\bar{y} = \bar{1}$, ce qui est equivalent à $pgcd(x, n) = 1$. (Exercice). On conclut que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Soit A un anneau. Pour $n \in \mathbb{N}^*$ et $a \in A$, on définit

$$na = \underbrace{a + a + \ldots + a}_{n \text{ termes}} \in A.$$

Si $n = -k$ ou $k \in \mathbb{N}^*$, on pose

$$na = -(ka).$$

Enfin, si $n = 0_A$, on sait que $a \cdot 0_A = 0_A$.

En particulier, si $a = 1_A$, on obtient une application $\phi : \mathbb{Z} \to A$ définie par

$$\phi(n) = n1_A$$

Cette application est un morphisme d'anneaux, on a $\phi(1) = 1_A$, $\phi(n+m) = \phi(n) + \phi(m)$ et $\phi(nm) = \phi(n)\phi(m)$. (Ce n'est pas complètement evident, il faut justifier !)

Supposons maintenant que $\psi : \mathbb{Z} \to A$ est un morphisme d'anneaux. Par définition $\psi(0) = 0_A$, $\psi(1) = 1_A$ et pour $n \geq 1$, on a

$$\psi(n) = \psi(1 + 1 + \cdots + 1) = 1_A + 1_A + \cdots 1_A = n1_A.$$

Pour $n = -k$ avec $k \geq 1$ on a

$$\psi(-k) = -\psi(k) = -(k1_A).$$

Donc $\phi = \psi$, et on conclut qu'il y a un et un seul morphisme d'anneaux de $\mathbb{Z}$ dans A.

Caractéristique d'un anneau Soit A un anneau non-trivial et $\phi : \mathbb{Z} \to A$ le morphisme d'anneaux. Soit $I = Ker(\phi)$. Comme $\phi(1) \neq 0_A$, l'idéal I n'est pas Z. Donc $I = n\mathbb{Z}$ pour un $n \geq 2$. Alors $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\phi(\mathbb{Z})$. Nous allons dire que A contient $\mathbb{Z}/n\mathbb{Z}$. Comme $\phi(n) = 0_A$ et $\phi(n) = n1_A$, on conclut que $n1_A = 0_A$. En fait pour tout $a \in A$, on a $na = (n1_A)a = 0_A$. On dit que A est de caractéristique n.

Remarque 4. *Pour tout anneau A non-nul il y a un seul $n \in \mathbb{N}^*$ tel que A contient $\mathbb{Z}/n\mathbb{Z}$. (exercice)*

Théorème 1.2.2. *Soit A un anneau intègre. Si A contient $\mathbb{Z}/n\mathbb{Z}$, alors n et 0 ou un nombre premier.*

Démonstration. Soit $n \neq 0$. Si $n = mk$ avec $m, k \geq 2$, alors m, k ne sont pas dans le noyau du $\phi : \mathbb{Z} \to A$. Donc $m1_A \neq 0$ et $k1_A \neq 0$ mais $mk1_A = n1_A = 0_A$. Ce n'est pas possible parce que A n'a pas de diviseurs de zéro. □

Soit K un corps, et $\phi : \mathbb{Z} \to K$ le morphisme d'anneaux. Si $Ker(\phi) = \{0\}$, alors K contient $\mathbb{Z}$. Nous allons dire que K est de **caractéristique** 0. Si $Ker(\phi)$ n'est pas trivial, il est engendré par un nombre premier p, et nous allons dire que K est de **caractéristique** p. Par exemple $F_p = \mathbb{Z}/p\mathbb{Z}$ est de caractéristique p. Tout corps K de caractŕistique p contient F_p. On appelle F_p **corps premier.**

Théorème 1.2.3. *Soit G un groupe cyclique d'ordre N. Soit $m \in \mathbb{Z}$ tel que $pgcd(m, N) = 1$. Alors l'application $\sigma_m : G \to G$ définie par $\sigma_m(x) = x^m$ est un automorphism de G. L'application*

$$m \mapsto \sigma_m$$

définit un isomorphisme $(\mathbb{Z}/N\mathbb{Z})^* \to Aut(G)$.

Définition 1.2.10. *Soit A un anneau commutatif. Soit P un idéal dans A. On dit que P est un **idéal premier** si $P \neq A$ et si pour tout $a, b \in A$, $ab \in P$ implique $a \in P$ ou $b \in P$.*

Définition 1.2.11. *Soit A un anneau commutatif, et M un idéal. On dit que M est un **idéal maximal** si $M \neq A$ et si le seul idéal I tel que $M \subset I$ et $M \neq I$ est $I = A$.*

Théorème 1.2.4. *Soit A un anneau commutatif. Alors*

1. *Tout idéal maximal est premier.*
2. *Un idéal P est premier si et seulement si A/P est intègre.*
3. *Un idéal M est maximal si et seulement si A/M est un corps.*

Corps des fractions

Soit A un anneau commutatif intègre. Considérons l'ensemble.

$$A \times (A \setminus \{0_A\}) = \{(a, b) | a, b \in A,\ b \neq 0_A\}$$

Nous allons dire que couples (a, b) et (a', b') sont équivalents et écrire $(a, b) \sim (a', b')$ si $ab' - a'b = 0_A$.

Exercice 1.2.1. *Montrer que $\sim$ est bien une relation d'équivalence.*

Notons $\frac{a}{b}$ la classe d'équivalence de (a, b), i.e. l'ensemble des tous (a', b') tels que $(a, b) \sim (a', b')$. Les classes d'équivalence forment une partition de

$A \times (A \setminus \{0_A\})$. Notons K l'ensemble des classes $\frac{a}{b}$. Soit $\frac{a}{b}, \frac{c}{d} \in K$. On définit leur somme et leur produit par

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{et} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Il faut montrer que la somme et le produit sont bien définis. Si $(a', b') \sim (a, b)$ et $(c', d') \sim (c, d)$, alors

$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'} = \frac{ad+bc}{bd}$$

parce que $(a'd' + b'c')(bd) = (ad + bc)(b'd')$ où la dernière egalité se vérifie en utilisant $ab' = a'b$ et $cd' = c'd$. De la même façon on a $\frac{a'}{b'} \cdot \frac{c'}{d'} = \frac{a'c'}{b'd'} = \frac{ac}{bd}$ parce que $a'c'bd = acb'd'$.

Proposition 1.2.5. *Montrer que $(K, +, \cdot)$ est un corps.*

Démonstration. En exercice □

Exemple 1.2.15. *On peut construire le corps des nombres rationnels $\mathbb{Q}$ à partir d'anneau $\mathbb{Z}$.*

Exemple 1.2.16. *Soit K un corps et $K[t]$ l'anneau des polynômes sur K. Un utilisant cette construction on obtient le corps des fractions rationnels $K(t)$.*

Exemple 1.2.17. *Soit K un corps de caractéristique 0. Alors K contient $\mathbb{Q}$.*

1.3 Polynomes et Fractions Rationnelles

Définition 1.3.1. *Soit K un corps. On appelle polynôme à coéfficients dans K et à une indeterminée toute suite $(a_0, a_1, \ldots, a_n, \ldots)$ d'éléments dans K tous nuls à partir de certain rang.*

Le polynôme $P = (0, 0, \ldots)$ dont tous les coéfficients sont 0, est un polynôme nul. Soit $P = (a_0, a_1, a_2, \ldots)$ et $Q = (b_0, b_1, b_2, \ldots)$ deux polynômes. On peut définir la somme de P et Q par

$$P + Q = (c_0, c_1, c_2, \ldots) \text{ où } c_k = a_k + b_k$$

et le produit

$$PQ = (d_0, d_1, d_2, \ldots) \text{ où } d_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Notons $X = (0, 1, 0, \ldots)$, alors on peut vérifier que $X^2 = (0, 0, 1, 0, \ldots)$, $X^3 = (0, 0, 0, 1, 0, 0, \ldots)$ etc. Alors si $P = (a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots)$, alors on peut écrire P de la façon usuelle

$$P = a_o + a_1 X + a_2 X^2 + \ldots + a_n X^n.$$

On dénote $K[X]$ l'ensemble des polynômes à une indéterminée à coéfficients dans K.

Lemme 1.3.1. *$K[X]$ est un anneau commutatif.*

Définition 1.3.2. *Soit $P \in K[X]\backslash 0$. On appelle degré de P et on note $deg(P)$ le plus grand indice $n \in \mathbb{N}$ tel que le coéfficient a_n de P est non-nul. On pose $deg(0) = -\infty$.*

Soit L un corps tel que K est un sous-corps de L (on dit que L est une extension de K). A tout polynôme $P = a_o + a_1 X + a_2 X^2 + \ldots + a_n X^n$ dans $K[X]$ on peut associer une fonction polynôme $P_F : F \to F$ définie par

$$P_K(t) = a_o + a_1 t + a_2 t^2 + \ldots + a_n t^n.$$

Soit $c \in F$. On définie une application $\phi_c : K[X] \to L$ par $\phi_c(P) = P(c)$. Alors ϕ_c est un morphisme d'anneaux, parce que $(P + Q)(c) = P(c) + Q(c)$, $(PQ)(c) = P(c)Q(c)$ et $\phi_c(1) = 1_L$. (Exercice : Verifier que ϕ_c est un morphisme)

Notons $K[c]$ l'image $\phi_c(K[X])$ dans F. Alors $K[c]$ est un sous-corps de F. Si $\phi_c : K[X] \to K[c]$ est un isomorphisme, on dit que c est **transcendant** sur K.

Exemple 1.3.1. *$K = \mathbb{Q}$ et $F = \mathbb{R}$. Alors $K[\sqrt{2}] = \{a + b\sqrt{2} |\ a, b \in Q\}$ est un sous-corps de $\mathbb{R}$. Est-ce que $\sqrt{2}$ est transcendant sur $\mathbb{Q}$? Non. Par exemple $\phi_{\sqrt{2}}(X^2 - 2) = 0$, donc $\phi_{\sqrt{2}}$ n'est pas injectif.*
Par contre π est transcendant sur Q (ce n'est pas évident).

Racines des polynômes

Définition 1.3.3. *Soit $P \in K[X]$ et $\alpha \in L$ ou L est une extension de K. On dit que α est une racine de P si $P_K(\alpha) = 0_K$.*

Théorème 1.3.1. *Soit K un corps et $P \in K[X]$ un polynome de degré $n \geq 0$. Alors P a au plus n racines dans K.*

On aura besoin de lemme suivant.

Lemme 1.3.2. *Soit K un corps, $P \in K[X]$ et $\alpha \in K$. Il existent $c_0, c_1, \ldots, c_n \in K$ tels que*

$$P(X) = c_0 + c_1(X-\alpha) + c_2(X-\alpha)^2 + \ldots + c_n(X-\alpha).$$

On remarque que ici on identifie $\alpha \in K$ avec l'élément $(\alpha, 0, 0, \ldots)$ de $K[X]$.

Démonstration. On écrit $X = \alpha + (X-\alpha)$, $X^2 = (\alpha+(X-\alpha))(\alpha+(X-\alpha)) = \alpha^2 + 2\alpha(X-\alpha) + (X-\alpha)^2$, etc . □

du Théorème. On remarque que $P(\alpha) = c_0$. Donc si α est une racine de P, on a $c_0 = 0$ et on peut écrire

$$P(X) = (X-\alpha)Q(X),$$

et on peut écrire $Q(X) = c_1 + c_2(X-\alpha) + c_n(X-\alpha)^{n-1}$. Supposons que $\alpha, \alpha_1, \ldots, \alpha_n$ sont des racines distincts de P (donc il y a $n+1$ racines au moins). Alors $0 = P(\alpha_i) = (\alpha_i - \alpha)Q(\alpha_i)$. Comme $\alpha - \alpha_i \neq 0$, on a $Q(\alpha_i) = 0$ pour $i = 1, \ldots, n$. Par récurrence on voit que ce n'est pas possible. □

Corollaire 1.3.1. *Soit K un corps et $P, Q \in K[X]$ polynômes sur K. Supposons que K est infini. Si $P(c) = Q(c)$ pour tout $c \in K$, alors $P = Q$, i.e. les coefficients correspondants sont égaux.*

Démonstration. Il suffit de considérer le polynôme $R = P - Q$. Il a un nombre infini de racines dans K, donc $P = 0$. □

Attention ! ! Si K est fini, l'enoncé n'est pas vrai. Par exemple, pour $K = F_p$, comme F_p^* est d'ordre $p-1$, tout élément $c \in F_p^*$ satisfait $c^{p-1} = 1$. Donc si on pose $P = X^p$ et $Q = X$, on voit que $P(c) = Q(c)$ pour tout $c \in F_p$, mais $P \neq Q$.

Arithmétique dans $K[X]$

Théorème 1.3.2. *Soit $P, Q \in K[X]$ deux polynômes. Alors*

$$deg(PQ) = deg(P) + deg(Q).$$

Démonstration. Soit $P = a_0 + \ldots a_n X^n$ avec $a_n \neq 0$ et $Q = b_0 + \ldots + b_m X^m$ tel que $b_m \neq 0$. Alors

$$PQ = a_0 b_0 + \ldots a_n b_m X^{n+m}.$$

Comme K est un corps, il n'a pas de diviseurs de zéro et donc $a_n b_m \neq 0$. □

Corollaire 1.3.2. *L'anneau $K[X]$ est un anneau commutatif intègre.*

Remarque 5. *Comme $K[X]$ est un anneau commutatif et intègre, on construit le corps des fractions rationnelles $K(X)$ comme dans la chapitre précédent. On rappel que $K(X)$ est l'ensembles des classes déquivalence des coupes $(P,Q) \in K[X]$ où $Q \neq 0$ et où $(P,Q) \sim (P',Q')$ ssi $PQ' = QP'$. On appelle* ***fonctions rationnelles*** *les éléments de $K(X)$.*

Théorème 1.3.3 (Division euclidienne)**.** *Soit $A, B \in K[X]$ et $B \neq 0$. Alors il existent uniques $P, Q \in K[X]$ tels que*

$$A = BQ + R$$

avec $deg(R) < deg(B)$.

Démonstration. Voici une idée d'une preuve. Soit $A = a_n X^n + \dots a_1 X + a_0$ et $B = b_m X^m + \dots + b_1 X + b_0$ où $b_m \neq 0$. Si $n < m$, on pose $Q = 0$ et $R = A$. Supposons donc $n \geq m$. Soit $Q_1 = a_n b_m^{-1} X^{n-m}$. Soit

$$A_1 = A - Q_1 B.$$

On a

$$deg(A_1) < deg(A).$$

On peut donc écrire $A = BQ_1 + A_1$. Si $deg(A_1) < deg(B)$, on s'arrète la, sinon on trouve des polynômes A_2 et Q_2 avec $deg(A_2) < deg(A_1)$ et

$$A_1 = BQ_2 + A_2.$$

On a $A = B(Q_1 + Q_2) + A_2$ et $deg(A_2) < deg(A_1) < deg(A)$. On continue de cette façon jusqu'au moment où $deg(A_k) < deg(B)$. □

Définition 1.3.4. *On dit que un corps K est algébriquement clos si tout polynôme $P \in K[X]$ de degré $deg(P) \geq 1$ a une racine dans K.*

Exemple 1.3.2. *Les corps $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas alébriquement clos. Le corps $\mathbb{C}$ est algébriquement clos. Nous n'allons pas montrer ce résultat.*

Exemple 1.3.3. *Les corps finis ne sont pas algébriquement clos. Soit K un corps fini. Soit $P = \prod_{\alpha \in K}(X - \alpha) + 1_K$. Alors $P(\alpha) = 1_K$ pour tout $\alpha \in K$, donc P n'a pas de racines dans K.*

Corollaire 1.3.3. *Soit K un corps alébriquement clos. Alors pour tout $P \in K[X]$ de degré $n \geq 1$ il existent $\alpha_1, \dots \alpha_n, c \in K$ tels que*

$$P = c(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n).$$

Démonstration. Soit α_1 une racine de P. Alors par la division euclidienne $P = (X - \alpha_1)Q_1$ où $deg(Q_1) = n - 1$. Si $n - 1 \geq 1$, le polynôme Q_1 a une racine α_2 et on donc $Q_1 = (X - \alpha_2)Q_2$ etc... □

Le pgcd des deux polynômes.

Théorème 1.3.4. *Soit I un idéal de $K[X]$.*

1. *Il existe un polynôme P tel que I est engendré par P, i.e. $I = \{QP |\ Q \in K[X]\}$.*
2. *Si $I \neq \{O\}$, tout polynôme P tel que $P \neq 0$ et $deg(P)$ est le plus petit degré positif dans I, alors P est un générateur de I.*

Démonstration. Soit $I \neq \{0\}$. Soit d le plus petit degré positif des polynômes dans I et soit P un polynôme dans I de degré d. Montrons que P engendre I. Soit $Q \in I$. Montrons que Q est un multiple de P, i.e. qu'il existe $B \in K[X]$ tel que $Q = BP$. Par la division euclidienne, il existent B et B' dans $K[X]$ tels que $Q = BP + B'$ où $deg(B') < deg(P) = d$. On a $B' = Q - BP$ et donc $B' in I$. Comme d est le plus petit degré positif des polynômes dans I, et $deg(B') < d$, on conclut que $deg(B') = -\infty$ et donc $B' = 0$. Donc $Q = BP$. □

Remarque 6. *Soit I un idéal de $K[X]$. D'apres le théorème, I est principal, i.e. engendré par un élément. Soit $P \in I$ un générateur. Supposons que $P' \in I$ est aussi un générateur de I.*

Comme P est un générateur de I, Il existe $B \in K[X]$ tel que $P' = BP$. Alors $deg(P') = deg(B) + deg(P)$ et donc $deg(P') \geq deg(P)$. Mais par l'hypothèse P' est aussi un générateur, donc $deg(P) \geq deg(P')$. Les deux inégalités donnent $deg(P') = deg(P)$. Ca implique que $deg(B) = 0$ et donc B est une constante. Alors on peut écrire

$$P' = cP.$$

Si $P = a_0 + a_1X + a_2X^2 + \ldots + a_dX^d$ alors $P' = ca_0 + ca_1X + ca_2X^2 + \ldots + ca_dX^d$. Si on choisi $c = (a_d^{-1}, 0, 0, \ldots)$ (K est un corps et $a_d \neq 0$ donc a_d admet inverse multiplicatif), on voit que I a un générateur avec coéfficient dominant 1_K. Ce générateur est unique.

Définition 1.3.5. *Soit $P \in K[X]$. On va dire que P est un polynôme unitaire si le coefficient dominant de P est 1_K.*

Définition 1.3.6. *Soit $P, Q \in K[X]$ deux polynômes. On dit que Q divise P et on écrit $Q|P$ s'il existe $B \in K[X]$ tel que $P = QB$.*

Définition 1.3.7. *Soit $P, Q \in K[X] \setminus \{0\}$. On dit que H est un **plus petit diviseur commun** de P et Q si $H|P$, $H|Q$ et pour tout H' tel que $H'|P$ et $H'|Q$, on a $H'|H$.*

Ce H n'est pas unique, tout produit de H et une constante $a \neq 0$ est aussi un plus grand diviseur commun. Mais c'est tout, si H' est un *pgcd* de P et Q, alors il existe $a \in K^*$ tel que $H' = aH$. Donc on va écrire $H = \mathbf{pgcd}(P, Q)$ si en plus H est unitaire.

Théorème 1.3.5. *Soit $P, Q \in K[X] \setminus \{0\}$, et soit I l'idéal engendré par P et Q. Soit H un générateur de I unitaire, alors $H = pgcd(P, Q)$.*

Démonstration. Les polynômes P et Q appartiennent à I, et H est un générateur, H divise P et Q. Comme $H \in I$, $H = AP + A'Q$. Soit H' un diviseur de P et de Q. Alors il existent $B, B' \in K[X]$ tels que $P = BH'$ et $Q = B'H'$. On a

$$H = AP + A'Q = ABH' + A'B'H' = H'(AB + A'B')$$

et donc H' divise H. On a donc $H = pgcd(P, Q)$. □

Remarque 7. *On peut definir $pgcd(P_1, \ldots, P_n)$ de la même façon, et montrer que si I est un idéal endendré par $P_1, \ldots, P_n$ et si H est un générateur unitaire de I alors $H = pgcd(P_1, \ldots, P_n)$.*

Définition 1.3.8. *Deux polynômes P et Q dans $K[X]$ sont premiers entre eux si $pgcd(P, Q) = 1_K$.*

Décomposition unique des polynômes

Définition 1.3.9. *Un polynôme $P \in K[X]$ est **irreductible** dans $K[X]$ si $deg(P) \geq 1$ et pour tout factorisation $P = QR$ avec $Q, R \in K[X]$, on a $deg(Q) = 0$ ou $deg(R) = 0$ (Q est constante ou R est constante).*

Exemple 1.3.4. *$P = X^2 + 1$ est irreductible dans $\mathbb{Q}[X]$ et $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$.*

Exemple 1.3.5. *Si $K = \mathbb{Z}/2\mathbb{Z}$, on peut aussi considérer $P = X^2 + 1 \in K[X]$. P n'est pas irréductible dans $K[X]$ parce que on a $(1+X)(1+X) = 1 + 2X + X^2 = 1 + X^2$. Par exemple $P = X^2 + X + 1$ est irréductible sur K.*

Exemple 1.3.6. *Polynômes de degré 1 sont toujours irréductibles parce que si $P = QR$, on a $1 = deg(Q) + deg(R)$. Si $K = \mathbb{C}$, les seuls polynômes irréductibles sont ceux de degré 1.*

Théorème 1.3.6. *Soit $P \in K[X]$ un polynôme non nul. Alors P se décompose de manière unique à ordre prés sous la forme*

$$P = cP_1^{k_1}P_2^{k_2}\dots P_n^{k_n},$$

où $c \in K^*$, $\alpha \in \mathbb{N}^*$ et les $P_i \in K[X]$ sont des polynômes unitaires, distincts et irréductibles dans $K[X]$.

Pour démontrer le théorème on a besoin de lemme suivant.

Lemme 1.3.3. *Soit H un polynôme irréductible dans $K[X]$. Soit $P, Q \in K[X] \setminus \{0\}$ tels que H divise PQ. Alors H divise P ou H divise Q.*

Démonstration. Comme H divise PQ, il existe $C \in K[X]$ tel que $CH = PQ$. Supposons que H ne divise pas P. Alors $pgcd(H, P) = 1_K$ et donc il existe $A, B \in K[X]$ tels que $1_K = AH + BP$. En multipliant par Q on obtient

$$Q = QAH + QBP = QAH + BCH = (QA + BC)H$$

et donc H divise Q. □

Démonstration du Théorème. Montrons d'abord qu'une tell décomoposition existe. Soit $P \in K[X]$ de degré $n \geq 1$. Si P est irreductible, on écrit $P = a_nP_1$ où $P_1 = a_n^{-1}P$. On suppose donc que P n'est pas irréductible dans $K[X]$. Alors on peut écrire

$$P = QR$$

où $deg(Q) < n$ et $deg(R) < n$. Démonstration est par récurrence. Les polynômes de degré 1 sont irréductibles. Supposons que la décomposition existe pour tous les polynomes de degré $2 \leq k \leq n-1$. Donc on peut décomposer Q et R sous forme de produit des polynômes irréductibles dans $K[X]$ et donc $P = QR$ se décompose aussi sous cette forme (on multiplie les décompositions corréspondants et on fait le ménage).

Le fait que la décombposition est unique se démontre en appliquant successivement le Lemme précédant. (en exercice)

□

Corollaire 1.3.4. *Soit K un corps algébriquement clos et $P \in K[X]$. Alors P se décompose sous forme*

$$P = c(X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2}\dots(X - \alpha_n)^{k_n},$$

où $\alpha_i \in K$ et $c \in K^*$.

Définition 1.3.10. *Soit $P \in K[X]$ et $\alpha \in K$ un racine de P. Soit m tel que $P = (X-\alpha)^m Q$ où $pgcd((X-\alpha), Q) = 1$, alors on dit que α est de **multiplicité** m. Si $m = 1$, on dit que α est une racine **simple**.*

Définition 1.3.11. *Soit $P = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$ un polynôme dans $K[X]$. Le polynôme dérivé de P est $P' = na_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$.*

On a les propriétés habituelles :

Lemme 1.3.4. *Soit $P, Q \in K[X]$ et $c \in K$. On a*

1. $(cP)' = cP'$,
2. $(P+Q)' = P' + Q'$,
3. $(PQ)' = P'Q + PQ'$.

Démonstration. En exercice □

Théorème 1.3.7. *Soit $P \in K[X]$ et $deg(P) \geq 1$ et soit $\alpha \in K$ une racine de P. Alors α est de multiplicité > 1 si et seulement si α est une racine de P'.*

Anneaux quotients

On a vu pour les anneaux en général que si A est un anneau commutatif, et I un idéal de A, alors A/I est un corps si et seulement si I est maximal (voir Feuille 9). L'anneau $K[X]$ est commutatif, et on voudrait voir quels idéax sont maximaux dans $K[X]$.

Lemme 1.3.5. *Un idéal I de $K[X]$ est maximal si et seulement si I est engendré par un polynôme irréductible.*

Démonstration. Soit $P \in K[X]$ un polynôme de degré ≥ 1. Soit I_p l'idéal engendré par P. Il suffit de montrer que I_p est maximal. Comme les éléments de I_P sont les multiples de P, I ne contient pas de 1_K, et donc $I_P \neq K[X]$. Soit $J \subset K[X]$ un idéal qui contient I_P. Montrons que J est maximal. Soit H le generateur unitaire de J. Alors $H|P$. Comme P est irreductible, $H = 1_K$ ou $H = P$. Comme I_P n'est pas egal à J, $H \neq P$. Donc $H = 1_K$. Mais s'idéal engendré par 1_K est égal à K. On a montré que I_P est maximal.

□

1.4 Espaces Vectoriels

Soit K un corps. Un espace vectoriel sur K est un ensemble V muni d'une LCI notée $+$ et d'une loi externe $\cdot : V \times K \to V$ qui satisfont

1. $(V, +)$ est un groupe abélien
2. Pour tout $x, y \in V$ et $a, b \in K$ on a
   a) $a \cdot (x + y) = a \cdot x + a \cdot y$;
   b) $(a + b) \cdot x = a \cdot x + b \cdot y$;
   c) $a \cdot (b \cdot x) = (ab) \cdot x$;
   d) $1_K \cdot x = x$

Remarque 8. *Notez que les deux dernières conditions impliquent que K agit sur V.*

On appelle les éléments de V *vecteurs* et les éléments de K *scalaires.*

Exemple 1.4.1. *$V = \{f : [0, 1] \to \mathbb{R}$ continue $\}$ est un espace vectoriel sur $\mathbb{R}$.*

Exemple 1.4.2. *Soit E un ensemble non-vide, K un corps et*

$$V = \{f : E \to K\}$$

l'ensemble des applications de V dans K. Alors V est un espace vectoriel sur K.

Exemple 1.4.3. *Soit $V = K^n = \{(x_1, \ldots, x_n) |\ x_i \in K\}$. Alors V est un espace vectoriel sur K.*

Voici quelques propriétés immédiates.

Proposition 1.4.1. *Soit V un espace vectoriel sur K et 0 l'élément neutre pour l'addition.*

- *Pour tout $v \in V$ on a $0_K v = 0$.*
- *Pour tout $c \in K$ on a $c0 = 0$.*
- *Si $c \in K^*$, $v \in K$ et $cv = 0$, alors $v = 0$.*
- *Pour tout $v \in V$, on a $(-1_K)v = -v$.*

Démonstration.

- On écrit $0_K v + v = (0_K + 1_K)v = 1_K v = v$ d'où $0_K v = 0$.
- $c\,0 = c(x - x) = cx - cx = 0$.

— Si $c \neq 0_K$, alo,,rs c admet un inverse multiplicatif. Alors $v = 1_K v = (c^{-1}c)v = c^{-1}(cv) = c^{-1}0 = 0$.
— On a $v + (-1_K)v = 1_K v + (-1_K)v = (1_K - 1_K)v = 0$. Donc $-1_K)v = -v$.

□

Définition 1.4.1. *Soit V un espace vectoriel sur K et W un sous-ensemble de V. On dit que W est un **sous-espace vectoriel** de V si*

1. *$(W, +)$ est un sous-groupe de $(V, +)$.*
2. *$\forall c \in K$ et $w \in W$, on a $cw \in W$.*

On peut également définir un sous-espace W comme un sous-ensemble de V contenant 0, tel que si $v, w \in W$ alors $v + w \in W$ et si $c \in K$ et $w \in W$ alors $cw \in W$. On vérifie que W est aussi un espace vectoriel sur K.

Définition 1.4.2. *Soit V un espace vectoriel sur K et $\{v_i\}_{i\in I}$ une famille dans V. Une combinaison linéaire des $\{v_i\}_{i\in I}$ est toute somme $\sum_{i\in I} c_i v_i$ où les coéfficients $c_i \in K$ sont tous nuls sauf un nombre fini.*

Exemple 1.4.4. *Soit V un espace vectoriel sur K et $\{v_i\}_{i\in I}$ dans V. On considère l'ensemble W des combinaisons linéaires des vecteurs $(v_i)_{i\in I}$, i.e.*

$$W = \{\sum_{i\in I} c_i v_i |\ \ c_i \in K \text{ ou } c_i = 0_K \text{ sauf un nombre fini}\}.$$

On vérifie facilement que W est un sous-espace vectoriel de V.(en exercice) On dit que W est engendré par les éléments $\{v_i\}_{i\in I}$ et que la famille $\{v_i\}_{i\in I}$ est une famille generatrice sont des de W. On écrit aussi $W = Vect(\{v_i\}_{i\in I})$.

Définition 1.4.3. *Soit V un espace vectoriel sur K. On dit que vecteurs $\{v_i,\}_{i\in I}$ dans V sont **linéairement dépendants sur** K s'il existe $\{c_i\}_{i\in I}$ dans K tels que $c_i \neq 0_K$ pour au moins un $i \in I$ et tels que*

$$\sum_{i\in I} c_i v_i = 0.$$

*S'il n'existe pas de tels $\{c_i\}_{i\in I}$ dans K, on dit que les vecteurs $\{v_i\}_{i\in I}$ sont **linéairement indépendants sur** K ou que la famille $\{v_i\}_{i\in I}$ est libre.*

Exemple 1.4.5. *Soit $V = K^n$. Les éléments $v_1 = (1, 0, \ldots, 0), \ldots, v_n = (0, 0, \ldots, 1)$ sont linéairement indépendants. (Pourquoi ?)*

Exemple 1.4.6. *$V = K[X]$ est un espace vectoriel sur K. Les polynômes $\{P_i = X^i\}_{i=1}^n$ pour $n \in \mathbb{N}$ sont linéairement indépendants.*

Définition 1.4.4. *Soit V un espace vectoriel sur K. Une famille libre des vecteurs $\{v_i\}_{i\in I}$ est* ***une base*** *de V si $V = Vect(\{v_i\}_{i\in I})$.*

Proposition 1.4.2. *Soit V un espace vectoriel sur K et soit $\{v_i\}_{i\in I}$ une famille libre dans V. Soit $w = \sum_{i\in I} c_i v_i$ une combinaison linéaire des vecteurs v_i. Si $w = \sum_{i\in I} b_i v_i$ alors $c_i = b_i$ pour tout $i \in I$. Autrement dit, si $w \in Vect(\{v_i\}_{i\in I})$ alors w s'écrit de manière unique comme combinaison linéaire des $\{v_i\}_{i\in I}$.*

Démonstration. Soit $\sum_{i\in I} b_i v_i = \sum_{i\in I} c_i v_i$, alors $\sum_{i\in I}(b_i - c_i)v_i = 0$. Comme les vecteurs $\{v_i\}_{i\in I}$ sont linéairement indépendants, on a $b_i = c_i$ pour tout $i \in I$. □

Si $\{v_i\}_{i\in I}$ est une base d'un espace vectoriel V, et $w = \sum c_i v_i \in V$, on appelle les coéfficients c_i les coordonnées de w dans la base $\{v_i\}_{i\in I}$

Exemple 1.4.7. *Soit $V = K^n$. Les vecteurs $(1, 0, \ldots, 0), \ldots (0, 0, \ldots, 1)$ forment une base de V.*

Définition 1.4.5. *Soit V un espace vectoriel. S'il existe une famille finie des vecteurs $v_i \in V$ qui engendrent V, on dit que V est de* ***dimension finie****. Sinon, V est de* ***dimension infinie****.*

Exemple 1.4.8. *L'espace vectoriel $K[X]$ sur K est de dimension infinie.*

Nous allons donner une définition de dimension plus tard. Nous allons maintenant montrer qu'un espace vectoriel de dimension finie admet une base. (C'est vrai aussi en dimension infinie, mais la démonstration est plus compliqueée).

Soit $\{v_1, \ldots, v_n\}$ des vecteurs dans un espace vectoriel V. On appelle un sous-ensemble $\{w_1, w_2, \ldots, w_r\} \subset \{v_1, \ldots, v_n\}$ famille maximale libre si les vecteurs $\{w_1, \ldots, w_r\}$ sont linéairement indépendants et si tout vecteur $v_j \notin \{w_1, \ldots, w_r\}$ est une combinaison linéaire des $\{w_1, \ldots, w_r\}$. Une telle famille existe toujours. Voici une recette. On commence par v_1. Si $v_1 \neq 0$, on pose $w_1 = v_1$, sinon w_1 est le premier vecteur $v_k \neq 0$. w_2 est le premier vecteur (apres w_1) qui n'est pas une combinaison linéaire des vecteurs précedants. A la fin on prend tous les vecteurs de la liste $\{v_1, \ldots, v_n\}$ qui ne sont pas combinaisons linéaires des vecteurs précedants.

Proposition 1.4.3. *Soit V un K-espace vectoriel de dimension finie et soit $\{v_1, \ldots, v_n\}$ une famille génératrice de V. Soit $\{w_1, w_2, \ldots, w_r\} \subset \{v_1, \ldots, v_n\}$ une famille maximale des vecteur linéairement indépendants. Alors la famille $\{w_1, w_2, \ldots, w_r\}$ est une base de V.*

Démonstration. Pour simplifier la présentation, nous allons supposer que $w_1 = v_1, w_2 = v_2, \ldots, w_r = v_r$. Il faut montrer que cette famille engendre V. Soit $u \in V$. Alors $u = \sum_{i=1}^{n} c_i v_i$. Supposons que $c_{r+j} \neq 0$, pour $1 \leq j \leq n-r$. Le vecteur v_{r+j} est une combinaison linéaire des $v_1, \ldots v_r$, donc on peut écrire $v_{r+j} = \sum_{i=1}^{r} a_i^j v_i$. Alors dans l'expression pour u on remplace v_{r+j} par la combinaison linéraire correspondante :

$$u = c_1 v_1 + \ldots c_r v_r + c_{r+1} \sum_{i=1}^{r} a_i^1 v_i + \ldots + c_n \sum_{i=1}^{r} a_i^{n-r} v_i.$$

□

Donc tout espace vectoriel de dimension finie admet une base.

Définition 1.4.6. *Soit V, W deux espaces vectoriels sur un corps K. Une application $\phi : V \to W$ est dite linéaire ou morphisme des espaces vectoriels si*

1. *$\forall x, y \in V$, on a $\phi(x+y) = \phi(x) + \phi(y)$.*
2. *$\forall x \in V, c \in K$, on a $\phi(cx) = c\phi(x)$.*

Exemple 1.4.9. *On connait deja les applications linéaires de $\mathbb{R}^n \to \mathbb{R}^n$.*

Exemple 1.4.10. *Voici un exemple de l'analyse. Soit $V = C^\infty(\mathbb{R})$ fonctions de $\mathbb{R}$ dans $\mathbb{R}$ telles que $f^{(n)}$ existe pour tout $n \in \mathbb{N}$. Alors V est un espace vectoriel. (pourquoi ?) Soit $D : V \to V$ l'application définie par $D(f) = f'$. Alors D est linéaire.*

Proposition 1.4.4. *Soit V, W et U des espaces vectoriels sur un corps K. Soit $\phi : V \to W$ et $\psi : W \to U$ des applications linéaires. Alors l'application $\phi \circ \phi : V \to U$ est une application linéaire.*

Démonstration. Soit $v_1, v_2 \in V$. Alors

$$\begin{aligned}&(\psi \circ \phi)(v_1 + v_2) = \\ &\psi(\phi(v_1 + v_2)) = \psi(\phi(v_1) + \phi(v_2)) = \psi(\phi(v_1)) + \psi(\phi(v_2)) \\ &= (\psi \circ \phi)(v_1) + (\psi \circ \phi)(v_2).\end{aligned}$$

Pour $c \in K$ et $v \in V$, on a

$$(\psi \circ \phi)(cv) = \psi(\phi(cv)) = \psi(c\phi(v)) = c\psi(\phi(v)) = c(\psi \circ \phi)(v).$$

□

On définit le **noyau** et **l'image** d'une application linéaire comme d'habitude : si $\phi : V \to W$ est une application linéaire, alors le noyau $Ker(\phi) = \{v \in V |\ \phi(v) = 0\} \subset V$. L'image $Im(\phi) = \{\phi(v) \mid v \in V\} \subset W$.

Proposition 1.4.5. *Le noyau $Ker(\phi)$ d'une application linéaire $\phi : V \to W$ est un sous-espace vectoriel de V. L'image $Im(\phi)$ est un sous-espace vectoriel de W.*

Démonstration. En exercice □

Proposition 1.4.6. *Une application linéaire $\phi : V \to W$ est injective si et seulement si $Ker(\phi) = \{0\}$.*

Exercice 1.4.1. *Soit $\phi : V \to W$ une application lin'éaire. Montrer que si ϕ est bijective, alors son inverse est une application linéaire de W dans V.*

On peut alors définir un isomorphisme entre des espaces vectoriels.

Définition 1.4.7. *Une application linéaire $\phi : V \to W$ est un isomorphisme des espaces vectoriels V et W si ϕ est une bijection.*

Théorème 1.4.1. *Soit V, W des espaces vectoriels sur K, et $\{v_1, v_2, \ldots, v_n\}$ une base the V. Alors pour toute famille $\{w_1, \ldots, w_n\}$ de vecteurs dans W il existe une unique application linéaire $\phi : V \to W$ telle que $\phi(v_i) = w_i$ pour tout $1 \leq i \leq n$.*

Démonstration. Une telle application est unique parce que si $x \in V$, alors x est une combinaison linéaire de $\{v_1, \ldots, v_n\}$, et donc $x = a_1v_1 + \ldots + a_nv_n$, et sont image par ϕ est forcement $\phi(x) = a_1w_1 + \ldots + a_nw_n$.

Une telle application linéaire existe : pour tout $x = a_1v_1 + \ldots + a_nv_n$, on pose $\phi(x) := a_1w_1 + \ldots + a_nw_n$. Il nous reste à vérifier que ϕ est linéaire.

Soit $x, y \in V$, et on écrit $x = a_1v_1 + \ldots + a_nv_n$ et $y = b_1v_1 + \ldots + b_nv_n$. Alors $\phi(x+y) = (a_1+b_1)v_1 + \ldots + (a_n+b_n)w_n = a_1w_1 + \ldots + a_nw_n + b_1w_1 + \ldots b_nw_n = \phi(x) + \phi(y)$. De la même manière on montre que $\phi(cx) = c\phi(x)$ pour tout $c \in K$. □

Soit V, W des espaces vectoriels sur K. On dénote

$$Hom_K(V, W) = \{\phi : V \to W \text{ application linéaire }\}$$

l'ensemble de toutes les applications linéaires de V dans W. Si $V = W$, on dénote $End(V) = Hom(V, V)$ et on appelle **endomorphismes de** V les éléments de $End(V)$.

On peut montrer que $Hom_K(V,W)$ est un espace vectoriel sur K. En effet, pour $\phi, \psi \in Hom_K(V,W)$ et $c \in K$, on définit $\phi + \psi$ par $(\phi + \psi)(x) = \phi(x) + \psi(x)$, pour tout $x \in V$ et $c\phi$ par $(c\phi)(x) = c\phi(x)$.

Exercice 1.4.2. *Montrer que $Hom_K(V,W)$ est un espace vectoriel sur K.*

Théorème 1.4.2. *Soit V un espace vectoriel sur un corps K. Soit $\{v_1, \ldots, v_n\}$ linéairement indépendants dans V. Soit $\{w_1, \ldots w_m\}$ une famille génératrice de V. Alors $n \leq m$.*

Démonstration. Comme $V = Vect(w_1, \ldots, w_m)$ et les vecteurs v_i sont dans V, on peut écrire

$$\begin{aligned} v_1 &= a_{11}w_1 + a_{21}w_2 + \ldots + a_{m1}w_m \\ v_2 &= a_{12}w_1 + a_{22}w_2 + \ldots + a_{m2}w_m \\ &\ldots \\ v_n &= a_{1n}w_1 + a_{2n}w_2 + \ldots + a_{mn}nw_m \end{aligned}$$

Comme $v_1 \neq 0$, a_{i1} est non nul pour au moins un i. Pour simplifier la présentation, supposons que a_{11} est non nul, et donc admet un inverse multiplicatif (noté $\frac{1}{a_{11}}$). Alors on peut écrire w_1 comme une combinaison linéaire de $v_1, w_2, \ldots, w_m$:

$$w_1 = \frac{1}{a_{11}}v_1 - \frac{a_{21}}{a_{11}}w_2 - \ldots - \frac{a_{m1}}{a_{11}}w_m.$$

Dans l'expression pour v_2 on remplace w_1 par la combinaison linéaire ci-dessus. Alors v_2 est une combinaison linéaire de $v_1, w_2, \ldots w_m$. Écrivons cette combinaison linéaire :

$$v_2 = b_1v_1 + b_2w_2 + \ldots + b_mw_m$$

Il existe un indice $2 \leq i \leq m$ tel que le coefficient devant w_i est non nul. Pour simplicité supposons que $b_2 \neq 0$ et écrivons

$$w_2 = -\frac{b_1}{b_2}v_1 + \frac{1}{b_2}v_2 - \ldots - \frac{b_m}{b_2}v_m.$$

Donc $w_2 \in Vect(v_1, v_2, w_3 \ldots w_m)$. Mais v_3 est donc aussi dans $Vect(v_1, v_2, w_3 \ldots w_m)$. On donc écrit

$$v_3 = c_1v_1 + c_2v_2 + c_3w_3 + \ldots + c_mw_m.$$

Comme v_3 n'est pas une combinaison linéaire de v_1 et v_2, il y a un indice $3 \leq i \leq m$ tel que a_i est non-nul. On suppose que $i = 3$ (mais rien ne change

si $i \neq 3$). On remarque que $w_3 \in Vect(v_1, v_2, v_3, w_4, \ldots, w_m)$, puis que $v_4 \in Vect(v_1, v_2, v_3, \ldots, w_m)$. On continue de cette manière en remplaçant w_i par v_i. Si $m < n$, on arrivera a la situation quand on a $v_n \in Vect(v_1, v_2, \ldots v_{n-1})$ et ça contredit l'hypothèse que $(v_1, v_2, \ldots, v_n)$ sont linéairement indépendants. □

Théorème 1.4.3. *Soit V un espace vectoriel. Si $\{v_1, \ldots, v_n\}$ et $\{w_1, \ldots, w_m\}$ sont des bases de V, alors $n = m$.*

On a donc montré que toute base d'un espace vectoriel V de dimension finie contient le même nombre d'éléments. On appelle ce nombre **la dimension de** V et on la dénote $dim(V)$. Si $V = \{0\}$, on définie $dim(V) = 0$.

Théorème 1.4.4. *Soit V, W deux espaces vectoriels sur K et $\phi : V \to W$ une application linéaire. Supposons que V et W sont de dimension finie et $dimV = dimW$. Si $Ker(\phi) = \{0\}$ ou si $Im(\phi) = W$, alors ϕ est un isomorphisme.*

Corollaire 1.4.1. *Soit V, W espaces vectoriels sur K, de dimension finie et tels que $dimV = dimW$. Alors V et W sont isomorphes.*

En particulier, tout espace vectoriel V sur un corps K de dimension $n > 0$ est isomorphe à l'espace K^n.

Matrices

On a déjà vu matrices à coéfficients dans $\mathbb{R}$. Voici une définition plus général Soit K un corps. Une **matrice** A de taille $m \times n$ est un tableau

$$A = \begin{pmatrix} a_{11} & a_{12} & .. & .. & .. & a_{1n} \\ a_{21} & a_{22} & .. & .. & .. & .. \\ .. & .. & .. & .. & .. & .. \\ .. & .. & .. & .. & .. & .. \\ a_{m1} & .. & .. & .. & .. & a_{mn} \end{pmatrix}$$

où $a_{ij} \in K$ pour $1 \leq i \leq m$ et $1 \leq j \leq n$. On dénote $M_{m,n}(K)$ l'ensemble des matrices des taille $m \times n$ à coéfficients dans K. Si $m = n$, on écrit tout simplement $M_n(\mathbb{R})$.

Comme dans le cas $K = \mathbb{R}$, on définit $A + B$ pour $A, B \in M_{m,n}(K)$, kA pour $k \in K$ et $A \in M_{m,n}(K)$. La matrice $0 \in M_{m,n}(K)$ est la matrice dont tout les coéfficients sont zéros.

Proposition 1.4.7. *$M_{n,k}(K)$ est un espace véctoriel sur K.*

On peut aussi définir le produit des deux matrices : si A est de taille $m \times n$ et B de taille $n \times k$, alors leur **produit** AB est une matrice de taille $m \times k$ définie par $c_{ij} = \sum_{l=1}^{n} a_{ij} b_{jk}$.

En particulier on peut multiplier éléments de $M_n(K)$.

Proposition 1.4.8. *Soit K un corps et $n \in \mathbb{N}^*$. Alors $(M_n(K), +, \cdot)$ est un anneau.*

Comme pour $K = \mathbb{R}$, à toute application linéaire on associe une matrice. Ici nous décrivons la corréspondance entre matrices et applications linéaires pour K un corps arbitraire. D'abord, nous allons identifier un espace vectoriel K^n avec $M_{n,1(K)}$ pour tout $n \in \mathbb{N}^*$ par

$$(x_1, x_2, \ldots, x_n) \mapsto \begin{pmatrix} x_1 \\ x_2 \\ .. \\ .. \\ x_n \end{pmatrix}.$$

Soit $A \in M_{m,n}(K)$. Alors A définit une application $\phi_A : K^n \to K^m$ par

$$\phi_A(\bar{x}) = A \begin{pmatrix} x_1 \\ x_2 \\ .. \\ .. \\ x_n \end{pmatrix}.$$

Théorème 1.4.5. *L'association $A \mapsto \phi_A$ est un isomorphisme des espaces vectoriels entre $M_{m,n}(K)$ et $Hom(K^n, K^m)$.*