Faculté des sciences
Département de Mathématiques
HAX501X

Année 2021–2022

Introduction à la théorie des groupes et des anneaux

Polycopié de cours

P.-L. Montagard

Table des matières

Chapitre 1

Théorie des Groupes, une introduction

Nous allons commencer par définir la notion de groupe, ainsi que les notions associées, puis après avoir défini quelques exemples, nous montrerons les premiers résultats sur les cardinaux des groupes finis. À cette occasion, nous verrons que l'arithmétique de $\mathbb{Z}$ intervient de manière importante dans l'étude des groupes finis.

1.1 Loi sur un ensemble

Avant de définir la notion de groupe, nous allons rappeler la notion générale de loi sur un ensemble.

Définition 1.1.1. On dit qu'un ensemble G est muni d'une loi, s'il existe une application :

$$\begin{array}{rccc} \varphi & : & G \times G & \to & G \\ & & (s,t) & \mapsto & \varphi(s,t) \end{array}.$$

On notera sous forme de couple (G, φ) un tel ensemble.

Une loi sur un ensemble est donc simplement une procédure qui à partir de deux éléments de G en construit un troisième. On peut facilement donner des exemples.

Exemple(s) 1.1.1.

1. Si $G = \{e\}$ est un ensemble à un seul élément, alors il existe une seule loi sur $\{e\}$ définie par $\varphi(e, e) = e$.
2. Sur l'ensemble des réels $\mathbb{R}$, on peut définir les deux lois suivantes : pour tout $(x, y) \in \mathbb{R}$, $\varphi(x, y) = x + y$ et $\varphi(x, y) = xy$. On peut remplacer $\mathbb{R}$ par un autre corps $\mathbb{Q}, \mathbb{C}$ ou par un anneau $\mathbb{Z}, \mathbb{D}$.
3. Soient $\mathbb{K}$ un corps et E un espace vectoriel sur $\mathbb{K}$, l'addition des vecteurs est une loi. Par contre, la multiplication par un scalaire n'est pas une loi au sens de la définition vue ici. On utilise la dénomination loi *externe*.
4. Soient X un ensemble et $E = \mathrm{End}(X)$ l'ensemble des applications de X dans lui-même, alors la composition qui à tout couple $(f, g) \in E$ associe l'élément $\varphi(f, g) = f \circ g$ est une loi sur E.
5. Soit X un ensemble, l'ensemble des suites finies d'éléments de X, noté $\mathscr{M}(X)$ s'appelle l'ensemble des mots en l'alphabet X. Le nombre de termes de la suite est appelé longueur du mot. Par exemple si $X = \{a, b\}$ alors les éléments aba et $abba$ sont des mots de longueur respectives 3 et 4. Notons qu'il existe un mot de longueur 0, c'est le mot vide. Sur l'ensemble $G = \mathscr{M}(X)$, on peut définir une loi par juxtaposition (on dit aussi concaténation) ; par exemple $\varphi(aba, abba) = abaabba$. Ceci définit bien une loi sur G.

Remarque(s) 1.1.1. En général, tout comme dans les exemples ci-dessus, on utilise plutôt une notation "binaire" du type $x * y, x + y, xy, x \times y$ pour désigner l'élément $\varphi(x, y)$.

1.2 Définition de groupe

Nous allons maintenant définir la notion de groupe.

Définition 1.2.1. Soit $(G, *)$ un ensemble muni d'une loi. On dit que G est un groupe, si les trois axiomes suivants sont vérifiés :

1. Il existe un élément $e \in G$, appelé l'élément neutre de G tel que pour tout $g \in G$: $g * e = e * g = g$.
2. Soit e un élément neutre pour G, alors pour tout élément $s \in G$ il existe un élément $t \in G$, que tel que $s * t = t * s = e$; un tel élément est appelé un inverse de s.
3. Pour tout triplet $(s, t, u) \in G^3$ l'égalité suivante est vérifiée :

$$(s * t) * u = s * (t * u) \ ;$$

   on dit que la loi $*$ est associative.

Si de plus, pour tout $(s, t) \in G^2$ on a l'égalité $s * t = t * s$ on dira que $(G, *)$ est un groupe commutatif (ou abélien).

Comme nous allons le voir dans la propriété qui suit, le choix de l'élément neutre e pour énoncer l'existence d'un élément symétrique est superflu.

Propriété 1.2.1. *Soit $(G, *)$ un groupe, alors on a les deux propriétés suivantes :*

1. *Il existe un unique élément neutre dans G.*
2. *Tout élément $s \in G$ admet un unique inverse.*

Démonstration. Soit $e, e' \in G$ deux éléments neutres ; alors par définition pour tout $g \in G$, on a : $e * g = g * e = g$ et $e' * g = g * e' = g$. En particulier, $e * e' = e$ et $e * e' = e'$ ce qui montre le premier point. Pour le deuxième point, soient $s \in G$ et t, t' deux inverses de s. On a donc les égalités : $s * t = t * s = e$ et $s * t' = t' * s = e$; on en déduit les deux égalités suivantes : $t * (s * t') = t * e = t$ et : $(t * s) * t' = e * t' = t'$.
Mais par la propriété d'associativité $t * (s * t') = (t * s) * t'$ d'où $t = t'$. □

Dans le même ordre d'idée, pour vérifier que s est l'inverse de t une seule égalité suffit.

Propriété 1.2.2. *Soient $(G, *)$ un groupe et $(s, t) \in G^2$ tel que $s * t = e$, alors $t * s = e$ et donc $s = t^{-1}$.*

Démonstration. Comme dans la preuve de la proposition précédente, on calcule $s * t * s$ de deux façons. D'une part $s * t * s = (s * t) * s = s$ et $s * t * s = s * (t * s)$. D'où $s = s * (t * s)$ et on conclut en multipliant à gauche par s^{-1}. □

Exemple(s) 1.2.1. Parmi les exemples d'ensemble muni d'une loi, certains sont des groupes.

1. Tout ensemble muni d'un seul élément $\{e\}$ avec la loi $e * e = e$ est un groupe. Ce groupe est appelé le groupe trivial.
2. L'ensemble des réels muni de l'addition est un groupe ; 0 est l'élément neutre et l'inverse de $x \in \mathbb{R}$ est l'opposé $-x$.

   Par contre $\mathbb{R}$ muni de la multiplication n'est pas un groupe ; 0 n'a pas d'inverse ; mais l'ensemble $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ est bien un groupe avec 1 comme élément neutre. Ici on peut remplacer $\mathbb{R}$ par n'importe quel corps comme $\mathbb{Q}$ ou $\mathbb{C}$.

   Pour un anneau $\mathbb{A}$, la situation est légèrement différente : les couples $(\mathbb{A}, +)$ et $(\mathbb{A}^\times, \times)$ sont des groupes, où $\mathbb{A}^\times$ est l'ensemble des éléments inversibles de $\mathbb{A}$ pour la multiplication, par exemple $\mathbb{Z}^\times = \{\pm 1\}$.
3. Si V est un espace vectoriel sur un corps $\mathbb{K}$, alors l'addition est une loi de groupe commutatif sur V.
4. Si X est un ensemble, alors l'ensemble $E = \mathrm{End}(X)$ muni de la loi de composition des applications n'est pas un groupe ; mais le sous-ensemble de E des applications bijectives de X dans lui-même est bien un groupe pour cette loi. Cet ensemble sera noté $\mathrm{Bij}(X)$ ou Σ_X. L'élément neutre est l'application identité que l'on notera $\mathbb{1}_X$, et l'inverse de $f \in \Sigma_X$ est l'application réciproque de f.
5. Les premiers exemples sont des groupes commutatifs (on dit aussi groupes abéliens) ; par contre, si le cardinal de X est plus grand que 3 alors Σ_X n'est pas commutatif (voir l'exercice en TD).

Remarque(s) 1.2.1. 1. En pratique, la notation $*$ est rarement employée. En général, la loi est notée avec un point, ou même par simple juxtaposition (le produit de a par b est noté ab). Dans ce cas, on peut aussi utiliser le symbole 1 pour l'unité. L'inverse d'un élément a est noté a^{-1} et si n est un entier positif, a^n désigne le produit de a par lui-même n fois. En posant $a^{-n} = (a^{-1})^n$, et $a^0 = e$ on étend cette notation à tous les entiers relatifs. Les relations usuelles sur les puissances entières pour $\mathbb{R}$ sont vraies dans un groupe, à savoir :

$$a^n a^m = a^{n+m} \text{ et } (a^n)^m = a^{nm}.$$

On utilise aussi fréquemment le symbole $+$, mais l'usage de celui-ci est réservé aux lois commutatives. Dans ce cas, on note 0 l'élément neutre et na la composition de a avec lui-même n fois.

2. Le cardinal de l'ensemble G s'appelle aussi l'ordre du groupe $(G, *)$. On le notera ici : $|G|$.
3. *Quelques règles de calculs.* Soit G un groupe dont la loi est notée par concaténation et d'élément neutre e. Voici quelques règles à retenir :
   (i) Produits de n termes : soit $(g_1, \dots, g_n) \in G^n$, alors par associativité, dans le produit $(((\cdots(g_1g_2)g_3)\cdots)g_n)$, on peut modifier à sa guise les parenthèses. Tous ces produits sont égaux et seront notés $g_1 \dots g_n$.
   (ii) Simplification à droite : pour tout $(g, s, t) \in G^3$, $gs = ts \Leftrightarrow g = t$;
   (iii) Simplification à gauche : pour tout $(g, s, t) \in G^3$, $sg = st \Leftrightarrow g = t$;
   (iv) Inverse d'un produit : Pour tout $(s, t) \in G^2$, l'inverse du produit st est égal au produit $t^{-1}s^{-1}$. Plus généralement l'inverse du produit $g_1 \dots g_n$ est égal à $g_n^{-1} \dots g_1^{-1}$ (attention à l'ordre des facteurs dans l'inverse).

1.3 Sous-groupe, morphismes, produit

Si G est un groupe, et H un sous-ensemble de G, on peut se demander si H lui-même est un sous-groupe (muni de la restriction de la loi sur G), ce qui conduit à la définition suivante.

Définition 1.3.1. Soient $(G, *)$ un groupe et H une partie de G. On dit que H est un sous-groupe de G si H est non vide et si pour tout $(s, t) \in H^2$, on a $st^{-1} \in H$.

Remarque(s) 1.3.1. 1. La condition de stabilité peut être découplée en deux conditions. En effet il y a équivalence :

$$\forall (s, t) \in H^2,\ st^{-1} \in H \quad \Leftrightarrow \quad (\forall (s, t) \in H^2,\ st \in H) \text{ et } (\forall s \in H, s^{-1} \in H).$$

2. On peut donc paraphraser cette définition, en disant qu'une partie H de G est un sous-groupe si H est non vide, stable par multiplication et par passage à l'inverse.
3. Si H est un sous-groupe, alors la restriction de la loi de G à H est bien définie et fait de H un groupe d'élément neutre e, l'élément neutre de G.

   Si on doit vérifier qu'une partie H est un sous-groupe, il est pratique de regarder si l'élément neutre e appartient à G. Si ce n'est pas le cas H n'est pas un sous-groupe ; si c'est le cas, on a montré que H est non vide et il reste à vérifier la stabilité de la multiplication et par passage à l'inverse.
4. Pour montrer qu'un ensemble est un groupe, très souvent on montre que c'est un sous-groupe. Voici un exemple typique : si on considère V un espace vectoriel et $G = \mathrm{GL}(V)$ l'ensemble des applications linéaires et bijectives de V dans lui-même, alors G est un sous-ensemble de Σ_V, non vide puisqu'il contient l'identité, et comme la composée et l'inverse d'une application linéaire sont des applications linéaires, G est un sous-groupe de Σ_V, donc un groupe.

Comme pour les espaces vectoriels, la notion de sous-groupe se comporte bien par rapport aux intersections. On a la propriété suivante :

Propriété 1.3.1. *Soient G un groupe, I un ensemble et $(H_i)_{i\in I}$ un ensemble de sous-groupes de G, alors : $\cap_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. Comme $\cap_{i\in I} H_i$ contient l'identité, cet ensemble est non vide.

Soit $(x, y) \in \cap_{i\in I} H_i$, alors comme chacun des H_i est un sous groupe, pour tout $i \in I$, on a : $x \in H_i$ et $y^{-1} \in H_i$, et donc $\forall i \in I\ xy^{-1} \in H_i$, c'est à dire $xy^{-1} \in \cap_{i\in I} H_i$. □

Par contre, en général l'union de deux sous-groupes n'est pas un sous-groupe (voir l'exercice en TD).

Grâce à cette propriété sur l'intersection de deux sous-groupes, nous allons pouvoir définir le sous-groupe engendré par une partie. Commençons par un théorème.

Propriété 1.3.2. *Soit G un groupe et X une partie de G. Alors l'intersection de tous les sous-groupes contenant X est l'unique plus petit (pour l'inclusion) sous-groupe de G contenant X.*

Démonstration. Notons H l'intersection des sous-groupes contenant X. D'après la propriété 1.3.1, H est un sous-groupe. Soit H' un sous-groupe contenant X, alors par définition de H, on a $H \subset H'$. On en déduit immédiatement l'unicité de H. □

On peut donc parler du plus petit sous-groupe de G contenant X, on le notera $< X >_G$. En algèbre linéaire l'espace vectoriel engendré par une partie peut être défini de deux manières : d'une part comme le plus petit sous-espace contenant cette partie, d'autre part comme l'ensemble des combinaisons linéaires d'éléments de la partie. Nous allons voir un analogue de cette deuxième définition. Si X est une partie d'un groupe G, nous noterons X^{-1}, la partie définie par : $X^{-1} = \{g^{-1} \mid g \in X\}$. Enfin si X est une partie de G, alors l'ensemble des mots sur l'alphabet X peut être vu comme un élément de G si on remplace la juxtaposition par le produit de G. Par convention, le mot vide correspond à l'élément neutre de G. Par un abus de notation, ces mots en $X \subset G$, vus comme éléments de G seront notés de la même façon. On a le théorème suivant :

Théorème 1. *Soit X une partie d'un groupe G, alors le sous-groupe engendré par X est égal à l'ensemble des mots dans l'alphabet $X \cup X^{-1}$. Autrement dit,*

$$< X >_G = \mathscr{M}(X \cup X^{-1}).$$

Démonstration. On vérifie tout d'abord que $\mathscr{M}(X \cup X^{-1})$ est un sous-groupe. Soient x, y deux éléments de $\mathscr{M}(X \cup X^{-1})$, alors il existe deux entiers n et m, deux suites d'éléments de X : $s_1, \ldots, s_n$ et $t_1, \ldots, t_m$ et deux suites d'éléments de l'ensemble $\{\pm 1\}$: $\varepsilon_1, \ldots, \varepsilon_n$ et $\varepsilon'_1, \ldots, \varepsilon'_m$ tels que $x = s_1^{\varepsilon_1} \ldots s_n^{\varepsilon_n}$ et $y = t_1^{\varepsilon'_1} \ldots t_m^{\varepsilon'_m}$. Alors $y^{-1} = t_m^{-\varepsilon'_m} \ldots t_1^{-\varepsilon'_1}$ et $xy^{-1} = s_1^{\varepsilon_1} \ldots s_n^{\varepsilon_n} t_m^{-\varepsilon'_m} \ldots t_1^{-\varepsilon'_1}$ appartient à $\mathscr{M}(X \cup X^{-1})$. Par minimalité de $< X >_G$, on a l'inclusion $< X >_G \subset \mathscr{M}(X \cup X^{-1})$. Réciproquement, $< X >_G$ étant un sous-groupe qui contient X, il contient tous les éléments de X ainsi que leur inverse, et tous les produits de ces éléments, c'est à dire $\mathscr{M}(X \cup X^{-1})$. □

Remarque(s) 1.3.2. Dans le cas où $X = \{g\}$, les mots en l'alphabet $\{g, g^{-1}\}$ sont les puissances de g. On en déduit que $< g >= \{g^m \mid m \in \mathbb{Z}\}$.

Nous allons maintenant définir les applications entre deux groupes qui sont compatibles avec les lois de ces deux groupes.

Définition 1.3.2. Soient $(G, *)$, $(K, .)$ deux groupes et f une application de G dans K. On dit que f est un morphisme de groupe, si pour tout $(s, t) \in G$, on a : $f(s * t) = f(s).f(t)$.

Exemple(s) 1.3.1. Donnons quelques exemples.

1. Si E et F sont deux espaces vectoriels, et si f est une application linéaire de E dans F, alors en particulier f est un morphisme de groupe pour l'addition sur E et F.
2. Si H est une partie de G, alors H est un sous-groupe de G si et seulement si l'application inclusion de H dans G est un morphisme de groupe (exercice).
3. Si V est un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et G le groupe $\mathrm{GL}(V)$ défini ci-dessus, on peut considérer l'application déterminant :

$$\begin{array}{rccc} \det : & G & \to & \mathbb{K}^* \\ & A & \mapsto & \det(A). \end{array}$$

Rappelons que pour tout $(A, B) \in \mathrm{GL}(V)$, on a $\det(AB) = \det(A).\det(B)$, ce qui se traduit par : l'application ci-dessus est un morphisme de groupe entre $\mathrm{GL}(V)$ et $\mathbb{K}^*$.

4. Soient G un groupe et $g \in G$, alors l'application de G dans lui-même définie par $\varphi_g(s) = gsg^{-1}$ est un morphisme de groupe (exercice).

Voici quelques propriétés des morphismes.

Propriété 1.3.3. *Soient G_1, G_2 deux groupes, f un morphisme de G_1 dans G_2 ;*

1. *Si e_1, e_2 sont les éléments neutres respectifs de G_1, G_2 alors $f(e_1) = e_2$.*
2. *Si $s \in G_1$ alors $f(s^{-1}) = f(s)^{-1}$.*
3. *Si H_1 un sous-groupe de G_1 et H_2 un sous-groupe de G_2, alors $f(H_1)$ est un sous-groupe de G_2 est $f^{-1}(H_2)$ est un sous-groupe de G_1.*

Démonstration.

1. Il suffit d'écrire $f(e_1) = f(e_1e_1) = f(e_1)^2$, et en simplifiant par $f(e_1)$ on obtient $e_2 = f(e_1)$.
2. En utilisant le point 1, et le fait que f soit un morphisme, on a :

$$e_2 = f(e_1) = f(ss^{-1}) = f(s)f(s^{-1}).$$

   Et donc $f(s^{-1})$ est l'inverse de $f(s)$, c'est à dire $f(s^{-1}) = f(s)^{-1}$.
3. Tout d'abord puisque H_1 est non vide, $f(H_1)$ est également non vide ; soient s_2, t_2 deux éléments de $f(H_1)$, on doit montrer que $s_2t_2^{-1}$ appartient à $f(H_1)$. Par définition de $f(H_1)$, il existe s_1, t_1 dans H_1 tels que $f(s_1) = s_2$ et $f(t_1) = t_2$. D'autre part, comme f est un morphisme de groupe et d'après les points précédents, on a les égalités :

$$s_2t_2^{-1} = f(s_1)f(t_1)^{-1} = f(s_1)f(t_1^{-1}) = f(s_1t_1^{-1}).$$

   Comme H_1 est un sous-groupe l'élément $u_1 = s_1t_1^{-1} \in H_1$ et donc $s_2t_2^{-1} = f(u_1)$ appartient à H_2. La preuve de l'autre énoncé du point 3 est laissée en exercice.

□

En particulier la pré-image de l'élément neutre $e_2 \in G_2$ est un sous-groupe. Dans le cas d'une application linéaire, c'est un espace vectoriel noté $\ker f$, on garde cette notation dans le cas des morphismes de groupes, c'est à dire :

$$\ker f = \{g \in G_1 \mid f(g) = e_2\}.$$

Comme dans le cas linéaire, l'injectivité de f peut se caractériser par son noyau.

Propriété 1.3.4. *Soient G_1, G_2 deux groupes et f un morphisme de G_1 dans G_2, alors f est injective si et seulement si* $\ker f = \{e_1\}$.

Démonstration. Si f est injective, alors la pré-image de tout élément de G_2 est vide ou réduite à un élément. Mais comme $e_1 \in \ker f$ on a bien l'égalité $\{e_1\} = \ker f$. Réciproquement, supposons que $\ker f = \{e_1\}$. Soit $(s,t) \in G_1^2$ tel que $f(s) = f(t)$, alors on a $f(s)f(t)^{-1} = e_2$. Comme f est un morphisme de groupe, on a donc $f(st^{-1}) = e_2$, c'est à dire st^{-1} appartient à $\ker f$, et donc $st^{-1} = e_1$, *i.e.* $s = t$. □

Voici une propriété très utile des morphismes bijectifs de groupes.

Propriété 1.3.5. *Soient G_1, G_2 deux groupes, f un morphisme bijectif de G_1 dans G_2, alors f^{-1} est un morphisme de groupe.*

Démonstration. Soit $(s_2, t_2) \in G_2^2$, on doit montrer que $f^{-1}(s_2)f^{-1}(t_2) = f^{-1}(s_2t_2)$. Pour cela puisque f est bijective, il existe $(s_1, t_1) \in G_1^2$ tels que $f(s_1) = s_2$ et $f(t_1) = t_2$. On a les égalités suivantes :

$$f^{-1}(s_2t_2) = f^{-1}(f(s_1)f(t_1)) = f^{-1}(f(s_1t_1)) = s_1t_1 = f^{-1}(s_2)f^{-1}(t_2).$$

Vérifier que vous savez justifier chacune des égalités ci-dessus ! □

Cette propriété est à rapprocher d'une propriété semblable en algèbre linéaire : la réciproque d'une application linéaire bijective est linéaire. Mais ce type d'énoncé n'est pas vrai dans tous les contextes. Par exemple, en topologie, la réciproque d'une application continue bijective n'est pas forcément continue.

Concernant les morphismes de groupes, on retrouve la même terminologie que pour les applications linéaires. Un morphisme bijectif de groupe de G_1 dans G_2 est appelé un *isomorphisme*. Lorsqu'il existe

un isomorphisme entre deux groupes G_1 et G_2, on dit que les deux groupes sont isomorphes. Ils ne sont pas forcément égaux en tant qu'ensemble, mais en tant que groupe ils sont "identiques", c'est à dire que toutes les propriétés de G_1 en tant que groupe seront vraies pour G_2 (et réciproquement). Par exemple si G_1 est commutatif, G_2 l'est aussi, s'il existe un élément $x_1 \in G_1$ tel que $x_1^n = e$ alors il existe un élément $x_2 \in G_2$ avec la même propriété, etc.

On rencontre aussi le terme *endomorphisme* pour désigner un morphisme de G dans lui-même. Et enfin un endomorphisme bijectif est un *automorphisme*. On notera $\mathrm{Mor}(G_1, G_2)$ l'ensemble des morphismes de G_1 dans G_2 et $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G dans lui-même. Les morphismes définis dans l'exemple 1.3.1.4 sont des automorphismes (le vérifier) ; on les appellent les automorphismes intérieurs de G. On note $\mathrm{Int}(G) = \{\varphi_g \mid g \in G\}$, l'ensemble des automorphismes intérieurs.

L'ensemble des automorphismes de G est un groupe. On a en effet les propriétés suivantes.

Propriété 1.3.6. *Soit G un groupe, on a les trois assertions suivantes.*

(i) Soient φ, ψ deux automorphismes de G, alors $\varphi \circ \psi$ est un automorphisme de G.

(ii) $\mathrm{Aut}(G)$ est un groupe (pour la composition des applications).

(iii) $\mathrm{Int}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$.

Démonstration.

(i) La preuve de ce point est laissée en exercice.

(ii) On va utiliser la méthode évoquée dans l'exemple 1.2.1. L'ensemble $\mathrm{Aut}(G)$ est un sous-ensemble du groupe : $\mathrm{Bij}(G)$. Montrons que c'est un sous-groupe. Soient φ, ψ deux automorphismes. Alors on a déjà vu que ψ^{-1} est un automorphisme de G (voir la proposition 1.3.5). Ensuite, grâce au point (i), $\varphi \circ \psi$ est un automorphisme de groupe.

(iii) On considère l'application suivante :

$$\begin{array}{rccc} \Theta & : & G & \to & \mathrm{Int}(G) \\ & & g & \mapsto & \varphi_g \end{array}$$

où pour tout $s \in G$, $\varphi_g(s) = gsg^{-1}$. Alors d'une part, par définition $\mathrm{Im}\,\Theta = \mathrm{Int}(G)$ et d'autre part Θ est un morphisme de groupe (le vérifier). Et donc par la propriété 1.3.3, $\mathrm{Int}(G)$ est un sous-groupe.

□

Terminons cette section en introduisant la notion de produit de groupes.

Propriété 1.3.7. *Soit n un entier naturel non nul, et soient n groupes :*

$$(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n).$$

Alors le produit cartésien $\prod_{i=1}^n G_i$ est un groupe pour la loi produit définie par :

$$(s_1, s_2, \ldots, s_n) * (t_1, t_2, \ldots, t_n) = (s_1 *_1 t_1, s_2 *_2 t_2, \ldots, s_n *_n t_n).$$

Pour cette loi de groupe, les n projections π_j de $\prod_{i=1}^n G_i$ dans G_j sont des morphismes de groupes.

Démonstration. La preuve est laissée en exercice. □

1.4 Rappels sur les relations d'équivalence

Soit X un ensemble ; une relation sur X est un sous-ensemble $\mathscr{R} \subset X \times X$. En général, $(x, y) \in \mathscr{R}$ est noté $x \sim y$. On va ici s'intéresser aux relations d'équivalence.

Définition 1.4.1. Soit X un ensemble muni d'une relation $\sim$. Cette relation sera appelée relation d'équivalence si les trois propriétés suivantes sont vérifiées :

1. La relation est réflexive : pour tout $x \in X$ $x \sim x$.
2. La relation est symétrique : pour tout couple $(x, y) \in X^2$, $x \sim y$ implique $y \sim x$.
3. La relation est transitive : pour tout $(x, y, z) \in X^3$, $x \sim y$ et $y \sim z$ implique $x \sim z$.

Exemple(s) 1.4.1. Voici quelques exemples de relations d'équivalences.

1. Sur tout ensemble X, on peut définir la relation telle que tout élément n'est en relation qu'avec lui-même (c'est la relation définie par l'égalité).
2. Toujours sur un ensemble X quelconque, on peut définir la relation où pour tout couple $(x, y) \in X$, $x \sim y$.
3. Soit n un entier positif ou nul ; sur l'ensemble $\mathbb{Z}$, on définit $p \sim q$ si et seulement si $p - q$ est un multiple de n (donc $p = q$ si $n = 0$). Cela définit bien une relation d'équivalence (exercice).
4. Soit H un sous-groupe d'un groupe G, on définit la relation suivante : pour tout $(s, t) \in G^2$, $s \sim_H t$ si et seulement si $st^{-1} \in H$. La relation $\sim_H$ est une relation d'équivalence. On vérifie les trois propriétés qui définissent une relation d'équivalence. D'abord comme $ss^{-1} = e \in H$, la relation est réflexive. Ensuite si $s \sim_H t$ alors $st^{-1} \in H$, mais H étant un sous-groupe, $ts^{-1} \in H$ et donc $t \sim_H s$, la relation est symétrique. Enfin si $s \sim_H t$ et $t \sim_H u$, alors $st^{-1} \in H$ et $tu^{-1} \in H$, mais alors $st^{-1}tu^{-1} = su^{-1} \in H$, *i.e.* $s \sim_H u$, la relation est transitive.

Si X est un ensemble muni d'une relation d'équivalence, et si $x \in X$ alors on définit la classe d'équivalence de x ou la classe d'équivalence passant par x le sous-ensemble de X défini par
$\overline{x} = \{y \in X \,|\, y \sim x\}$.
On dit aussi que x est un représentant de la classe $\overline{x}$. Ces classes vérifient les propriétés suivantes.

Propriété 1.4.1. *Soit X muni d'une relation d'équivalence $\sim$, soit $(x, y) \in X^2$, on a équivalence entre les propriétés suivantes :*

(i) $\overline{x} = \overline{y}$;

(ii) $x \in \overline{y}$;

(iii) $y \in \overline{x}$;

(iv) $\overline{x} \cap \overline{y} \neq \emptyset$;

(v) $x \sim y$.

Démonstration.

$(i) \Rightarrow (ii)$ Remarquons d'abord que puisque la relation est réflexive, $x \in \overline{x}$. Donc si $\overline{x} = \overline{y}$, alors $x \in \overline{y}$ et donc $x \sim y$.

$(ii) \Rightarrow (iii)$ Si $x \in \overline{y}$, alors $x \sim y$ et donc par symétrie $y \in \overline{x}$.

$(iii) \Rightarrow (iv)$ Si $y \in \overline{x}$, alors $y \in \overline{x} \cap \overline{y}$ et donc $\overline{x} \cap \overline{y}$ est non vide.

$(iv) \Rightarrow (v)$ Supposons que $\overline{x} \cap \overline{y} \neq \emptyset$, alors il existe $z \in \overline{x} \cap \overline{y}$, et donc par définition $x \sim z$ et $y \sim z$, et par les propriétés de réflexivité et de transitivité des relations d'équivalence, on a bien $x \sim y$.

$(v) \Rightarrow (i)$ Supposons $x \sim y$, et soit $z \in \overline{x}$, alors $z \sim x$ et donc $z \sim y$, d'où $z \in \overline{y}$ et on a $\overline{x} \subset \overline{y}$. L'autre inclusion se montre de la même façon.

□

Rappelons que si X est un ensemble et que si $\mathscr{P} \subset \mathscr{P}(X)$ est un ensemble de parties de X deux à deux disjointes qui recouvrent X, on dit que $\mathscr{P}$ est une partition de X. La propriété précédente montre que l'ensemble des classes d'équivalence forme une partition de X. Réciproquement, si on se donne une partition de X, alors on peut définir une relation d'équivalence, en définissant $x \sim y$ si et seulement s'il existe un sous-ensemble de X de la partition qui contienne x et y.

On va maintenant donner un nom à cette partition définie par une relation d'équivalence, c'est la notion d'ensemble quotient qui va nous être très utile pour la suite.

Définition 1.4.2. Soit X un ensemble muni d'une relation d'équivalence. L'ensemble quotient $X/\sim$ est le sous-ensemble de $\mathscr{P}(X)$ défini par :

$$X/\sim = \{\overline{x} \,|\, x \in X\}.$$

On définit l'application quotient :

$$\begin{array}{rccc} \pi & : & X & \to & X/\sim \\ & & x & \mapsto & \overline{x} \end{array}.$$

D'après les remarques précédentes, l'application π est bien définie et surjective (exercice).

Exemple(s) 1.4.2. Reprenons maintenant les quatre exemples de relations d'équivalence donnés précédemment et pour chacun d'eux calculer l'ensemble et l'application quotient.

1. Si les éléments de X ne sont en relation qu'avec eux-même, dans ce cas pour tout $x \in X$, on a $\overline{x} = \{x\}$ et l'application quotient est dans ce cas une bijection.
2. Si deux éléments quelconques de X sont en relation, alors la partition $X/\sim$ contient un seul élément qui est X lui-même.
3. Si n est un entier positif ou nul, et $X = \mathbb{Z}$ muni de la relation de congruence : $p \sim q$ si et seulement si $p-q$ est un multiple de n. Alors la classe d'équivalence de p est définie par $\overline{p} = \{p+kn\,|, k \in \mathbb{Z}\}$; si $n = 0$ les classes d'équivalence contiennent un seul élément, et on se retrouve dans un cas particulier du premier exemple. Si $n \neq 0$, en utilisant la division euclidienne de p par n, chaque classe contient un entier compris entre 0 et $n-1$. La partition réalisée par la relation d'équivalence est donc la suivante :
$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{n-1}.$$
et l'application quotient $\pi(p)$ peut s'interpréter comme le reste modulo n de l'entier p. Notons que l'on a fait le choix ici de représenter chaque classe par un entier compris entre 0 et $n-1$, mais on aurait très bien pu choisir un autre paramétrage de l'espace quotient, par exemple les entiers entre n et $2n-1$.

Terminons cette section par un résultat dans le cas particulier où l'ensemble X est de cardinal fini.

Propriété 1.4.2. *Soit X un ensemble fini muni d'une relation d'équivalence $\sim$, alors $X/\sim$ et toutes les classes d'équivalence de $\sim$ sont de cardinal fini, et on a :*
$$|X| = \sum_{C \in X/\sim} |C|.$$

Démonstration. Comme toutes les classes sont incluses dans X elles sont de cardinal fini, et comme ces classes sont distinctes, il ne peut pas y en avoir un nombre infini. La deuxième assertion est la simple conséquence du partitionnement de X par les classes d'équivalence. □

1.5 Rappels sur $\mathbb{Z}$, ses sous-groupes, ses quotients

L'ensemble des entiers relatifs muni de l'addition est un groupe. On peut facilement donner la liste de tous les sous-groupes de $\mathbb{Z}$. Commençons par une remarque simple. Soit $n \in \mathbb{N}$, alors l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. En effet, si p et q sont deux multiples de n, alors $p-q$ est évidemment un multiple de n. En fait il n'y a pas d'autres sous-groupes de $\mathbb{Z}$.

Théorème 2. *Soit H un sous-groupe de $\mathbb{Z}$, alors il existe un unique entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration. Montrons l'existence de n : soit H un sous-groupe de $\mathbb{Z}$; si $H = \{0\}$, alors $H = 0\mathbb{Z}$ et c'est terminé dans ce cas. Supposons donc que $H \neq \{0\}$. On sait que si $h \in H$ alors $-h \in H$, donc $H \cap \mathbb{N}^* \neq \emptyset$, et soit $n = \min H \cap \mathbb{N}^*$. Maintenant considérons $h \in H$; effectuons la division euclidienne de h par n : il existe un couple $(q, r) \in \mathbb{Z}$ tel que $0 \leq r < n$ et $h = nq + r$. Comme $n \in H$, alors nq qui est la somme de n avec lui-même q fois est dans H, et donc $r = h - nq$ appartient à H également. Si r est non nul alors $r \in H \cap \mathbb{N}^*$, ce qui amène une contradiction entre la définition de n et la condition $r < n$. Donc $r = 0$ et $h = nq \in \mathbb{Z}$.

L'unicité est laissée en exercice. □

Remarque(s) 1.5.1. Rappelons qu'il est facile de déterminer si deux tels sous-groupes de $\mathbb{Z}$ sont inclus. En effet $m\mathbb{Z} \subset n\mathbb{Z}$ si et seulement si n divise m (attention au sens).

Pour chaque sous-groupe de $\mathbb{Z}$, nous allons définir une relation d'équivalence.

Définition 1.5.1. Soit $n \in \mathbb{N}^*$ et soit $(p, q) \in \mathbb{Z}^2$, on pose $p \sim_n q$ si $p - q \in n\mathbb{Z}$.

Cette relation a déjà été considérée (voir les exemples 1.4.1). L'ensemble quotient $\mathbb{Z}/\sim_n$ que l'on note aussi $\mathbb{Z}/n\mathbb{Z}$ est un groupe. En effet, on a le théorème suivant.

Théorème 3. *L'addition dans $\mathbb{Z}$ définit une loi sur $\mathbb{Z}/n\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ muni de cette loi est un groupe.*

Démonstration. La loi + sur $\mathbb{Z}$ passe au quotient, en effet si $p \sim_n p'$ et si $q \sim_n q'$ alors $p+q \sim_n p'+q'$, on peut donc définir : $\overline{p}\bar{+}\overline{q} = \overline{p+q}$. Ensuite, on vérifie facilement les propriétés nécessaires à partir des propriétés sur $\mathbb{Z}$. Par exemple pour l'associativité, si $\overline{p}, \overline{q}, \overline{r}$ sont trois éléments de $\mathbb{Z}/n\mathbb{Z}$, on peut écrire :

$$(\overline{p}\bar{+}\overline{q})\bar{+}\overline{r} = (\overline{p+q})\bar{+}\overline{r} = \overline{(p+q)+r} = \overline{p+(q+r)} = \overline{p}\bar{+}\overline{q+r} = \overline{p}\bar{+}(\overline{q}\bar{+}\overline{r}).$$

On vérifie ensuite que $\overline{0}$ est l'élément neutre et que si $\overline{p} \in \mathbb{Z}/n\mathbb{Z}$ alors $\overline{-p}$ est son inverse (exercice). □

Finissons cette section en rappelant un autre résultat en donnant un énoncé qui utilise la théorie des groupes.

Théorème 4. Le théorème des restes chinois. *Soient n, m deux entiers non nuls et premiers entre eux. Alors il existe un isomorphisme de groupes entre $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$.*

Démonstration. Si $l \in \mathbb{Z}$ et $r \in \mathbb{N}^*$, dans cette preuve nous noterons $\bar{l}^{\{r\}}$ la classe de l modulo r. On définit l'application suivante :

$$\begin{array}{rccc} \Psi & : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & l & \mapsto & (\bar{l}^{\{n\}}, \bar{l}^{\{m\}}). \end{array}$$

Cette application est un morphisme de groupe. De plus, si $\bar{l}^{\{mn\}} = \bar{s}^{\{mn\}}$ alors $l - s$ est un multiple de mn donc de m et de n ; on en déduit que $\Psi(l) = \Psi(s)$. On peut donc définir une application définie sur le quotient $\mathbb{Z}/nm\mathbb{Z}$:

$$\begin{array}{rccc} \overline{\Psi} & : & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & \bar{l}^{\{mn\}} & \mapsto & \overline{\Psi}(\bar{l}^{\{mn\}}) = \Psi(l). \end{array}$$

Cette application est un morphisme de groupe (car Ψ est un morphisme de groupe). Calculons son noyau :

$$\ker \overline{\Psi} = \left\{ \bar{l}^{\{mn\}} \mid \bar{l}^{\{n\}} = \overline{0}^{\{n\}} \text{ et } \bar{l}^{\{m\}} = \overline{0}^{\{m\}} \right\}.$$

Mais si un entier l est divisible par deux nombres n et m premiers entre eux, alors il est divisible par leur produit mn. Donc $\bar{l}^{\{mn\}} = \overline{0}^{\{mn\}}$ et $\overline{\Psi}$ est injective. Comme les ensembles de départ et d'arrivée sont de même cardinal *fini*, $\overline{\Psi}$ est bijective, ce qui achève la preuve. □

Remarque(s) 1.5.2.
1. En fait le produit dans $\mathbb{Z}$ permet de définir une multiplication dans $\mathbb{Z}/nm\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui fait de ces deux groupes des anneaux. Et le morphisme $\overline{\Psi}$ ci-dessus est un morphisme d'anneau.
2. Par une récurrence très simple, on peut étendre ce résultat au cas de r entiers $n_1, n_2, \ldots, n_r$ premiers deux à deux.

1.6 L'ordre d'un élément, ordre et indice d'un sous-groupe

Rappelons qu'il est d'usage dans la théorie des groupes d'appeler ordre d'un groupe G son cardinal et que celui-ci est noté $|G|$. Définissons maintenant l'ordre d'un élément de G.

Définition 1.6.1. Soit G un groupe et $g \in G$, on appelle ordre de g (noté $o(g)$) l'ordre du groupe engendré par g, c'est à dire $o(g) = | < g > |$.

Évidemment l'ordre d'un groupe ou d'un élément n'est pas forcément fini, on dit alors que le groupe ou l'élément est d'ordre infini.

Exemple(s) 1.6.1.
1. Si G est quelconque alors son élément neutre e est d'ordre 1 ; en effet on a $< e >= e$. Réciproquement, si $g \in G$ est d'ordre 1, alors $< g >= \{e\}$ et donc g est égal à e.
2. Soit $X = \{1, 2, 3\}$, $G = \Sigma_X$ et σ l'élément de G qui échange 1 et 2 et qui laisse 3 invariant. Il est immédiat de vérifier que $\sigma = \sigma^{-1}$ et que pour tout $m \in \mathbb{Z}$, $\sigma^{2m} = e$ et $\sigma^{2m+1} = \sigma$. On en déduit que $< \sigma >= \{\sigma^n \mid n \in \mathbb{Z}\} = \{e, \sigma\}$ et σ est d'ordre 2.

3. Soit G le groupe $\mathbb{Z}$ et $m \in \mathbb{Z}$; on a vu que si $m = 0$, alors il est d'ordre 1. Si $m \neq 0$, alors $< m >= |m|\mathbb{Z}$ et m est d'ordre infini.
4. Soit $G = \mathbb{Z}/4\mathbb{Z}$, alors G a quatre éléments $G = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. On a vu que $\overline{0}$ est l'élément neutre de G donc d'ordre 1. Les éléments $\overline{1}$ et $\overline{3}$ sont d'ordre 4, et $\overline{2}$ est d'ordre 2 (exercice).

Nous allons voir maintenant une autre façon de calculer l'ordre d'un élément. Commençons par une remarque : soit G un groupe dont la loi est notée par simple concaténation, et soit $g \in G$, on a vu précédemment que pour tout $(m, n) \in \mathbb{Z}$, on a l'égalité : $g^m g^n = g^{m+n}$. Ceci peut se traduire par la propriété qui suit.

Propriété 1.6.1. *Soient G et $g \in G$ comme ci-dessus, et soit ψ_g l'application de $\mathbb{Z}$ dans G définie par $\psi_g(m) = g^m$. L'application ψ_g est un morphisme de groupe, et de plus* $\operatorname{Im}\psi_g =< g >$.

Démonstration. Il reste à vérifier la deuxième assertion. Pour cela, on se souvient que $< g >$ est l'ensemble des mots en l'alphabet $\{g\}$ et donc $< g >= \{g^n \mid n \in \mathbb{Z}\}$. □

Le noyau du morphisme ψ_g est directement lié à l'ordre de g. En effet, on a la propriété suivante.

Théorème 5. *Soient G, $g \in G$ et ψ_g comme ci dessus. Soit $n \in \mathbb{N}$ tel que* $\ker\psi_g = n\mathbb{Z}$ *Alors on a les assertions suivantes :*

(i) Si $n = 0$, alors l'application ψ_g est un isomorphisme de groupe entre $\mathbb{Z}$ et $\operatorname{Im}\psi_g$ *; si $n \neq 0$ alors l'application ψ_g induit un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et* $\operatorname{Im}\psi_g$.

(ii) On a $\ker(\psi_g) \neq \{0\}$ *si et seulement si g est d'ordre fini et dans ce cas on a $n = o(g)$.*

Démonstration.

(i) Si $n = 0$, alors $\ker\psi_g = \{0\}$ et l'application ψ_g est injective, d'où l'assertion.
Si $n \neq 0$, alors considérons l'application suivante :

$$\begin{array}{rccc} \overline{\psi_g} & : & \mathbb{Z}/n\mathbb{Z} & \to & < g > \\ & & \overline{m} & \mapsto \psi_g(m). & \end{array}$$

Cette application est bien définie ; en effet si $\overline{m} = \overline{l}$, alors $m - l$ est un multiple de n, c'est à dire qu'il existe un $k \in \mathbb{Z}$ tel que $l = m + kn$, mais alors :

$$\psi_g(l) = \psi_g(m + kn) = \psi_g(m)\psi_g(n)^k = \psi_g(m)$$

puisque $n \in \ker\psi_g$ et donc $\psi_g(n) = e$.
Cette application est surjective, puisque $< g >= \{g^m \mid m \in \mathbb{Z}\}$.
Son noyau est réduit à $\{\overline{0}\}$, en effet si $\overline{\psi_g}(\overline{m}) = \psi_g(m) = e$, alors $m \in \ker\psi_g$ et donc $\overline{m} = \overline{0}$, cette application est donc bijective.
Finalement, c'est un morphisme de groupe. En effet soit $(m, l) \in \mathbb{Z}^2$, alors :

$$\overline{\psi}_g(\overline{m} + \overline{l}) = \overline{\psi}_g(\overline{m + l}) = \psi_g(m + l) = \psi_g(m)\psi_g(l) = \overline{\psi}_g(\overline{m})\overline{\psi}_g(\overline{l}).$$

L'application $\overline{\psi}_g$ est donc un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et $\operatorname{Im}\psi_g =< g >$.

(ii) Si $\ker\psi_g \neq \{0\}$, alors grâce au point précédent, on a :

$$o(g) = | < g > | = |\mathbb{Z}/n\mathbb{Z}| = n.$$

Réciproquement si $\ker\psi_g = \{0\}$, alors dans ce cas l'application ψ_g est injective et on a un isomorphisme entre $\mathbb{Z}$ et $< g >$, et g est d'ordre infini.

□

À partir de cette caractérisation de l'ordre d'un élément, on peut en obtenir quelques propriétés.

Propriété 1.6.2. *Soient G un groupe et g un élément de G d'ordre fini égal à n. On a les propriétés suivantes.*

(i) Soit $m \in \mathbb{Z}, m \neq 0$ alors $g^m = e$ si et seulement si n divise m ;

(ii) $n = \min\{m \in \mathbb{N}^* \text{ tel que } g^m = e\}$.

Démonstration.

(i) D'après la propriété précédente, $\ker \psi_g = n\mathbb{Z}$; Soit $m \in \mathbb{Z}$ non nul, on a les équivalences suivantes : $g^m = e \Leftrightarrow m \in \ker \psi_g \Leftrightarrow m \in n\mathbb{Z} \Leftrightarrow n \mid m$.

(ii) Il suffit de remarquer que n est le plus petit multiple positif non nul de n.

□

Remarque(s) 1.6.1.

1. Attention au point (i) : une erreur classique est d'écrire que si $g^m = e$, alors g est d'ordre m ce qui évidemment faux.
2. Par contre si on montre qu'il existe n un entier tel que $g^m = e$ si et seulement m est un multiple de n, alors par définition n est égal à l'ordre de g.

L'application ψ_g permet de classer à isomorphismes près les groupes qui sont engendrés par un seul élément. Commençons par définir ces sous-groupes.

Définition 1.6.2. Soit G un groupe. S'il existe $g \in G$ tel que $G =< g >$, on dit que G est monogène. Si de plus G est d'ordre fini, on dit que G est cyclique.

Propriété 1.6.3. *Soit G un groupe monogène ; alors si G est d'ordre infini, G est isomorphe à $\mathbb{Z}$ et si G est cyclique, alors il existe $n \in \mathbb{N}^*$ tel que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Soit $g \in G$ tel que $G =< g >$; alors on a égalité : $\operatorname{Im} \psi_g = G$ et donc si g est d'ordre infini, ψ_g est un isomorphisme entre $\mathbb{Z}$ et G, et si g est d'ordre fini égal à n, $\overline{\psi_g}$ est un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G. □

Exemple(s) 1.6.2. Toutes les assertions de cet exemple sont à montrer en exercice.

Soit $n \in \mathbb{N}^*$; on définit l'ensemble des racines n-ièmes de l'unité :

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

L'ensemble $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$ de cardinal n, de plus il est engendré par l'élément $\exp(\frac{2i\pi}{n})$ et donc $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

1.7 Le théorème de Lagrange

Nous allons maintenant énoncer et démontrer le théorème de Lagrange. Soient G un groupe et H un sous-groupe, rappelons que la relation définie par $\forall (s,t) \in G^2$, $s \sim_H t$ si et seulement si $st^{-1} \in H$ est une relation d'équivalence (voir le dernier exemple dans 1.4.1), ce qui permet de définir l'indice de H dans G.

Définition 1.7.1. Soient G un groupe, H un sous-groupe et $\sim_H$ la relation définie ci-dessus. Alors le cardinal de $G/\sim_H$ est appelé l'indice de H dans G. Cet indice est noté $[G : H]$.

La preuve du théorème de Lagrange repose essentiellement sur la propriété qui suit.

Propriété 1.7.1. *Soit C_e la classe d'équivalence passant par l'identité et C une autre classe d'équivalence ; alors $C_e = H$, et il existe une bijection entre C_e et C. En conséquence, toutes les classes d'équivalence ont donc le même cardinal que celui de H.*

Démonstration.

Soit C_e la classe d'équivalence contenant l'identité. Si $t \in C_e$, alors par définition $t \sim_H e$ et donc $te^{-1} = t \in H$. Et donc $C_e \subset H$. Réciproquement si $t \in H$ alors $te^{-1} \in H$ et $t \sim e$. Soit C une classe d'équivalence (qui est non vide par définition), et soit $s \in C$. Alors on définit l'application suivante :

$$\begin{array}{rccc} \Theta & : & C_e & \to & G \\ & & h & \mapsto & hs \end{array}$$

On vérifie d'abord que $\mathrm{Im}\,\Theta = C$. C'est une simple traduction, en effet :

$$t \in \mathrm{Im}\,\Theta \Leftrightarrow (\exists h \in H) \text{ tel que } t = hs \Leftrightarrow ts^{-1} = h \in H \Leftrightarrow t \sim_H s \Leftrightarrow t \in C.$$

On peut donc considérer l'application Θ comme une application de C_e dans C. Par définition elle est surjective. Soient maintenant h et h' tels que $\Theta(h) = \Theta(h')$ alors $hs = h's$, et donc $h = h'$ et Θ est bijective. □

Théorème 6. *Théorème de Lagrange.*
Soient G un groupe fini et H un sous-groupe. Alors l'ordre et l'indice de H sont finis et on a l'égalité :

$$|G| = |H|[G : H].$$

En conséquence $|H|$ et $[G : H]$ divise l'ordre de G. En particulier l'ordre de tout élément de G divise l'ordre de G.

Démonstration. Comme $H \subset G$, H est de cardinal fini. De même, il y a un nombre fini de classes d'équivalence de $\sim_H$ dans G et donc $[G : H]$ est fini. Ensuite, la propriété 1.4.2 sur les relations d'équivalence permet d'écrire :

$$|G| = \sum_{C \in G/\sim_H} |C|.$$

Mais on a vu que toutes les classes avaient le même cardinal que le cardinal de H, et donc la somme ci-dessus est simplement la somme de $[G : H]$ termes égaux à $|H|$, soit $|G| = |H|[G : H]$. La dernière remarque provient de la propriété 1.6.2 qui affirme que l'ordre d'un élément est égal à l'ordre du groupe engendré par cet élément. □

Avec l'aide de ce théorème, on a maintenant un outil puissant pour commencer à classifier les groupes d'ordre finis. Par exemple, il est maintenant facile de montrer que les groupes d'ordre un nombre premier sont cycliques, ou bien qu'il existe, à isomorphisme près deux groupes d'ordre 6 (exercice).

Pour les groupes d'ordre 8 la situation est un peu plus compliquée : à isomorphisme près, il y a trois groupes commutatifs distincts et deux groupes non commutatifs d'ordre 8. L'un de ces groupe est le groupe des quaternions que nous allons maintenant définir. Considérons les quatre éléments suivants de $\mathrm{Mat}_2(\mathbb{C})$:

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

Définition 1.7.2. On définit l'ensemble suivant :

$$Q_8 = \{\pm\mathbb{1}, \pm I, \pm J, \pm K\}.$$

On vérifie par un simple calcul que $I^2 = J^2 = K^2 = -\mathbb{1}$ et que $IJ = -JI = K$; de ces égalités on déduit que les trois éléments I, J et K sont d'ordre 4 et que Q_8 est un groupe non commutatif d'ordre 8.

1.7.1 Compléments sur les groupes cycliques

Dans le cas des groupes cycliques, il y a une « réciproque » au théorème de Lagrange, c'est à dire que pour tout diviseur d de n il existe un sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Précisons cela.

Propriété 1.7.2. *Soit $n \in \mathbb{N}^*$ et G un groupe cyclique d'ordre n. Alors pour tout $d \mid n$ il existe un unique sous-groupe d'ordre d de G ; de plus ce sous-groupe est cyclique.*

Démonstration. Soit d un diviseur de n. Montrons d'abord l'existence d'un sous-groupe de G de cardinal d. Pour cela, on définit l'ensemble suivant :

$$G_d = \{g \in G \mid g^d = e\}.$$

Comme G est commutatif l'ensemble G_d est un sous-groupe (le vérifier).

Vérifions que G_d est de cardinal d. Comme G est cyclique d'ordre n, on peut supposer que $G = \mathbb{Z}/n\mathbb{Z}$. Soit $l = 1, 2, \ldots, n$, la classe $\bar{l} \in G_d$ si et seulement si $d\bar{l} = \bar{0}$ ce qui est équivalent à dl est divisible par n, mais $n \mid dl$ si et seulement si $\frac{n}{d} \mid l$, on obtient donc comme solution d classes distinctes et on a :

$$G_d = \{k\overline{\Big(\frac{n}{d}\Big)} : 1 \leq k \leq d\}.$$

G_d est bien un groupe cyclique de générateur la classe $\overline{\big(\frac{n}{d}\big)}$.

Maintenant soit H un sous-groupe de G de cardinal d. Alors par le théorème de Lagrange, on a l'inclusion $H \subset G_d$. Mais comme H et G_d ont même cardinal, on a l'égalité $H = G_d$. □

Chapitre 2

Théorie des anneaux, une introduction

2.1 Anneaux et corps, premières définitions

2.1.1 Définitions

Définition 2.1.1 (Anneau)**.** Un *anneau* est un triplet $(A, +, \times)$ où A est un ensemble et $+$, $\times$ sont deux lois de composition internes sur A telles que :

(1) $(A, +)$ est un groupe abélien ;

(2) associativité de $\times$: $\forall x, y, z \in A$, $(x \times y) \times z = x \times (y \times z)$ (qu'on peut donc noter $x \times y \times z$) ;

(3) élément neutre pour $\times$: il existe un élément $1_A \in A$ tel que $\forall x \in A$, $x \times 1_A = x = 1_A \times x$;

(4) compatibilité entre $+$ et $\times$: $x \times (y + z) = x \times y + x \times z$ et $(x + y) \times z = x \times z + y \times z$.

Définition 2.1.2 (Anneau commutatif)**.** Un anneau $(A, +, \times)$ est *commutatif* si la multiplication est commutative : $\forall x, y \in A$, $x \times y = y \times x$.

Remarque(s) 2.1.1. Quand il n'y a pas d'ambiguïté on écrit simplement A pour $(A, +, \times)$, 0 pour 0_A et 1 pour 1_A, afin d'alléger les notations. On utilise aussi la notation habituelle $xy = x \times y$.

Propriété 2.1.1. *Soit A un anneau, alors on a les propriétés suivantes :*

(i) L'élément neutre 1_A est unique ;

(ii) pour tout $x \in A$, $x \times 0_A = 0_A = 0_A \times x$;

(iii) pour tous $x, y \in A$, $(-x) \times y = -(x \times y) = x \times (-y)$;

(iv) pour tout $x \in A$ $(-1_A) \times x = -x = x \times (-1_A)$.

Démonstration. La démonstration de ces propriétés est laissée en exercice. □

Exemple(s) 2.1.1. (a) Exemple trivial : l'*anneau nul* $A = \{0\}$. Les lois sont $0 + 0 = 0$, $0 \times 0 = 0$, et 0 est à la fois le neutre pour $+$ et le neutre pour $\times$.

(b) Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ avec l'addition et la multiplication usuelles.

(c) L'anneau des polynômes $\mathbb{R}[X]$ avec l'addition et la multiplication usuelles.

(d) L'anneau des fonctions $\mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$, muni de la somme $(f + g)(x) = f(x) + g(x)$ et du produit $(fg)(x) = f(x)g(x)$. Le neutre pour la somme est la fonction constante 0 ; le neutre pour le produit est la fonction constante 1.

(e) Plus généralement si X est un ensemble et A un anneau, l'ensemble $\mathcal{F}(X, A)$ des fonctions de X dans A est un anneau.

(f) Les exemples (a) à (d) sont commutatifs. Les matrices carrées de taille n forment un anneau $(\mathcal{M}_n(\mathbb{R}), +, \times)$ qui n'est pas commutatif pour $n \geq 2$. Par exemple les matrices $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ne commutent pas : $AB \neq BA$.

(g) Pour E un $\mathbb{R}$-espace vectoriel on a l'anneau des endormorphismes $\mathbb{R}$-linéaires de E, noté $(\mathcal{L}(E), +, \circ)$. (Le produit est ici la composition.)

Exercice 1 Soit $(A, +, \times)$ un anneau. Montrer que si $0_A = 1_A$ alors $A = \{0_A\}$ est l'anneau nul.

Définition 2.1.3 (Corps)**.** Un *corps* est un anneau $\mathbb{K} \neq \{0\}$ qui est *commutatif* et tel que pour tout élément $x \in \mathbb{K} \setminus \{0_\mathbb{K}\}$ il existe $y \in \mathbb{K}$ tel que $x \times y = 1_\mathbb{K} = y \times x$.

Exemple(s) 2.1.2. (a) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.

(b) $\mathbb{Z}$ n'est pas un corps car il n'existe pas de $y \in \mathbb{Z}$ tel que $2 \times y = 1$.

(c) $\mathbb{R}[X]$ n'est pas un corps car il n'existe pas de $f \in \mathbb{R}[X]$ tel que $X \times f = 1$.

2.1.2 Règles de calcul dans un anneau

Soit $(A, +, \times)$ un anneau. On peut définir, pour $x \in A$ et $n \in \mathbb{N}$, la puissance

$$x^n = \underbrace{x \times \cdots \times x}_{n \text{ fois}}$$

(produit n fois de x) avec la convention $x^0 = 1_A$. (Si on veut être précis, la notation x^n est définie par récurrence sur n.) Les propriétés usuelles sont satisfaites : $x^0 = 1_A$, $x^1 = x$, $x^{m+n} = x^m x^n$, $(x^m)^n = x^{mn}$.

Attention : on n'a pas en général $(xy)^n = x^n \times y^n$ pour $x, y \in A$ et $n \in \mathbb{N}$. Par exemple, $(xy)^2 = xyxy$ et $x^2y^2 = xxyy$. Si $xy = yx$ alors ces deux expressions sont égales.

Dans un anneau $(A, +, \times)$ on peut utiliser la compatibilité entre $+$ et $\times$ pour développer comme on a l'habitude, par exemple : $(x+y)(z+t) = xz + xt + yz + yt$. Cas particulier : $(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2$. Attention : si $xy \neq yx$ on a $(x+y)^2 \neq x^2 + 2xy + y^2$.

Propriété 2.1.2. *Soit A un anneau et $x, y \in A$ tels que $xy = yx$. Alors on a les propriétés habituelles, pour $n \in \mathbb{N}$:*

1. $(xy)^n = x^n y^n$;
2. *(Formule du binôme)*
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \ ;$$
3. $$x^n - y^n = (x-y) \left(\sum_{k=0}^{n-1} x^k y^{n-1-k} \right) \ .$$

Démonstration. 1. C'est évident. (En fait, pour être rigoureux, la preuve nécessite *deux* récurrences sur n... c'est un exercice conseillé !)

2. Par récurrence sur n en utilisant la formule de Pascal : $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. On rappelle qu'on a $\binom{n}{k} = 0$ si $k < 0$ ou $k > n$. La formule est clairement vraie pour $n = 0$: $(x+y)^0 = 1$ et $\binom{0}{0} x^0 y^0 = 1$. Pour $n \geq 1$, supposons qu'on a montré la formule pour $n-1$ et montrons-la pour n. On calcule :

$$\begin{aligned}
(x+y)^n &= (x+y)^{n-1}(x+y) \\
&= \left(\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k} \right) (x+y) \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \left(\binom{n-1}{k-1} + \binom{n-1}{k} \right) x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \ .
\end{aligned}$$

3. On développe le produit pour trouver une somme télescopique :

$$\begin{aligned}(x-y)\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right) &= \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} x^k y^{n-k} \\ &= \sum_{k=1}^{n} x^k y^{n-k} - \sum_{k=0}^{n-1} x^k y^{n-k} \\ &= x^n - y^n \ .\end{aligned}$$

□

Exercice 2 Vérifiez que vous savez identifier l'endroit où on utilise $xy = yx$ dans les preuves ci-dessus.

2.1.3 Morphismes d'anneaux

Définition 2.1.4. Soient A et B deux anneaux. Un *morphisme d'anneaux* de A vers B est une application $\varphi : A \to B$ qui vérifie les conditions :

(a) compatibilité à la somme $+$: $\forall x, y \in A\,,\ \varphi(x+y) = \varphi(x) + \varphi(y)$ (dit autrement, φ est un morphisme de groupes abéliens) ;

(b) compatibilité au produit $\times$: $\forall x, y \in A\,,\ \varphi(x \times y) = \varphi(x) \times \varphi(y)$;

(c) compatibilité aux unités : $\varphi(1_A) = 1_B$.

La condition (a) implique que $\varphi(0_A) = 0_B$, mais la condition (b) n'implique pas la condition (c). Par exemple le morphisme nul donné pour tout $x \in A$ par $\varphi(x) = 0_B$ vérifie (a) et (b) mais pas (c). Voici deux propriétés sur les morphismes d'anneaux.

Propriété 2.1.3. *La composée de deux morphismes d'anneaux est un morphisme d'anneaux. La réciproque d'un morphisme d'anneaux bijectif est un morphisme d'anneaux.*

Démonstration. Exercice (il faut s'inspirer des propriétés équivalentes montrées pour les morphismes de groupes) □

Définition 2.1.5. Un *isomorphisme* d'anneaux de A vers B est un morphisme d'anneaux $\varphi : A \to B$ qui est bijectif. On dit alors que A et B sont *isomorphes* et on note parfois simplement $A \simeq B$.

Remarque(s) 2.1.2. Comme pour les groupes, si deux anneaux sont isomorphes, ils partagent les mêmes propriétés d'anneaux.

2.1.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$.

Théorème 7. *La multiplication $\overline{x} \times \overline{y} = \overline{x \times y}$ est bien définie et fait de $\mathbb{Z}/n\mathbb{Z}$ un anneau commutatif.*

Démonstration. On montre d'abord que l'opération est bien définie. Si $\overline{x'} = \overline{x}$ et $\overline{y'} = \overline{y}$ alors on peut écrire $x' = x + nk$ et $y' = y + n\ell$ avec $k, \ell \in \mathbb{Z}$. On a donc $x'y' = (x+nk)(y+n\ell) = xy + n(ky + \ell x + nk\ell)$ et donc $\overline{x'y'} = \overline{xy}$. On montre alors facilement que $\mathbb{Z}/n\mathbb{Z}$ est un anneau :

(1) $(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien : déjà fait ;

(2) associativité : $(\overline{x} \times \overline{y}) \times \overline{z} = \overline{xy} \times \overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x} \times \overline{yz} = \overline{x} \times (\overline{y} \times \overline{z})$;

(3) élément neutre pour $\times$: $\overline{x} \times \overline{1} = \overline{x \times 1} = \overline{x}$ et $\overline{1} \times \overline{x} = \overline{1 \times x} = \overline{x}$;

(4) compatibilité entre $+$ et $\times$: $\overline{x} \times (\overline{y} + \overline{z}) = \overline{x} \times \overline{y+z} = \overline{x(y+z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{x} \times \overline{y} + \overline{x} \times \overline{z}$. De la même façon, ou par la commutativité de $\times$, $(\overline{x} + \overline{y}) \times \overline{z} = \overline{x} \times \overline{z} + \overline{y} \times \overline{z}$.

□

Exemple(s) 2.1.3. Dans $\mathbb{Z}/13\mathbb{Z}$ on a $\overline{3} \times \overline{6} = \overline{18} = \overline{5} = \overline{135}$.

2.1.5 Anneaux de polynômes

On se contente ici de considérer des polynômes dont les coefficients sont pris dans un anneau *commutatif* R.

Définition 2.1.6 (Anneau de polynômes)**.** Soit R un anneau commutatif. Un polynôme à une indéterminée à coefficients dans R est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de R qui est nulle à partir d'un certain rang, qu'on note comme la combinaison linéaire

$$f = \sum_{n=0}^{N} a_n X^n \ ,$$

où l'indéterminée X est un symbole formel. La somme et le produit des polynômes est définie comme d'habitude : si f a pour coefficients a_n et g a pour coefficients b_n alors $f+g$ a pour coefficients a_n+b_n et fg a pour coefficients $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Cela donne à l'ensemble des polynômes une structure d'anneau commutatif (vérifiez-le !). On note cet anneau $R[X]$.

Remarque(s) 2.1.3. Vous avez une certaine familiarité des polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$. Mais attention, des choses non intuitives peuvent arriver si R est un anneau (commutatif) général : par exemple, dans $(\mathbb{Z}/4\mathbb{Z})[X]$ on a $(\overline{1}+\overline{2}X)^2 = \overline{1}$.

À un polynôme $f \in R[X]$ on associe la *fonction polynomiale* correspondante, qu'on note par le même symbole $f : R \to R\ ,\ x \mapsto f(x)$. Sur les corps $\mathbb{R}$ ou $\mathbb{C}$, on peut considérer indifféremment le polynôme ou la fonction polynomiale associée. Mais sur un anneau en général, deux polynômes différents peuvent définir une même fonction (voir TD).

Morphismes d'évaluation

Soit A un anneau quelconque et $x \in A$. Pour un polynôme à coefficients entiers $f \in \mathbb{Z}[X]$, la structure d'anneau de A permet de donner un sens à l'*évaluation* $f(x) \in A$. Par exemple, pour $f = X^2 + 2X - 2$ on a $f(x) = x \times x + x + x - 1_A - 1_A$. Cette opération d'évaluation est compatible à la structure d'anneau sur $\mathbb{Z}[X]$ au sens de la proposition suivante, qui est très utile en pratique.

Propriété 2.1.4. *Soit A un anneau et $x \in A$. L'évaluation des polynômes en x définit un morphisme d'anneaux*

$$\varepsilon_x : \mathbb{Z}[X] \to A \ \ ,\ \ f \mapsto f(x) \ .$$

On l'appelle le morphisme d'évaluation *en x. C'est l'unique morphisme d'anneaux de $\mathbb{Z}[X]$ dans A qui envoie X sur x.*

Démonstration. On laisse au lecteur le soin de vérifier que l'évaluation en x définit un morphisme d'anneaux (les lois de l'anneau $\mathbb{Z}[X]$ ont été faites pour). On montre maintenant l'unicité. Soit un morphisme d'anneaux ψ de $\mathbb{Z}[X]$ dans A qui vérifie $\psi(X) = x$. Alors on a nécessairement, pour tous $a_n \in \mathbb{Z}$:

$$\psi\left(\sum_{n=0}^{N} a_n X^n\right) = \sum_{n=0}^{N} \psi(a_n X^n) = \sum_{n=0}^{N} a_n \psi(X^n) = \sum_{n=0}^{N} a_n \psi(X)^n = \sum_{n=0}^{N} a_n x^n \ .$$

Les deux premières égalités viennent de la compatibilité de ψ avec les sommes (et la soustraction), la troisième vient de la compatibilité de ψ avec les produits et l'unité 1_A. On a donc, pour tout $f \in \mathbb{Z}[X]$, $\psi(f) = f(x)$. Donc $\psi = \varepsilon_x$. □

Variantes : polynômes à plusieurs indéterminées

On peut aussi définir des anneaux de polynômes avec un nombre r d'indéterminées $X_1, \ldots, X_r$ à coefficients dans un anneau commutatif R, notés $R[X_1, \ldots, X_r]$. Un élément de cet anneau est une application $\mathbb{N}^r \to R\ ,\ (n_1, \ldots, n_r) \mapsto a_{n_1,\ldots,n_r}$ telle que $a_{n_1,\ldots,n_r} \neq 0$ seulement pour un nombre fini de multi-indices $(n_1, \ldots, n_r)$. On le représente par la combinaison linéaire *finie* :

$$f = \sum_{(n_1,\ldots,n_r)\in\mathbb{N}^r} a_{n_1,\ldots,n_r} X_1^{n_1} \cdots X_r^{n_r} \ .$$

Les lois $+$ et $\times$ sont définies de manière évidente. On note que les indéterminées commutent deux à deux : $X_i X_j = X_j X_i$ et que l'anneau $R[X_1, \ldots, X_r]$ est commutatif.

Remarque(s) 2.1.4. On a un isomorphisme d'anneaux naturel

$$R[X,Y] \simeq (R[X])[Y]$$

qui consiste à voir un polynôme en deux indéterminées X, Y comme un polynôme en une indéterminée Y dont les coefficients sont des polynômes en X. Plus généralement on a un isomorphisme d'anneaux naturel $R[X_1,\dots,X_r] \simeq (R[X_1,\dots,X_{r-1}])[X_r]$. Cette remarque permet parfois de prouver des propriétés des anneaux de polynomes à *plusieurs* indéterminées en se ramenant par récurrence au cas d'une seule indéterminée.

Remarque(s) 2.1.5. Soit un anneau quelconque A et des éléments $x_1,\dots,x_r \in A$ *qui commutent deux à deux*, c'est-à-dire : $x_i x_j = x_j x_i$ pour tout i,j (cette condition est automatiquement vérifiée si A est commutatif). Alors on peut évaluer un polynôme $f \in \mathbb{Z}[X_1,\dots,X_r]$ en les éléments $x_1,\dots,x_r$ pour produire un élément $f(x_1,\dots,x_r) \in A$. Cela donne lieu à un morphisme d'anneaux

$$\varepsilon_{x_1,\dots,x_r} : \mathbb{Z}[X_1,\dots,X_r] \to A \ , \ \ f \mapsto f(x_1,\dots,x_r)$$

qu'on appelle le morphisme d'évaluation en $x_1,\dots,x_r$. C'est l'unique morphisme d'anneaux de $\mathbb{Z}[X_1,\dots,X_r]$ dans A qui vérifie $\varepsilon_{x_1,\dots,x_r}(X_i) = x_i$ pour tout i.

2.1.6 Sous-anneaux

Définition 2.1.7 (Sous-anneau)**.** Soit $(A,+,\times)$ un anneau. Un *sous-anneau* de A est un sous-ensemble $B \subset A$ qui vérifie :

(1) $(B,+)$ est un sous-groupe abélien de $(A,+)$.

(2) $1_A \in B$.

(3) B est stable par $\times$: $\forall x,y \in B\,,\ x \times y \in B\,$;

Dans ce cas, $(B,+,\times)$ est alors un anneau, dont le neutre pour la multiplication est $1_B = 1_A$.

Remarque(s) 2.1.6. Si A est commutatif alors B l'est aussi.

Exemple(s) 2.1.4. (a) Exemple trivial : A est un sous-anneau de A.

(b) $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-anneaux de $\mathbb{R}$.

(c) L'ensemble des polynômes pairs $\mathbb{R}[X^2]$ est un sous-anneau de l'anneau des polynômes $\mathbb{R}[X]$.

(d) L'ensemble des fonctions continues $\mathcal{C}^0(\mathbb{R},\mathbb{R})$ est un sous-anneau de l'anneau des fonctions $\mathcal{F}(\mathbb{R},\mathbb{R})$.

(e) Le sous-groupe abélien $2\mathbb{Z} \subset \mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car il ne contient pas 1.

Exercice 3 Montrer que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$.

Propriété 2.1.5. *Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors* $\mathrm{Im}(\varphi)$ *est un sous-anneau de B.*

Démonstration. On vérifie les axiomes d'un sous-anneau :

(1) $\mathrm{Im}(\varphi)$ est un sous-groupe (abélien) de B car c'est l'image d'un morphisme de groupes (abéliens) ;

(2) $1_B = \varphi(1_A) \in \mathrm{Im}(\varphi)$;

(3) stabilité par $\times$: pour $y,y' \in \mathrm{Im}(\varphi)$ on peut écrire $y = \varphi(x)$ et $y' = \varphi(x')$ avec $x,x' \in A$, alors $yy' = \varphi(x)\varphi(x') = \varphi(xx') \in \mathrm{Im}(\varphi)$.

□

Remarque(s) 2.1.7. Attention : $\ker(\varphi)$ n'est pas un sous-anneau de A puisqu'il ne contient pas l'unité 1_A (sauf si B est l'anneau nul, c'est-à-dire si $0_B = 1_B$). La bonne notion est ici celle d'*idéal*, qui sera introduite et étudiée dans le chapitre suivant.

Remarque(s) 2.1.8. Si $B \subset A$ est un sous-anneau d'un anneau A, alors le morphisme d'inclusion $i : B \to A$ est un morphisme d'anneaux injectif. Plus généralement, si A et B sont des anneaux quelconques et $\varphi : B \to A$ est n'importe quel morphisme d'anneaux qui est injectif, alors φ induit un isomorphisme de B vers le sous-anneau $\mathrm{Im}(\varphi) \subset A$.

Comme dans le cas des groupes abéliens, on a la notion de sous-anneau engendré par une partie. On se restreint ici au cas, plus simple, des anneaux *commutatifs*.

Propriété 2.1.6. *Soit A un anneau commutatif et soient $x_1, \dots, x_r \in A$. Soit B l'ensemble des évaluations $f(x_1, \dots, x_r)$ pour $f \in \mathbb{Z}[X_1, \dots, X_r]$. Alors B est un sous-anneau de A. De plus, tout sous-anneau B' de A qui contient $x_1, \dots, x_r$ vérifie $B \subset B'$.*

Définition 2.1.8 (Sous-anneau engendré)**.** On l'appelle le *sous-anneau de A engendré par $x_1, \dots, x_r$*.

C'est donc le plus petit (pour l'inclusion) sous-anneau de A qui contient les éléments $x_1, \dots, x_r$.

Démonstration. Soit $\varepsilon_{x_1,\dots,x_r} : \mathbb{Z}[X_1, \dots, X_r] \to A$ le morphisme d'évaluation en $x_1, \dots, x_r$. Alors $B = \mathrm{Im}(\varepsilon_{x_1,\dots,x_r})$ est un sous-anneau de A. Si $B' \subset A$ est un sous-anneau qui contient $x_1, \dots, x_r$ alors (comme B' est un sous-groupe abélien de A, stable par $\times$ et qui contient 1_A) il contient l'évaluation de tout polynôme en $x_1, \dots, x_r$ et donc $B \subset B'$. □

2.1.7 Produits

Définition 2.1.9. Soient A et B deux anneaux. On munit le produit cartésien $A \times B$ d'une structure d'anneau en définissant la somme et le produit coordonnée par coordonnée :

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y)(x', y') = (xx', yy')$$

pour $(x, y), (x', y') \in A \times B$. L'élément neutre pour l'addition est $(0_A, 0_B)$ et l'élément neutre pour la multiplication est $(1_A, 1_B)$. Si A et B sont commutatifs alors $A \times B$ l'est aussi.

On peut aussi de cette façon définir une structure d'anneau sur le produit cartésien de n anneaux $\prod_{i=1}^{n} A_i$. Les propriétés suivantes se montrent directement à partir des définitions.

Exercice 4 Montrer que les projections sur les première et deuxième coordonnées sont des morphismes d'anneaux, par exemple $\pi_A : A \times B \to A$, $(x, y) \mapsto x$.
Montrer que les anneaux $A \times B$ et $B \times A$ sont isomorphes.
Montrer que les anneaux $(A \times B) \times C$, $A \times (B \times C)$, $A \times B \times C$ sont isomorphes.

Dans le cas particulier où $A_i = A$ pour tout i, la puissance cartésienne A^n est muni d'une structure d'anneau ; pour cette structure l'application $i : A \to A^n$, $x \mapsto (x, \dots, x)$ est un morphisme injectif d'anneaux. On peut plus généralement considérer une puissance cartésienne indexée par un ensemble S quelconque (notamment infini). Dans ce cas-là A^S se définit comme l'ensemble des applications $f : S \to A$, et les lois soit données par $(f + g)(s) = f(s) + g(s)$ et $(fg)(s) = f(s)g(s)$.

Exemple(s) 2.1.5.
1. Pour $S = A = \mathbb{R}$ on retrouve l'exemple déjà vu de l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.
2. Pour $S = \mathbb{N}$ on obtient l'anneau $A^{\mathbb{N}}$ des suites à valeurs dans A (où l'addition et la multiplication des suites se calcule terme à terme).

2.2 Éléments inversibles

Définition 2.2.1 (Inversible/unité)**.** Soit A un anneau. Un élément $x \in A$ est *inversible* (ou est une *unité*) s'il existe un élément $y \in A$ tel que $x \times y = 1_A = y \times x$. Alors y est unique et est noté x^{-1}, on l'appelle l'*inverse* de x dans l'anneau A.

Exercice 5 Montrer que l'inverse est bien unique (quand il existe).

Remarque(s) 2.2.1. On évite la notation $\frac{1}{x}$ dans un contexte non commutatif, et plus généralement les fractions, qui donnent lieu à des notations ambiguës, étant donné que $\frac{y}{x}$ pourrait signifier yx^{-1} ou $x^{-1}y$. Dans un contexte commutatif, ça ne pose pas de problème.

Définition 2.2.2. On note $A^\times$ l'ensemble des éléments inversibles de l'anneau A.

Propriété 2.2.1. *L'ensemble $A^\times$ des éléments inversibles d'un anneau A forme un groupe pour la multiplication, qu'on appelle le* groupe des inversibles de A *ou le* groupe des unités de A.

Démonstration. La multiplication est une loi de composition interne d'après le lemme précédent. On montre que les axiomes d'un groupe sont satisfaits :

(1) associativité : résulte de l'associativité de la multiplication dans l'anneau ;

(2) élément neutre : 1_A est inversible dans A (car $1_A \times 1_A = 1_A$) et est l'élément neutre pour la multiplication ;

(3) inverse : par définition, pour x inversible, x a un inverse x^{-1} pour la multiplication.

□

Si A est commutatif alors $A^\times$ est un groupe abélien (on insiste : la loi de groupe est la multiplication : le neutre est 1_A et l'inversion est $x \mapsto x^{-1}$).

Exemple(s) 2.2.1. (a) Le groupe des éléments inversibles de $\mathbb{Z}$ est $(\{-1, 1\}, \times)$. Il est isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z}, +)$.

(b) Le groupe des éléments inversibles de $\mathbb{R}$ est $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \times)$.

(c) Le groupe des éléments inversibles de $\mathcal{M}_n(\mathbb{R})$ est le groupe $(\mathrm{GL}_n(\mathbb{R}), \times)$. Il n'est pas abélien si $n \geq 2$.

Propriété 2.2.2. *Soit $\varphi : A \to B$ un morphisme d'anneaux et soit $x \in A^\times$, alors $\varphi(x) \in B^\times$ et $\varphi(x)^{-1} = \varphi(x^{-1})$. De plus, l'application induite $\varphi : A^\times \to B^\times$ est un morphisme de groupes.*

Démonstration. On calcule : $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_A) = 1_B$, et de même $\varphi(x^{-1})\varphi(x) = 1_B$. Le fait que $\varphi : A^\times \to B^\times$ est un morphisme de groupes est évident puisqu'on a $\varphi(xy) = \varphi(x)\varphi(y)$ pour tous $x, y \in A$ et donc notamment pour tous $x, y \in A^\times$. □

On va s'intéresser maintenant aux éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$; ceux-ci peuvent être décrit assez facilement.

Théorème 8. *Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$, alors on a les équivalences :*

(i) k est premier avec n.

(ii) la classe $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est un élément inversible pour la multiplication ;

(iii) la classe $\overline{k}$ est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. $(i) \Rightarrow (ii)$ Par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $ku + nv = 1$. Alors en prenant les classes modulo n on obtient $\overline{k}\overline{u} = \overline{1}$, donc $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

$(ii) \Rightarrow (iii)$ Supposons que $\overline{k}$ soit inversible ; pour calculer l'ordre de $\overline{k}$ dans le groupe abélien $\mathbb{Z}/n\mathbb{Z}$, on doit étudier l'ensemble suivant $\{l \in \mathbb{Z} \mid l.\overline{k} = \overline{0}\}$. Mais $l\overline{k} = \overline{0} \Leftrightarrow \overline{lk} = \overline{0}$. Mais puisque $\overline{k}$ est inversible la dernière égalité est équivalente à $\overline{l} = \overline{0}$ et donc $l \in n\mathbb{Z}$, et donc $\overline{k}$ est d'ordre n.

$(iii) \Rightarrow (i)$ Par contraposée : supposons que k ne soit pas premier avec n, et soit $d \geq 2$ un diviseur commun à k et n. Alors $\frac{n}{d}\overline{k} = \overline{n\frac{k}{d}} = \overline{0}$ et donc $\overline{k}$ est d'ordre un diviseur de $\frac{n}{d}$. □

Exemple(s) 2.2.2. Quel est l'inverse de $\overline{9}$ dans $\mathbb{Z}/31\mathbb{Z}$? On l'obtient grâce à une relation de Bézout, obtenue par l'algorithme d'Euclide : $31 = 9\times3+4$, $9 = 4\times2+1$, d'où $31\times2 = 9\times3\times2+4\times2 = 9\times6+9-1$, ou encore $9 \times 7 - 31 \times 2 = 1$, donc $\overline{9} \times \overline{7} = \overline{1}$. (Bien sûr, en multipliant 9 par 1, 2, 3, etc. et en prenant le reste modulo 31 on finira bien par tomber sur 1, mais c'est une méthode moins pratique...)

Propriété 2.2.3. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Démonstration. Si n est premier, alors par le théorème précédent $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\mathbb{Z}/n\mathbb{Z} \setminus \overline{0}$ et donc $\mathbb{Z}/n\mathbb{Z}$ est bien un corps. Réciproquement si n est composé, alors il existe a, b tels que $ab = n$ avec $a, b \neq 1, n$. Du coup on a l'égalité $\overline{a}\overline{b} = \overline{0}$. Si $\overline{a}$ est inversible, cela entraîne $\overline{b} = \overline{0}$ ce qui est une contradiction. Il existe donc un élément $\neq \overline{0}$ et non inversible. □

2.3 Indicatrice d'Euler

Définissons la fonction indicatrice d'Euler, ou plus brièvement l'indicatrice d'Euler.

Définition 2.3.1. L'indicatrice d'Euler est la fonction de $\mathbb{N}^*$ dans $\mathbb{N}$ définie par :

$$\varphi(n) = |\{k = 0, 1, \ldots, n-1 \mid k \text{ est premier avec } n\}|.$$

Remarque(s) 2.3.1. En utilisant le théorème 8, on voit immédiatement que $\varphi(n)$ est égal au nombre d'élements inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ ou bien au nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$.

Cette interprétation nous sera très utile pour montrer le théorème suivant.

Théorème 9. *L'indicatrice d'Euler vérifie les propriétés suivantes :*

(i) Pour tout n, m entiers non nuls premiers entre eux, on a : $\varphi(nm) = \varphi(n)\varphi(m)$;

(ii) Si p est un nombre premier et s un entier naturel alors $\varphi(p^s) = p^{s-1}(p-1)$.

(iii) Pour tout $n \in \mathbb{N}$ on a l'égalité :

$$\sum_{d|n} \varphi(d) = n.$$

Démonstration. Pour montrer le point (i), on fait appel au théorème des restes chinois vus dans la première partie. Si n et m sont premiers entre eux alors il existe un isomorphisme de groupes :

$$\bar{\Psi} : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Cet isomorphisme est en fait un isomorphisme d'anneaux (pour cela reprendre la définition de $\bar{\Psi}$ dans la démonstration du théorème des restes chinois de la partie I). D'après la proposition 2.2.2, il existe donc un isomorphisme de groupes :

$$\bar{\Psi} : (\mathbb{Z}/nm\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^\times,$$

mais par défintion de la loi produit (a, b) est inversible si et seulement si a et b sont inversibles et $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. Les deux groupes $(\mathbb{Z}/nm\mathbb{Z})^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ ont donc même cardinal ce qui se traduit par l'égalité $\varphi(nm) = \varphi(n)\varphi(m)$.

La preuve du point (ii) est laissée en exercice.

Pour le point (iii) on se place dans le groupe cyclique $G = \mathbb{Z}/n\mathbb{Z}$. Pour $d \mid n$, on considère définit l'ensemble suivant :

$$O_d = \{g \in G : g \text{ est d'ordre } d\}.$$

Les ensembles O_d forment une partition de G :

$$G = \coprod_{d|n} O_d.$$

Il suffit donc de montrer que O_d est de cardinal $\varphi(d)$. Mais par définition, on a $O_d \subset G_d$, où G_d est défini dans la propriété 1.7.2 :

$$G_d = \{g \in G \mid g^d = e\}.$$

Mais comme G_d est un groupe cyclique d'ordre d, les éléments de O_d, c'est à dire les éléments d'ordre d dans G_d sont de cardinal $\varphi(d)$ d'après le théorème 8, ce qui permet de conclure. □

2.4 Idéaux d'un anneau

Dans cette dernière partie, tous les anneaux sont implicitement supposés *commutatifs*.

2.4.1 Idéaux

Définition 2.4.1 (Idéal)**.** Soit A un anneau. Un *idéal* de A est un sous-ensemble I qui vérifie :

(1) I est un sous-groupe abélien de A ;

(2) I est stable par multiplication par tout élément de A :

$$\forall x \in I \ , \ \forall a \in A \ , \ ax \in I \ .$$

Exemple(s) 2.4.1. Exemples triviaux : $\{0\}$ et A sont des idéaux de A.

Remarque(s) 2.4.1. Ne surtout pas confondre la notion d'idéal et la notion de sous-anneau, qui sont différentes et qui jouent des rôles très différents dans la théorie des anneaux. En général, un idéal I ne contient pas 1_A.

La proposition suivante montre qu'il est facile de construire des idéaux.

Propriété 2.4.1. *Soit A un anneau et $x_1, \dots, x_r \in A$. Soit I l'ensemble des combinaisons linéaires $a_1x_1 + \cdots + a_rx_r$ avec $a_i \in A$ pour $i = 1, \dots, r$. Alors I est un idéal de A. De plus, tout idéal I' de A qui contient $x_1, \dots, x_r$ vérifie $I \subset I'$.*

Démonstration. (i) $0 \in I$ car $0 = 0x_1 + \cdots + 0x_r$.

(ii) I est stable par $+$: pour $a_1, \dots, a_r, a'_1, \dots, a'_r \in A$ on a

$$(a_1x_1 + \cdots + a_rx_r) + (a'_1x_1 + \cdots + a'_rx_r) = (a_1 + a'_1)x_1 + \cdots + (a_r + a'_r)x_r \in I \ .$$

(iii) I est stable par $-$: pour $a_1, \dots, a_r \in A$ on a

$$-(a_1x_1 + \cdots + a_rx_r) = (-a_1)x_1 + \cdots + (-a_r)x_r \ .$$

(iv) I est stable par multiplication par tout élément de A : pour $a_1, \dots, a_r \in A$ et $a \in A$ on a

$$a(a_1x_1 + \cdots + a_rx_r) = (aa_1)x_1 + \cdots + (aa_r)x_r \ .$$

Cela montre que I est un idéal de A. Maintenant, si I' est un idéal de A qui contient $x_1, \dots, x_r$, alors pour tout $a_1, \dots, a_r \in A$ on a par l'axiome (2) : $a_ix_i \in I'$, et par l'axiome (1) la somme $a_1x_1 + \cdots + a_rx_r$ doit aussi être dans I'. Donc $I \subset I'$. □

Cette proposition permet de donner la définition qui suit.

Définition 2.4.2 (Idéal engendré)**.** On appelle I l'*idéal de A engendré par $x_1, \dots, x_r$*, c'est le plus petit idéal de A contenant $x_1, \dots, x_r$ et on le note $(x_1, \dots, x_r)$ ou $Ax_1 + \cdots + Ax_r$.

Définition 2.4.3 (Idéal principal)**.** Soit A un anneau. Un *idéal principal* de A est un idéal engendré par un seul élément, c'est-à-dire de la forme

$$(x) = \{ax \ , \ a \in A\} \ .$$

Exemple(s) 2.4.2. (a) Les idéaux $\{0\} = (0)$ et $A = (1)$ sont principaux.

(b) Pour $A = \mathbb{Z}$ et $n \in \mathbb{Z}$ on a $(n) = n\mathbb{Z}$ l'ensemble des multiples de n.

(c) Pour $\mathbb{K}$ un corps, $A = \mathbb{K}[X]$, et un polynôme $f \in \mathbb{K}[X]$, on a l'idéal principal (f), l'ensemble des multiples de f.

Exercice 6 Soit $u \in A$ un élément inversible et $x \in A$ un élément quelconque. Montrer qu'on a l'égalité $(ux) = (x)$.

Exercice 7 Soit I un idéal de A et $x \in A$. Montrer qu'on a $(x) \subset I$ si et seulement si $x \in I$.

Nous allons maintenant rappeler une définition déjà utiliser en TD, puis définir la notion d'anneau principal.

Définition 2.4.4 (Anneau intègre)**.** Un anneau A est dit *intègre* si la propriété suivante est vérifiée : $\forall (a,b) \in A^2$, $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Définition 2.4.5 (Anneau principal)**.** Un anneau A est dit *principal* s'il est intègre et que tout idéal de A est principal.

Propriété 2.4.2. *Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z} = (n)$ pour $n \in \mathbb{N}$. En particulier, $\mathbb{Z}$ est un anneau principal.*

Démonstration. Un idéal de $\mathbb{Z}$ est en particulier un sous-groupe de $\mathbb{Z}$, et est donc de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$. Comme $n\mathbb{Z} = (n)$ est un idéal de $\mathbb{Z}$, ce sont tous les idéaux de $\mathbb{Z}$. □

Remarque(s) 2.4.2. On verra plus loin dans le cours que $\mathbb{K}[X]$ est un anneau principal si $\mathbb{K}$ est un corps. Par contre on montrera que l'anneau $\mathbb{Z}[X]$ n'est pas principal.

Propriété 2.4.3. *Soient A et B deux anneaux et $\varphi : A \to B$ un morphisme d'anneaux. Alors* $\ker(\varphi)$ *est un idéal de A.*

Démonstration. On sait déjà que $\ker(\varphi)$ est un sous-groupe abélien de A. Pour $x \in \ker(\varphi)$ et $a \in A$ on a $\varphi(ax) = \varphi(a)\varphi(x) = 0$ car $\varphi(x) = 0$, et donc $ax \in \ker(\varphi)$. □

La dernière proposition se généralise :

Propriété 2.4.4. *Soient A et B deux anneaux et $\varphi : A \to B$ un morphisme d'anneaux. Soit J un idéal de B. Alors $\varphi^{-1}(J)$ est un idéal de A.*

Pour $J = \{0\}$ on retrouve le fait que $\varphi^{-1}(\{0\}) = \ker(\varphi)$ est un idéal de A.

Démonstration. On sait déjà que $\varphi^{-1}(J)$ est un sous-groupe de A. Pour $x \in \varphi^{-1}(J)$ et $a \in A$ on a $\varphi(ax) = \varphi(a)\varphi(x) \in J$ car $\varphi(x) \in J$ et J est un idéal de B. Donc $ax \in \varphi^{-1}(J)$. □

Exercice 8 Montrer qu'en général l'image *directe* d'un idéal par un morphisme d'anneaux n'est pas un idéal.

2.5 Anneaux euclidiens

2.5.1 Définition

Un anneau euclidien est un anneau où il y a « une notion de division euclidienne ».

Définition 2.5.1. Soit A un anneau intègre. Une *jauge euclidienne* est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ qui vérifie : pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ avec

$$a = bq + r \quad \text{et} \quad (r = 0 \ \text{ ou } \ \nu(r) < \nu(b)) \ .$$

On appelle une telle identité une *division euclidienne* de a par b pour la jauge euclidienne ν. On dit que A est un *anneau euclidien* s'il possède une jauge euclidienne.

Notons qu'on ne demande pas d'avoir unicité de la division euclidienne.

Exemple(s) 2.5.1. L'anneau $\mathbb{Z}$ est euclidien, une jauge euclidienne est donnée par la valeur absolue : $\nu(m) = |m|$. (On pourra remarquer que pour cette jauge euclidienne, il n'y a pas unicité de la division euclidienne.)

Dans l'anneau des polynômes sur un corps $\mathbb{K}$ on peut également définir une division euclidienne.

2.5.2 Division euclidienne dans $\mathbb{K}[X]$

Soit R un anneau commutatif. On rappelle un peu de terminologie sur les polynômes (à coefficients dans R). Le *degré* d'un polynôme non nul $f = \sum_n a_n X^n$ est le plus grand entier n tel que $a_n \neq 0$, il est noté $\deg(f)$. On appelle *coefficient dominant* le coefficient du monôme $X^{\deg(f)}$. Par convention on pose $\deg(0) = -\infty$. Un polynôme est dit *unitaire* si son coefficient dominant est 1.

Propriété 2.5.1. *(1) On a* $\deg(f+g) \leq \max(\deg(f), \deg(g))$ *avec égalité si* $\deg(f) \neq \deg(g)$.

(2) L'égalité $\deg(fg) = \deg(f) + \deg(g)$ *est vraie (au moins) dans les cas suivants : si* $g \neq 0$ *a un coefficient dominant qui est inversible dans* R *(en particulier si* R *est un corps) ou si l'anneau* A *est intègre.*

Démonstration. 1) C'est évident.

2) L'égalité est toujours vraie si $f = 0$ ou $g = 0$ et on suppose donc que $f, g \neq 0$. Si a est le coefficient dominant de f et b le coefficient dominant de g alors le coefficient dominant de fg est le produit ab. Si b est inversible dans R ou si A est intègre et $b \neq 0$ l'égalité $ab = 0$ implique $a = 0$, ce qui est faux ; donc $ab \neq 0$.

□

Remarque(s) 2.5.1. La propriété sur le degré du produit de deux polynômes permet de montrer que l'anneau $\mathbb{Z}[X]$ n'est pas principal. Pour cela on peut considérer l'idéal

$$I = (2, X) = A.2 + AX = \{P.2 + QX : (P, Q) \in A^2\} = (2) + (X).$$

Par l'absurde : si I est principal, il existe $R \in \mathbb{Z}[X]$ tel que $I = (R)$. Comme $2 \in I$, on en déduit $2 = PR$ avec $P \in \mathbb{Z}[X]$, et donc par des considérations sur le degré, P est un polynôme constant. Comme $X \in I$, il existe $Q \in \mathbb{Z}[X]$ tel que $X = QP$, comme P est constant, toujours par des considérations de degré, on obtient que $P = \pm 1$, et donc au final $I = A$. Il existe donc P, Q tel que $1 = 2P + QX$ ce qui est impossible puisque le coefficient constant de $2P + QX$ est pair.
Voici une autre utilisation (plus directe) de la notion de degré : si $\mathbb{K}$ est un corps, l'ensemble des inversibles de $\mathbb{K}[X]$ est égal $\mathbb{K}^\times$ (exercice).

Le théorème suivant permet d'effectuer la division euclidienne pour des polynômes à coefficients dans un anneau, dans certains cas.

Propriété 2.5.2. *Soit* $f \in R[X]$ *et* $g \in R[X] \setminus \{0\}$ *tel que le coefficient dominant de* g *est inversible dans* R. *Alors il existe un couple* $(q, r) \in R[X]$ *avec* $\deg(r) < \deg(g)$ *tels que*

$$f = gq + r \ .$$

Le couple (q, r) *est unique.*

Le théorème est notamment valable dans le cas (utile) où g est unitaire. Si $R = \mathbb{K}$ est un corps, l'hypothèse sur g est automatiquement vérifiée.

Démonstration. – Existence. On fixe g et on prouve le résultat par récurrence sur le degré de f (pour être précis, c'est une récurrence qui est initialisée à $-\infty$, qu'on imagine comme le prédécesseur de 0). Soit $m = \deg(g)$. Si $\deg(f) < m$ le résultat est évident puisqu'on peut écrire $f = g \times 0 + f$. Soit donc $n \geq m$, on suppose que le résultat est prouvé pour tous les polynômes de degré $\leq n-1$. Soit f un polynôme de degré n. On note b le coefficient dominant de g et a le coefficient dominant de f. On a donc $g = bX^m +$ (termes de degré inférieur) et $f = aX^n +$ (termes de degré inférieur). Rappelons que par hypothèse b est inversible dans R. Donc $\widetilde{f} = f - g \times (ab^{-1}X^{n-m})$ est de degré $\leq n-1$. Par l'hypothèse de récurrence il existe $\widetilde{q}, \widetilde{r} \in R[X]$ avec $\deg(\widetilde{r}) < \deg(g)$ tels que $\widetilde{f} = g\widetilde{q} + \widetilde{r}$. On a donc $f = g(\widetilde{q} + ab^{-1}X^{n-m}) + \widetilde{r}$. En posant $q = \widetilde{q} + ab^{-1}X^{n-m}$ et $r = \widetilde{r}$, on a donc $f = gq + r$ et le résultat est prouvé. Fin de la récurrence.

– Unicité. Soient (q_1, r_1) et (q_2, r_2) deux couples qui fonctionnent. Alors on a $q_1 g + r_1 = q_2 g + r_2$ et donc $(q_1 - q_2)g = r_2 - r_1$. Si $q_1 \neq q_2$, comme le coefficient dominant de g est inversible dans R on a par le lemme précédent : $\deg(g(q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g)$. Or $\deg(r_2 - r_1) \leq \max(\deg(r_1), \deg(r_2)) < \deg(g)$, contradiction. Donc $q_1 = q_2$ et $r_1 = r_2$.

□

Théorème 10. *Tout anneau euclidien est principal.*

Démonstration. On copie la preuve du fait que $\mathbb{Z}$ est un anneau principal. Soit $I \subset A$ un idéal. Si $I = \{0\}$ alors $I = (0)$ est principal. Sinon I contient des éléments non nuls, et on choisit un élément $x \in I \setminus \{0\}$ tel que $\nu(x)$ est minimal, ce qui est possible car ν prend ses valeurs dans $\mathbb{N}$. On a donc : pour tout $y \in I \setminus \{0\}$, $\nu(y) \geq \nu(x)$. Comme $x \in I$, on a l'inclusion $(x) \subset I$ et on veut montrer l'inclusion réciproque. Soit $y \in I$, on a une division euclidienne $y = xq + r$, avec $r = 0$ ou $\nu(r) < \nu(x)$. Comme I est un idéal on a que $r = y - xq \in I$, et donc $r = 0$ par minimalité de $\nu(x)$. Ainsi, on a $y = xq \in (x)$. On a donc montré qu'on a $I = (x)$. Donc tout idéal de A est principal et A est un anneau principal. □

On déduit immédiatement de cette propriété le théorème qui suit.

Théorème 11. *(i) L'anneau $\mathbb{Z}$ est euclidien, donc principal ;*

(ii) Si $\mathbb{K}$ est un corps, alors l'anneau $\mathbb{K}[X]$ est euclidien donc principal.

Remarque(s) 2.5.2. Il existe des anneaux principaux qui ne sont pas euclidiens, mais ce n'est pas si facile à prouver en pratique. On n'en verra pas en exercice. Pour votre culture, un exemple d'un tel anneau est le sous-anneau de $\mathbb{C}$ donné par

$$A = \left\{ a + b\frac{1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\} .$$

(Vérifiez que c'est bien un sous-anneau de $\mathbb{C}$.)

Remarque(s) 2.5.3. On a vu que l'anneau $\mathbb{Z}[X]$ n'est pas principal, il n'est donc pas euclidien.

2.6 Algèbre sur un corps

On rappelle la définition d'un espace vectoriel sur un corps.

Définition 2.6.1 (Espace vectoriel)**.** Soit $\mathbb{K}$ un corps. Un $\mathbb{K}$-*espace vectoriel* (ou *espace vectoriel sur* $\mathbb{K}$) est un triplet $(E, +, .)$ où E est un ensemble, $+$ est une loi de composition interne sur E, et $.$ est une loi de composition externe $\mathbb{K} \times E \to E$, $(a, x) \mapsto a.x$ telles que :

(1) $(E, +)$ est un groupe abélien ;

(2) linéarité de la loi $. : \forall a \in \mathbb{K}, \forall x, y \in E, a.(x + y) = a.x + a.y$;

(3) compatibilité à l'addition dans $\mathbb{K} : \forall a, b \in \mathbb{K}, \forall x \in E, (a + b).x = a.x + b.x$;

(4) compatibilité à la multiplication dans $\mathbb{K} : \forall a, b \in \mathbb{K}, \forall x \in E, (ab).x = a.(b.x)$;

(5) compatibilité à l'unité de $\mathbb{K} : \forall x \in E, 1_{\mathbb{K}}.x = x$.

Remarque(s) 2.6.1. Les théorèmes classiques d'algèbre linéaire (pivot de Gauss, théorie des bases et de la dimension, existence de supplémentaires, théorème du rang, déterminant des matrices, etc.) sont vrais quel que soit le corps, même si on vous les a peut-être seulement énoncés pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Dans la définition précédente on peut remplacer le corps $\mathbb{K}$ par un anneau commutatif A, on obtient la notion de A-module que vous rencontrerez plus tard.

Définition 2.6.2 (Algèbre sur un corps)**.** Soit $\mathbb{K}$ un corps. Une $\mathbb{K}$-*algèbre* (ou *algèbre sur* $\mathbb{K}$) est un quadruplet $(A, +, ., \times)$ où :

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

(2) $(A, +, \times)$ est un anneau ;

(3) les lois $.$ et $\times$ sont compatibles : $\forall a, b \in \mathbb{K}, \forall x, y \in A, (a.x) \times (b.y) = (ab).(x \times y)$.

On a les notions évidentes de morphisme d'algèbres (application qui est à la fois $\mathbb{K}$-linéaire et un morphisme d'anneaux) et de sous-algèbre (sous-ensemble qui est à la fois un sous-$\mathbb{K}$-espace vectoriel et un sous-anneau).

Exemple(s) 2.6.1. (a) Le corps $\mathbb{K}$ lui-même est une $\mathbb{K}$-algèbre.

(b) Plus généralement, soit $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Alors $\mathbb{L}$ est naturellement une $\mathbb{K}$-algèbre. (Le vérifier !) Par exemple, $\mathbb{C}$ est une $\mathbb{R}$-algèbre.

(c) L'anneau de polynômes $\mathbb{K}[X_1, \ldots, X_r]$ est une $\mathbb{K}$-algèbre.

(d) L'anneau des matrices $\mathcal{M}_n(\mathbb{K})$ est une $\mathbb{K}$-algèbre (non commutative si $n \geq 2$).

(e) Pour E un $\mathbb{K}$-espace vectoriel on a la $\mathbb{K}$-algèbre des endomorphismes $\mathbb{K}$-linéaires de E, notée $\mathcal{L}(E)$, pour laquelle le produit est la composition. On a l'isomorphisme de $\mathbb{K}$-algèbres $\mathcal{L}(K^n) \simeq \mathcal{M}_n(K)$, qui à un endomorphisme de $\mathbb{K}^n$ associe sa matrice dans la base canonique.

Soit A une $\mathbb{K}$-algèbre et $x \in A$. Pour un polynôme $f \in \mathbb{K}[X]$ à coefficients dans $\mathbb{K}$, la structure de $\mathbb{K}$-algèbre de A permet de donner un sens à l'*évaluation* $f(x) \in A$. Par exemple, pour $f = \lambda X^2 + \mu X + \nu$ avec $\lambda, \mu, \nu \in K$, on a $f(x) = \lambda.(x \times x) + \mu.x + \nu.1_A$. Comme dans la Proposition 2.1.4, cette operation d'évaluation est compatible la structure de $\mathbb{K}$-algèbre sur $\mathbb{K}[X]$ au sens de la proposition suivante.

Propriété 2.6.1. *Soit A une $\mathbb{K}$-algèbre et $x \in A$. L'évaluation des polynômes en x définit un morphisme de $\mathbb{K}$-algèbres*

$$\varepsilon_x : \mathbb{K}[X] \to A \ , \ \ f \mapsto f(x) \ .$$

On l'appelle le morphisme d'évaluation *en x. C'est l'unique morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ dans A qui envoie X sur x.*

Démonstration. On montre facilement que l'évaluation définit un morphisme de $\mathbb{K}$-algèbres. L'unicité se montre aussi facilement, comme dans la Proposition 2.1.4. □

L'évaluation permet de définir la notion de polynômes annulateurs et minimaux. Soit A une $\mathbb{K}$-algèbre, pas nécessairement commutative (on pense notamment à $A = \mathcal{M}_n(\mathbb{K})$). Soit $x \in A$. Alors on a le morphisme d'évaluation en x :

$$\varepsilon_x : \mathbb{K}[X] \to A \ , \ \ f \mapsto f(x) \ .$$

Alors $\ker(\varepsilon_x)$ est un idéal de $\mathbb{K}[X]$. Un élément de cet idéal est appelé *polynôme annulateur* de l'élément $x \in A$. Comme $\mathbb{K}[X]$ est principal on a $\ker(\varepsilon_x) = (f)$ pour un certain polynôme $f \in \mathbb{K}[X]$, qu'on appelle un *polynôme minimal* de l'élément $x \in A$. Il est unique à multiplication par un scalaire non nul près (élément de $\mathbb{K}^\times$).

Remarque(s) 2.6.2. Dans le cas où $A = \mathcal{M}_n(\mathbb{K})$ est une algèbre de matrices, vous avez déjà rencontré l'évaluation d'un polynôme en une matrice dans vos cours d'algèbre linéaire. Nous retrouverons cette notion dans la troisième et dernière partie de cette UE.