Université Pierre & Marie Curie

Cours d'arithmétique

LM 220

Pierre Wassef

Le chapitre 0 *rappelle les notions prérequises et les définitions les plus importantes.*
Il n'est pas traité en cours
mais il est fortement recommandé de lire ce chapitre avant d'aborder le cours.

Les chapitres ou paragraphes dont les intitulés sont suivis du signe (♮)
sont des compléments de cours facultatifs.

Table des matières

Chapitre 0

Rappels

0.1 L'ensemble $\mathbb{N}$ des entiers naturels

L'arithmétique est l'étude des propriétés des nombres entiers, appelés aussi entiers naturels. L'ensemble $\mathbb{N}$ des entiers naturels est l'ensemble fondamental à partir duquel se sont construites les mathématiques, nous admettrons l'existence de cet ensemble ainsi que les trois propriétés qui le caractérisent :

- N_1 : *L'ensemble* $\mathbb{N}$ *est un ensemble totalement ordonné qui admet l'entier* 0 *comme plus petit élément.*
- N_2 : *Tout élément de* $n \in \mathbb{N}$ *admet un successeur*, c'est-à-dire un élément $n' > n$ tel qu'il n'existe aucun élément de $\mathbb{N}$ strictement compris entre n et n'. (Montrer à titre d'exercice que ce successeur est alors unique.)
  Cela permet de définir l'entier $1 \in \mathbb{N}$ comme le successeur de 0, l'entier 2 comme le successeur de 1, etc. Pour chaque entier $n \in \mathbb{N}$, on désigne par $n+1$ le successeur de n.
- N_3 : *L'ensemble* $\mathbb{N}$ *obéit au* **principe de récurrence**.

0.1.1 Principe de récurrence

Principe de récurrence *Soit A une partie de $\mathbb{N}$ vérifiant les deux conditions suivantes*

1. $\exists n_0 \in \mathbb{N},\ n_0 \in A$,
2. $\forall n \geq n_0, \quad [(n \in A) \Longrightarrow (n+1 \in A)]$.

alors

$$\forall n \geq n_0, \ \ n \in A.$$

Le principe de récurrence justifie ce qu'on appelle les démonstrations par récurrence, qui ne concernent que les énoncés où interviennent des entiers.

Démonstration par récurrence

Soit à démontrer qu'un énoncé $P(n)$ est vrai pour tout entier $n \geq n_0$. Si on pose

$$A = \{n \in \mathbb{N} \,|\, P(n) \text{ est vrai}\},$$

il suffit, en vertu du principe de récurrence, de démontrer que

1. $P(n_0)$ est vrai,
2. $\forall n \geq n_0, \quad [P(n) \Longrightarrow P(n+1)]$.

Il existe des variantes de démonstrations par récurrence, par exemple :

Variante 1 *Pour démontrer que $P(n)$ est vrai pour tout $n \geq n_0$, il suffit de démontrer que*

1. $P(n_0)$ et $P(n_0+1)$ sont vrais,
2. $\forall n \geq n_0+1, \quad [(P(n-1) \text{ et } P(n)) \Longrightarrow P(n+1)]$.

Variante 2 *Pour démontrer que $P(n)$ est vrai pour tout $n \geq n_0$, il suffit de démontrer que*

1. $P(n_0)$ est vrai,
2. $\forall n \geq n_0, \quad [(\forall k \in [n_0, n],\ P(k)) \Longrightarrow P(n+1)]$.

(On rappelle que l'intervalle $[n_0, n]$ désigne l'ensemble des entiers $k \in \mathbb{N}$ vérifiant $n_0 \leq k \leq n$.)

Exercice 1 — Montrer que si deux entiers admettent le même successeur, ils sont égaux.

Exercice 2 — Démontrer par récurrence que tout entier $n \geq 1$ admet un prédécesseur, c'est-à-dire un entier dont il est le successeur, et que ce prédécesseur est unique.

Exercice 3 — Pour chaque $n \in \mathbb{N}$, définir (par récurrence) l'entier $n+k$, pour tout $k \in \mathbb{N}$, à partir de la propriété N_2.

0.1.2 Propriété fondamentale de $\mathbb{N}$

La propriété suivante de l'ensemble $\mathbb{N}$, assez intuitive, intervient dans la démonstration des théorèmes essentiels de ce cours, elle implique en particulier l'existence de la division euclidienne. Elle constitue en elle-même un exemple important de ce qu'on appelle en mathématiques un *théorème d'existence*.

Théorème 0.1 Propriété fondamentale de $\mathbb{N}$ *Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.*

Preuve : Soit A une partie non vide de $\mathbb{N}$. Si $0 \in A$, 0 est le plus petit élément de A.
Si $0 \notin A$, alors $0 \in \mathbb{N} \setminus A$, et il existe un entier $n_1 \in \mathbb{N}$ tel que

1. $[0, n_1] \subseteq \mathbb{N} \setminus A$,
2. $(n_1+1) \in A$.

En effet, si tel n'était pas le cas, on aurait pour chaque entier $n \in \mathbb{N}$ l'implication

$$([0,n] \subseteq \mathbb{N} \setminus A) \Longrightarrow ((n+1) \in \mathbb{N} \setminus A),$$

et comme $0 \in \mathbb{N} \setminus A$, on en déduirait $\mathbb{N} \setminus A = \mathbb{N}$, (variante 2 ci-dessus), donc $A = \emptyset$, ce qui est contraire aux hypothèses. Il est clair que l'entier $a = n_1 + 1$ est le plus petit élément de A. □

0.2 Opérations

On définit une *addition* sur $\mathbb{N}$ à partir de la propriété N_2, (cf. exercice 3 ci-dessus), c'est-à-dire un application qui à chaque couple d'entiers $(n,k) \in \mathbb{N} \times \mathbb{N}$ fait correspondre leur somme $n+k \in \mathbb{N}$. On généralise cela, sous le vocable d' "opération", ou de "loi de composition interne", à un ensemble quelconque.

Une **loi de composition interne $*$, ou opération** $*$ sur un ensemble E est donc tout simplement une application de $E \times E$ dans E, que l'on note

$$(x,y) \longmapsto x * y.$$

Exemples

1. $E = \mathbb{N}$ avec $(x,y) \longmapsto x+y$.
2. E est l'ensemble des parties d'un ensemble A, avec $(x,y) \longmapsto x \cap y$.
3. E est l'ensemble des applications d'un ensemble A dans lui-même, avec $(x,y) \longmapsto x \circ y$.

Cependant, pour qu'une opération soit intéressante, il est nécessaire qu'elle possède un certain nombre des propriétés ci-dessous, qui ne sont autres que les propriétés bien connues de l'addition et de la multiplication usuelles.

Définition 0.1 *Une opération $*$ sur un ensemble E est dite*

1. ***Associative*** *si* $\forall (x,y,z) \in E \times E \times E, \quad (x*y)*z = x*(y*z)$.
   C'est l'associativité qui permet de définir l'élément $x*y*z \in E$ en écrivant
   $$x*y*z = (x*y)*z = x*(y*z).$$
2. ***Posséder un élément neutre*** *s'il existe un élément $e \in E$ vérifiant*
   $$\forall x \in E, \quad e*x = x*e = x.$$
3. ***Commutative*** *si* $\forall (x,y) \in E \times E, \quad x*y = y*x$.

Définition 0.2 *On dit qu'une partie F de E est* ***stable*** *pour l'opération $*$ si*

$$\forall (x,y) \in F \times F, \quad x*y \in F.$$

On peut alors parler de la ***restriction*** *de l'opération $*$ à l'ensemble F.*

Dans ce qui suit, les opérations seront notées sous l'une des deux formes suivantes.
- ***Notation additive*** $(x,y) \longmapsto x+y$. L'élément neutre, s'il existe, sera alors **toujours désigné par** 0.
- ***Notation multiplicative*** $(x,y) \longmapsto xy$ (ou $x.y$ ou $x \times y$). L'élément neutre, s'il existe et sauf mention du contraire, **sera désigné par** 1.

Définition 0.3 *Avec les notations précédentes, si l'opération possède un élément neutre, on dit qu'un élément $x \in E$ possède un* ***symétrique****, ou est* ***inversible*** *(en notation multiplicative) ou possède un* ***opposé*** *(en notation additive), s'il existe un élément $y \in E$ vérifiant*

$$\begin{array}{lccccccl} & x*y & = & y*x & = & e & \textit{en notation générale,} \\ \textit{respectivement} & xy & = & yx & = & 1 & \textit{en notation multiplicative,} \\ \textit{respectivement} & x+y & = & y+x & = & 0 & \textit{en notation additive.} \end{array}$$

En notation multiplicative, on dit alors que y est ***l'inverse*** *de x et on note $y = x^{-1}$.*
En notation additive, on dit que y est ***l'opposé*** *de x, on note $y = -x$.*

Voici un exemple de démonstration de portée générale, mais utilisant pour des raisons de légèreté et de lisibilité la notation multiplicative.

Proposition 0.2 *1. Si une opération possède un élément neutre, celui-ci est unique.*
2. Si l'opération est associative et possède un élément neutre, le symétrique d'un élément $x \in E$, s'il existe, est unique.

Preuve :

1. Soit 1 et e deux éléments neutres, alors
   $$\left.\begin{array}{rcl} (1 \text{ est élément neutre }) & \Longrightarrow & (1e = e1 = 1) \\ (e \text{ est élément neutre }) & \Longrightarrow & (1e = e1 = e) \end{array}\right\} \Longrightarrow (e = 1).$$
2. Si y et z sont deux inverses de $x \in E$, on écrit $z = 1z = (yx)z = y(xz) = y1 = y$. □

On admettra dans ce qui suit l'existence des ensembles suivants, construits à partir de $\mathbb{N}$, ainsi que les propriétés essentielles de l'addition et de la multiplication définies sur ces ensembles.
- L'ensemble $\mathbb{Z}$ des entiers relatifs.
- L'ensemble $\mathbb{Q}$ des nombres rationnels.
- L'ensemble $\mathbb{R}$ des nombres réels.
- L'ensemble $\mathbb{C}$ des nombres complexes.

0.3 Groupes

Définition 0.4 *Un groupe est la donnée d'un ensemble G muni d'une opération possédant les propriétés suivantes.*

1. *Elle est associative.*
2. *Elle possède un élément neutre.*
3. *Tout élément de G admet un inverse.*

Si de plus l'opération est commutative, on dit que le groupe est commutatif ou abélien.

Conventions et notations

- Un groupe dont l'opération est représentée par la multiplication sera appelé groupe multiplicatif, son élément neutre sera, sauf mention du contraire, désigné par 1.
- Un groupe dont l'opération est représentée par l'addition sera appelé groupe additif, et sauf mention du contraire, son élément neutre sera désigné par 0.
- S'il peut y avoir ambiguïté sur l'opération $*$ du groupe, ou si on veut préciser cette opération, on adoptera la notation $(G, +)$ ou $(G, \times)$.
- Si rien n'est spécifié, un groupe quelconque G sera noté multiplicativement.
- Tout **groupe additif** sera, sauf mention du contraire, **supposé commutatif**.

Exemples

1. $(\mathbb{Z}, +)$ est un groupe commutatif.
2. $(\mathbb{Q}, +)$ est un groupe commutatif.
3. $(\mathbb{R}, +)$ est un groupe commutatif.
4. $(\mathbb{C}, +)$ est un groupe commutatif.
5. $(\mathbb{Q}, \times)$ n'est pas un groupe.
6. $(\mathbb{Q} \setminus \{0\}, \times)$ est un groupe commutatif.
7. $(\mathbb{R}, \times)$ n'est pas un groupe.
8. $(\mathbb{R} \setminus \{0\}, \times)$ est un groupe commutatif.
9. $(\mathbb{R}_+ \setminus \{0\}, \times)$ est un groupe commutatif.
10. $(\mathbb{R}_- \setminus \{0\}, \times)$ n'est pas un groupe.
11. $(\mathbb{C}, \times)$ n'est pas un groupe.
12. $(\mathbb{C} \setminus \{0\}, \times)$ est un groupe commutatif.
13. $(\mathbb{N}, +)$ n'est pas un groupe.
14. $(\mathbb{Z}, \times)$ n'est pas un groupe.
15. Si A est un ensemble. L'ensemble G des bijections de A sur lui-même est un groupe pour la composition des applications $(f,\ g) \in G \times G \longmapsto f \circ g \in G$.

    L'élément neutre de G est l'application identique I_{d_A} de A sur A.

    Si A possède au moins trois éléments, ce groupe n'est pas commutatif.
16. En particulier, soit $n \geq 2$ un entier et soit $A = \{1, 2, \ldots, n\} \subset \mathbb{N}$. Le groupe des bijections de A s'appelle *groupe des permutations* de $\{1, 2, \ldots, n\}$, on le note $\mathcal{G}_n$, il possède $n!$ éléments. *Le groupe $\mathcal{G}_n$ n'est commutatif que si $n = 2$.*

Proposition 0.3 *Soit G un groupe, et soit x et y deux éléments de G, alors*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Preuve : $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1.$ □

Définition 0.5 *Soit G_1 et G_2 deux groupes. Une application $\boldsymbol{u}$ de G_1 dans G_2 est un **morphisme de groupes** si*

$$\forall (x,y) \in G_1 \times G_1, \quad \boldsymbol{u}(xy) = \boldsymbol{u}(x)\boldsymbol{u}(y).$$

*Si de plus l'application $\boldsymbol{u}$ est une bijection, on dit que $\boldsymbol{u}$ est un **isomorphisme** de groupes, les groupes G_1 et G_2 sont alors dits **isomorphes**.*

Exercice 4 — Écrire la définition qui précède en notation additive.

On démontrera les deux propositions qui suivent à titre d'exercice.

Proposition 0.4 *Soit $\boldsymbol{u}$ un morphisme du groupe G_1 dans le groupe G_2. Alors on a*

$$\boldsymbol{u}(1) = 1 \quad et \quad \forall x \in G_1, \quad \boldsymbol{u}(x^{-1}) = [\boldsymbol{u}(x)]^{-1}.$$

Proposition 0.5 *Soit $\boldsymbol{u}$ un isomorphisme du groupe G_1 sur le groupe G_2, alors l'application réciproque $\boldsymbol{u}^{-1}$ est un isomorphisme du groupe G_2 sur le groupe G_1. ($\boldsymbol{u}^{-1}$ est appelé **isomorphisme réciproque** de $\boldsymbol{u}$).*

Exercice 5 — Montrer que l'application exponentielle $x \mapsto e^x$ est un isomorphisme du groupe additif $(\mathbb{R}, +)$ sur le groupe multiplicatif $(\mathbb{R}_+ \backslash \{0\}, \times)$. Quel en est l'isomorphisme réciproque ?

Théorème 0.6 *Soit G un groupe, a et b deux éléments de G, l'équation $ax = b$ admet une solution et une seule dans G. Autrement dit,*

l'application $x \longmapsto ax$ est une bijection de G sur lui-même.

Preuve : On a les équivalences $(ax = b) \Longleftrightarrow (a^{-1}ax = a^{-1}b) \Longleftrightarrow (x = a^{-1}b)$. □

Ce résultat est évidemment vrai si le groupe est noté additivement, l'application $x \longmapsto a + x$ est une bijection de G sur lui-même.

Un groupe G est fini si l'ensemble G est fini. Le nombre d'éléments de G est alors appelé **ordre** du groupe G. Ainsi, le groupe $\mathcal{G}_n$ des permutations de l'ensemble $\{1, 2, \ldots, n\}$ est un groupe fini d'ordre $n!$.

Proposition 0.7 *Soit G_1 et G_2 deux groupes additifs. On munit l'ensemble produit $G_1 \times G_2$ de l'addition définie par*

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2). \tag{1}$$

1. *Cette addition fait de $G_1 \times G_2$ un groupe, appelé **groupe produit** de G_1 et G_2.*
2. *Le projecteur $\Pi_1 : (x, y) \mapsto x$ de $G_1 \times G_2$ dans G_1, (resp. $\Pi_2 : (x, y) \mapsto y$ de $G_1 \times G_2$ dans G_2) est un morphisme de groupes.*

Exercice 6 — Écrire l'analogue de (1) lorsque G_1 et G_2 sont deux groupes multiplicatifs.

0.3.1 Sous-groupes

Définition 0.6 (Sous-groupe) *Soit G un groupe. Une partie H de G est un sous-groupe de G si les conditions suivantes sont réalisées*

1. $\forall (x,y) \in H \times H,\ \ xy \in H$.
2. $1 \in H$.
3. $\forall x \in H,\ \ x^{-1} \in H$.

Remarques

1. La condition 1 ci-dessus signifie que H est stable pour l'opération de G.
2. La restriction à H de l'opération de G fait de H un groupe.

Exercice 7 — Réécrire la définition qui précède en notation additive.

Proposition 0.8 *Avec les notations ci-dessus, H est un sous-groupe de G si et seulement si*

1. $H \neq \emptyset$.
2. $\forall (x,y) \in H \times H,\ \ xy^{-1} \in H$.

Preuve : Il existe $x \in H$ d'après 1., il résulte alors de 2. que $xx^{-1} = 1 \in H$.
On en déduit que pour tout $y \in H$, $1y^{-1} = y^{-1} \in H$.
Il en résulte que si $(x,y) \in H \times H$, $(x, y^{-1}) \in H \times H$ donc $x(y^{-1})^{-1} = xy \in H$. □

Exercice 8 — Montrer que si H est un sous-groupe de G et si K est un sous-groupe de H, alors K est un sous-groupe de G.

Proposition 0.9 *Soit $\boldsymbol{u}$ un morphisme du groupe G_1 dans le groupe G_2.*

1. *Si H_1 est un sous-groupe de G_1, $\boldsymbol{u}(H_1) = \{\boldsymbol{u}(h) \,|\, h \in H_1\}$ est un sous-groupe de G_2.*
2. *Si H_2 est un sous-groupe de G_2, $\boldsymbol{u}^{-1}(H_2) = \{x \in G_1 \,|\, \boldsymbol{u}(x) \in H_2\}$ est un sous-groupe de G_1, en particulier, si e_2 est l'élément neutre de G_2, $\boldsymbol{u}^{-1}(\{e_2\})$ est un sous-groupe de G_1, appelé **noyau** de $\boldsymbol{u}$ et noté* $\ker(\boldsymbol{u})$.
3. *$\boldsymbol{u}$ est injectif si est seulement si* $\ker(\boldsymbol{u}) = \{e_1\}$. *Si c'est le cas, les groupes G_1 et $\boldsymbol{u}(G_1)$ sont isomorphes.*

Preuve : Les points 1. et 2. sont faciles à établir. Pour 3., remarquons que si x et $y \in G$, on a

$$(\mathbf{u}(x) = \mathbf{u}(y)) \Longleftrightarrow \left(e_2 = \mathbf{u}(x)\,(\mathbf{u}(y))^{-1} = \mathbf{u}(xy^{-1})\right) \Longleftrightarrow \left(xy^{-1} \in \ker(\mathbf{u})\right).$$ □

Exemples

1. $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$, qui est un sous-groupe de $\mathbb{R}$, lequel est un sous-groupe de $\mathbb{C}$.
2. Le groupe $\{-1, 1\}$ est un sous-groupe de $\mathbb{Q} \setminus \{0\}$, qui est un sous-groupe de $\mathbb{R} \setminus \{0\}$, lequel est un sous-groupe de $\mathbb{C} \setminus \{0\}$.
3. Le groupe $\mathbb{R}_+ \setminus \{0\}$ est un sous-groupe de $\mathbb{R} \setminus \{0\}$.
4. Tout groupe G admet les deux sous-groupes $H_1 = G$ et $H_2 = \{1\}$. Ces deux sous-groupes sont appelés **sous-groupes triviaux** de G.
5. Le cercle unité $C = \{z \in \mathbb{C} \,|\, |z| = 1\}$ est un sous groupe de $\mathbb{C} \setminus \{0\}$. (Le démontrer directement, puis à partir de la proposition 0.9.)

Dans la suite de ce paragraphe, G désigne un groupe et x un élément de G.

Définition 0.7 – *Si G est un groupe **multiplicatif**, on définit les **puissances** de x par*

$$\forall k \in \mathbb{Z}, \quad x^k = \begin{cases} 1 & si \ \ k = 0 \\ \underbrace{x.x.\ldots.x}_{k \text{ fois}} & si \ \ k > 0 \\ \underbrace{x^{-1}.x^{-1}.\ldots.x^{-1}}_{-k \text{ fois}} & \text{si } \ k < 0 \end{cases}$$

On pose alors $\langle x \rangle = \{x^k \,|\, k \in \mathbb{Z}\} \subseteq G.$

– *Si G est un groupe **additif**, on définit les **multiples** de x par*

$$\forall k \in \mathbb{Z}, \quad kx = \begin{cases} 0 & si \ \ k = 0 \\ \underbrace{x + x + \cdots + x}_{k \text{ fois}} & si \ \ k > 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{-k \text{ fois}} & si \ \ k < 0 \end{cases}$$

On pose alors $\langle x \rangle = \{kx \,|\, k \in \mathbb{Z}\} \subseteq G.$

Théorème 0.10 *Avec les notations précédentes, l'ensemble $\langle x \rangle$ est un sous-groupe de G. De plus, pour tout sous-groupe H de G, on a l'implication*

$$(x \in H) \quad \Longrightarrow \quad (\langle x \rangle \subseteq H)\,,$$

*ce qui signifie que $\langle x \rangle$ **est le plus petit sous-groupe de G contenant** x.*

Preuve : On a $1 = x^0 \in \langle x \rangle$,
$\forall k \in \mathbb{Z}, \ \ (x^k)^{-1} = x^{-k} \in \langle x \rangle$,
$\forall (k, k') \in \mathbb{Z}^2, \ \ x^k x^{k'} = x^{k+k'} \in \langle x \rangle$.
Enfin, H étant un sous-groupe de G, on a $x^k \in H$ pour tout entier $k \in \mathbb{Z}$, donc $\langle x \rangle \subseteq H$. □

Définition 0.8 *1. On dit que $\langle x \rangle$ est le sous-groupe de G **engendré** par x.*

*2. Le groupe G est dit **monogène** s'il existe un élément $x \in G$ tel que $G = \langle x \rangle$, un tel élément est alors appelé **générateur** de G. On dit aussi que le groupe G est **engendré** par x.*

*3. Un groupe **monogène fini** est appelé **groupe cyclique**.*

Exercice 9 — Montrer que même si le groupe G n'est pas commutatif, le sous-groupe $\langle x \rangle$ l'est. En particulier, tout groupe monogène est commutatif.

Exemple important $G = \mathbb{Z}$ et $n \in \mathbb{Z}$, alors $\langle n \rangle = \{kn \,|\, k \in \mathbb{Z}\}$.
Le sous-groupe $\langle n \rangle$ de $\mathbb{Z}$ est désigné par $n\mathbb{Z}$.
Remarquons que si $n = \pm 1$, on a $n\mathbb{Z} = \mathbb{Z}$, ce qui signifie que $\mathbb{Z}$ est monogène, engendré par 1 ou -1.

0.3.2 Groupes quotients

Rappelons qu'une relation binaire $\mathcal{R}$ définie sur un ensemble E est une relation d'équivalence si elle possède les propriétés suivantes :

$$\begin{cases} \text{Réflexivité} & \forall x \in E, & x\mathcal{R}x. \\ \text{Symétrie} & \forall (x,y) \in E \times E, & x\mathcal{R}y \Longleftrightarrow y\mathcal{R}x. \\ \text{Transitivité} & \forall (x,y,z) \in E \times E \times E, & \begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Longrightarrow x\mathcal{R}z. \end{cases}$$

Soit G un groupe commutatif noté additivement, et soit H un sous-groupe de G.
La notion de groupe quotient intervient lorsqu'on ne veut pas distinguer entre deux éléments x et y de G si leur différence $x - y$ appartient à H.
Si par exemple on fait des calculs sur les heures, on dira que deux entiers x et y de $\mathbb{Z}$ désignent la même heure si leur différence $x - y$ est un multiple de 24, c'est-à-dire si $x - y$ appartient au sous-groupe $24\mathbb{Z}$.
La définition du groupe quotient, que l'on désigne par G/H, se fait en deux étapes.
I – On définit d'abord *l'ensemble* G/H.
II – On munit cet ensemble d'une structure de groupe commutatif, appelée structure de groupe quotient, induite par celles de G et H.

Construction de l'ensemble G/H

Théorème 0.11 *Soit G un groupe noté additivement, (non nécessairement commutatif), et soit H un sous-groupe de G.*

1. *La relation binaire définie sur G par*

$$x\mathcal{R}y \text{ si et seulement si } y - x \in H$$

est une relation d'équivalence sur G.
Si $x\mathcal{R}y$, on dit que x et y sont équivalents ***modulo*** *H.*

2. *Pour chaque $x \in G$, si $\overline{x}$ désigne la classe d'équivalence de x, alors*

$$\overline{x} = \{x + h \,|\, h \in H\}.$$

On en déduit que toutes les classes d'équivalence sont équipotentes à H.
On les appelle classes d'équivalence modulo H.

Preuve :

1. Réflexivité : $\forall x \in G,\ \ x - x = 0 \in H$, donc $x\mathcal{R}x$.
   – Symétrie : $(x\mathcal{R}y) \Longleftrightarrow (y - x \in H) \Longleftrightarrow \Big(-(y-x) = x - y \in H\Big) \Longleftrightarrow (y\mathcal{R}x)$.
   – Transitivité :

$$\left.\begin{array}{l} x\mathcal{R}y \\ y\mathcal{R}z \end{array}\right\} \Rightarrow \left\{\begin{array}{l} y - x \in H \\ z - y \in H \end{array}\right\} \Rightarrow ((z-y) + (y-x) = z - x \in H) \Rightarrow (x\mathcal{R}z).$$

2. Soit $x \in G$, il résulte de la définition que pour tout $y \in G$, on a les équivalences

$$(1) \qquad (y \in \overline{x}) \iff (x\mathcal{R}y) \iff (\exists h \in H,\ \ y = x + h).$$

On en déduit en particulier $\overline{0} = H$. Soit $x \in G$, l'application α_x de H dans $\overline{x}$, définie par $\alpha_x(h) = x + h \in \overline{x}$ pour tout $h \in H$, est une bijection de H sur $\overline{x}$ car

– α_x est injective d'après le théorème 0.6 (page 9).
– α_x est surjective d'après (1). □

Remarque *En notation multiplicative, la relation d'équivalence ci-dessus s'écrit*

$$x\mathcal{R}y \text{ si et seulement si } yx^{-1} \in H$$

et les conclusions du théorème 0.11 restent évidemment vraies.

On désigne par G/H **l'ensemble quotient** de G par la relation d'équivalence associée à H.
Les *éléments* de G/H sont les *classes d'équivalence* modulo H.

Définition de l'addition sur G/H

On suppose maintenant le groupe G commutatif.

Proposition 0.12 *Soit x_1, y_1, x_2 et y_2 des éléments de G. On a, dans G/H, l'implication suivante*

$$\left.\begin{array}{l}\overline{x}_1 = \overline{x}_2 \\ \overline{y}_1 = \overline{y}_2\end{array}\right\} \quad \Longrightarrow \quad (\overline{x_1 + y_1} = \overline{x_2 + y_2})\,.$$

Preuve :

$$\left.\begin{array}{l}x_1 - x_2 \in H \\ y_1 - y_2 \in H\end{array}\right\} \Rightarrow ((x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2) \in H) \Leftrightarrow (\overline{x_1 + y_1} = \overline{x_2 + y_2})\,.$$

□

Soit α et β deux éléments de G/H, c'est-à-dire deux classes d'équivalence modulo H.
On *choisit* un représentant $x \in G$ de α, c'est-à-dire un élément x tel que $\overline{x} = \alpha$, et un représentant $y \in G$ de β. On a donc $\alpha = \overline{x}$ et $\beta = \overline{y}$.
La proposition 0.12 ci-dessus permet de définir la *somme* de α et β en posant

$$\alpha + \beta = \overline{x + y}. \tag{2}$$

Proposition 0.13 *1. Muni de l'addition définie par (2), G/H est un groupe commutatif.*

2. L'application P de G sur G/H définie, pour chaque $x \in G$, par

$$P(x) = \overline{x}$$

est un morphisme de groupes dont le noyau est égal à H.

Preuve :

1. Avec les notations qui précèdent, si x et $y \in G$, il résulte de (2) que
   - $\overline{x} + \overline{y} = \overline{y} + \overline{x}$ car $x + y = y + x$.
   - $\overline{0} + \overline{x} = \overline{x}$, ce qui prouve que $\overline{0}$ est l'élément neutre, (rappelons que $\overline{0} = H$).
   - $\overline{x} + \overline{-x} = \overline{-x} + \overline{x} = \overline{x - x} = \overline{0}$, ce qui signifie que $-\overline{x} = \overline{-x}$.
2. Résulte de 1. □

Le groupe G/H est appelé **groupe quotient** du groupe G par le sous-groupe H.
Remarquons que rien n'est plus facile que d'additionner deux éléments α et β de G/H, on choisit un représentant x de α, un représentant y de β, et la somme $\alpha + \beta$ est la classe de $x + y$.
On peut résumer en disant que **la somme des classes est la classe de la somme**.

Exercice 10 — Pourquoi a-ton supposé le groupe G commutatif pour définir l'addition sur G/H ?

Exercice 11 — Montrer que le groupe quotient $\mathbb{Z}/2\mathbb{Z}$ ne possède que les deux éléments $\overline{0}$ et $\overline{1}$, dresser sa table d'addition.

0.4 Anneaux et corps

Définition 0.9 *Un **anneau** est la donnée d'un ensemble A muni de deux opérations, une addition et une multiplication, vérifiant*

1. *$(A,+)$ est un groupe commutatif, d'élément neutre noté 0.*
2. *La multiplication est associative et possède un élément neutre noté 1, appelé élément unité.*
3. *La multiplication est distributive par rapport à l'addition, c'est-à-dire*

$$\forall (x,y,z) \in A\times A\times A, \quad \left\{ \begin{array}{l} x(y+z) = xy+xz, \\ (y+z)x = yx+zx. \end{array} \right.$$

– *Si la multiplication est commutative, on dit que l'anneau A est commutatif.*
– *L'anneau A est dit **intègre** si*

$$\forall (x,y) \in A\times A, \quad \left. \begin{array}{l} x\neq 0 \\ y\neq 0 \end{array} \right\} \Longrightarrow (xy\neq 0)\,.$$

Remarque : La définition générale d'un anneau ne suppose pas l'existence d'un élément unité, mais dans ce cours, on supposera cette condition toujours vérifiée.

Proposition 0.14 *Dans un anneau intègre, on peut "simplifier", c'est-à-dire que si a, b et c sont des éléments de A, avec $c\neq 0$, on a l'implication*

$$(ca = cb) \quad \Longrightarrow \quad (a=b).$$

Preuve : $(ca=cb) \Longrightarrow c(a-b)=0$, l'anneau est intègre et $c\neq 0$, on en déduit $a-b=0$. □

Définition 0.10 *Soit A et B deux anneaux, une application $\boldsymbol{u}$ de A dans B est un **morphisme d'anneaux** si*

$$\forall (x,y) \in A\times A, \quad \left\{ \begin{array}{l} \boldsymbol{u}(x+y) = \boldsymbol{u}(x)+\boldsymbol{u}(y) \\ \boldsymbol{u}(xy) = \boldsymbol{u}(x)\boldsymbol{u}(y). \end{array} \right.$$

*Si de plus l'application $\boldsymbol{u}$ est bijective, on dit que $\boldsymbol{u}$ est un **isomorphisme d'anneaux**, on dit alors que les anneaux A et B sont **isomorphes**.*

Proposition 0.15 *Soit A et B deux anneaux. On munit l'ensemble produit $A\times B$ de l'addition et de la multiplication définies respectivement par*

$$\begin{array}{rcl} (x,y)+(x',y') & = & (x+x',y+y'), \\ (x,y)\times(x',y') & = & (xx',yy'). \end{array}$$

1. *Ces opérations font de $A\times B$ un anneau, appelé **l'anneau produit** de A et B.*
2. *Le projecteur $\Pi_A : (x,y)\mapsto x$ de $A\times B$ dans A, (resp. $\Pi_B : (x,y)\mapsto y$ de $A\times B$ dans B) est un morphisme d'anneaux.*

On désigne par A^* l'ensemble des éléments inversibles (pour la multiplication) **d'un anneau** A.

Proposition 0.16 *Soit A un anneau, A^* est un groupe multiplicatif.*

Preuve : D'une part, on a $1 \in A^*$. D'autre part, soit x et y deux éléments de A^*, alors $xy^{-1} \in A^*$ car $(xy^{-1})^{-1} = yx^{-1}$. (Cf. proposition 0.3 page 8.) □

L'anneau $\mathbb{Z}$

La notion de "multiple" (définition 0.7 page 11) définit une multiplication sur $\mathbb{Z}$, qui avec l'addition, en fait un anneau commutatif intègre.

On retiendra donc que la multiplication sur $\mathbb{Z}$ est définie à partir de l'addition.

Les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1, ce qui fait que $\mathbb{Z}^*$ est le groupe multiplicatif $\{1, -1\}$ à deux éléments.

Proposition 0.17 (Formule du binôme de Newton) *Soit A un anneau commutatif. Soit a et b deux éléments de A, et soit $n \geq 1$ un entier, on a*

$$(N) \qquad (a+b)^n = \sum_{k=0}^{n} \mathcal{C}_k^n \, a^k \, b^{n-k}.$$

Preuve : Pour $n = 1$, la formule (N) se réduit à $a + b = a + b$. Supposons-la vérifiée pour un entier $n \geq 1$ et montrons que cela implique qu'elle l'est pour l'entier $(n+1)$. La démonstration repose sur l'égalité $\mathcal{C}_k^{n+1} = \mathcal{C}_{k-1}^n + \mathcal{C}_k^n$.

$$\begin{aligned}
(a+b)^{n+1} = (a+b)(a+b)^n &= (a+b) \sum_{k=0}^{n} \mathcal{C}_k^n \, a^k \, b^{n-k} \\
&= \sum_{k=0}^{n} \mathcal{C}_k^n \, a^{k+1} \, b^{n-k} + \sum_{k=0}^{n} \mathcal{C}_k^n \, a^k \, b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \mathcal{C}_{k-1}^n \, a^k \, b^{n-k+1} + \sum_{k=0}^{n} \mathcal{C}_k^n \, a^k \, b^{n-k+1} \\
&= \sum_{k=1}^{n+1} a^k \, b^{n+1-k} \, (\mathcal{C}_{k-1}^n + \mathcal{C}_k^n) + b^{n+1} \\
&= \sum_{k=0}^{n+1} \mathcal{C}_k^{n+1} \, a^k \, b^{n+1-k}. \qquad \square
\end{aligned}$$

Définition 0.11 *Un **idéal** I d'un un anneau commutatif A est un sous-groupe de A vérifiant*

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

*A et $\{0\}$ sont des idéaux de A, ce sont les idéaux **triviaux** de A.*

*Un idéal non trivial de A est appelé idéal **propre** de A.*

> **Exercice 12** — Soit I un idéal d'un un anneau commutatif A. Montrer que $I = A$ si et seulement si $1 \in I$.

Définition 0.12 *Un **corps** $\mathbb{K}$ est un anneau dans lequel tout élément non nul admet un inverse pour la multiplication, ce qui équivaut à l'égalité $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.*

Définition 0.13 *Une partie $\mathbb{L}$ d'un corps $\mathbb{K}$ est un **sous-corps** de $\mathbb{K}$ si*

1. $1 \in \mathbb{L}$,
2. $\mathbb{L}$ *est un sous-groupe de* $\mathbb{K}$,

3. pour tout couple $(a,b) \in \mathbb{K}^* \times \mathbb{K}^*$,

$$((a,b) \in \mathbb{L} \times \mathbb{L}) \quad \Longrightarrow \quad \left(ab^{-1} \in \mathbb{L}\right).$$

Cette dernière propriété signifiant que $\mathbb{L} \setminus \{0\}$ *est un sous-groupe de* $\mathbb{K}^*$.

Exercice 13 — Montrer que tout sous-corps d'un corps est un corps.

Proposition 0.18 *Tout corps est intègre.*

Preuve : Soit $\mathbb{K}$ un corps et soit a et b deux éléments de $\mathbb{K}$. Si $a \neq 0$, on écrit

$$(ab = 0) \implies \left(a^{-1}(ab) = (a^{-1}a)b = b = 0\right). \qquad \square$$

Remarque L'anneau $\mathbb{Z}$ n'est pas un corps car ses seuls éléments inversibles sont 1 et -1.

0.5 Espaces vectoriels et algèbres

Définition 0.14 *Soit* $\mathbb{K}$ *un corps commutatif. Un* $\mathbb{K}$***-espace vectoriel*** E*, ou espace vectoriel sur* $\mathbb{K}$*, est un groupe additif commutatif muni d'une* multiplication par les scalaires (les éléments de $\mathbb{K}$)*, c'est-à-dire une application*

$$(a,x) \in \mathbb{K} \times E \quad \longrightarrow \quad ax \in E$$

vérifiant, pour tout $(a,b) \in \mathbb{K} \times \mathbb{K}$ *et* $(x,y) \in E \times E$

$$(EV) \qquad \begin{cases} 1x = x, \\ a(x+y) = ax + ay, \\ (a+b)x = ax + ay, \\ (ab)x = a(bx). \end{cases}$$

Une partie F *de* E *est un* ***sous-espace vectoriel*** *de* E *si* F *est un sous-groupe de* E *tel que*

$$\forall (a,x) \in \mathbb{K} \times E, \qquad (x \in F) \implies (ax \in F).$$

Exemple Soit $\mathbb{K}$ un corps commutatif et soit n un entier ≥ 2. Le produit cartésien

$$\mathbb{K}^n = \{(x_1, x_2, \ldots, x_n) \,|\, \forall i = 1, 2, \ldots, n,\ x_i \in \mathbb{K}\}$$

est un $\mathbb{K}$-espace vectoriel pour l'addition définie par

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

et la multiplication par les scalaires définie par

$$\forall \lambda \in \mathbb{K},\ \forall (x_1, x_2, \ldots, x_n) \in \mathbb{K}^n, \quad \lambda(x_1, x_2, \ldots, x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n).$$

L'énoncé qui suit va jouer un rôle important au chapitre 5.

Proposition 0.19 *Soit* $\mathbb{K}$ *un corps commutatif et soit* $\mathbb{L}$ *un sous-corps de* $\mathbb{K}$*. Alors* $\mathbb{K}$ *est un* $\mathbb{L}$*-espace vectoriel.*

Preuve : Les relations (EV) ci-dessus sont vérifiées pour tout $(a,b) \in \mathbb{L} \times \mathbb{L}$ et $(x,y) \in \mathbb{K} \times \mathbb{K}$.$\square$

Définition 0.15 *Soit $\mathbb{K}$ un corps commutatif et soit E et F deux $\mathbb{K}$-espaces vectoriels. Une application $\boldsymbol{u}$ de E dans F est un* ***morphisme de $\mathbb{K}$-espaces vectoriels*** *si*
– $\boldsymbol{u}$ *est un morphisme de groupes additifs.*
– $\forall (a,x) \in \mathbb{K} \times E, \quad \boldsymbol{u}(ax) = a\boldsymbol{u}(x)$.
Si de plus l'application $\boldsymbol{u}$ est bijective, on dit que $\boldsymbol{u}$ est un ***isomorphisme de $\mathbb{K}$-espaces vectoriels****, les $\mathbb{K}$-espaces vectoriels E et F sont alors dits* ***isomorphes****.*

Soit A une partie non vide d'un $\mathbb{K}$-espace vectoriel E. Une ***combinaison linéaire*** d'éléments de A est un élément $x \in E$ de la forme

$$x = \sum_{i=1}^{n} \lambda_i x_i,$$

où n est un entier positif quelconque et où, pour chaque indice $i = 1, 2, \ldots, n$, $\lambda_i \in \mathbb{K}$ et $x_i \in A$.
On désigne par $\mathrm{vect}(A)$ l'ensemble des combinaisons linéaires d'éléments de A.
Si $A = \emptyset$, on convient que $\mathrm{vect}(A) = \{0\}$.

Proposition 0.20 *L'ensemble* $\mathrm{vect}(A)$ *est un sous-espace vectoriel de E, et si F est un sous-espace vectoriel de E, on a l'implication*

$$(A \subseteq F) \Longrightarrow (\mathrm{vect}(A) \subseteq F).$$

En d'autres termes, $\mathrm{vect}(A)$ *est le plus petit sous-espace vectoriel de E contenant A.*

Définition 0.16 *Soit E un $\mathbb{K}$-espace vectoriel.*

1. *Une partie (ou famille) A de E est dite* ***génératrice*** *si* $\mathrm{vect}(A) = E$.
2. *Une partie (ou famille) A de E est dite* ***libre*** *si, pour toute combinaison linéaire $\sum_{i=1}^{n} \lambda_i x_i$ d'éléments de A, on a l'implication*

$$\left(\sum_{i=1}^{n} \lambda_i x_i = 0 \right) \Longrightarrow (\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0).$$

3. *Une base de E est une partie de E à la fois génératrice et libre.*
4. *L'espace vectoriel E est de* ***dimension finie*** *s'il existe dans E une partie génératrice (ou famille génératrice)* ***finie****.*

Théorème 0.21 *Tout $\mathbb{K}$-espace vectoriel E de dimension finie possède une base. Deux bases de E ont même nombre d'éléments. Ce nombre est appelé la* ***dimension*** *de E. (On convient de dire que si E est réduit à 0, il possède une base formée de 0 vecteurs, il est de dimension 0.)*

Théorème 0.22 *Soi E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$.*

1. *Toute partie génératrice de E possède au moins n éléments et contient une base de E.*
2. *Toute partie libre de E possède au plus n éléments et peut être prolongée en une une base de E.*

Théorème 0.23 *Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geq 1$.*
Une famille $B = \{b_1, b_2, \ldots, b_n\}$ est une base de E si et seulement si tout élément $x \in E$ s'écrit d'une façon unique comme combinaison linéaire des éléments de B

$$x = \sum_{i=1}^{n} \lambda_i b_i.$$

Exemple Le $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$ est de dimension n. Parmi toutes les bases de $\mathbb{K}^n$, la **base canonique** de $\mathbb{K}^n$ est particulièrement utile, elle est définie par

$$B = \{e_1, e_2, \ldots, e_n\} \text{ où, pour chaque } i = 1, \ldots, n, \quad e_i = \underbrace{(0, \ldots, 0, 1, 0, \ldots, 0)}_{1 \text{ en ième position}} \in \mathbb{K}^n.$$

Théorème 0.24 *Soit $n \geq 1$ un entier. Tout $\mathbb{K}$-espace vectoriel E de dimension n est isomorphe à l'espace vectoriel $\mathbb{K}^n$.*

Définition 0.17 *Soit $\mathbb{K}$ un corps commutatif. Une $\mathbb{K}$-**algèbre** $\mathcal{A}$ est un anneau commutatif qui est un $\mathbb{K}$-espace vectoriel vérifiant, pour tout $(a, b) \in \mathbb{K} \times \mathbb{K}$ et $(x, y) \in \mathcal{A} \times \mathcal{A}$,*

$$(ax)(by) = (ab)(xy).$$

Définition 0.18 *Soit $\mathbb{K}$ un corps commutatif et soit $\mathcal{A}$ et $\mathcal{B}$ deux $\mathbb{K}$-algèbres. Une application $\boldsymbol{u}$ de $\mathcal{A}$ dans $\mathcal{B}$ est un **morphisme de $\mathbb{K}$-algèbres** si*
– $\boldsymbol{u}$ est un morphisme d'anneaux.
– $\boldsymbol{u}$ est un morphisme d'espaces vectoriels.
*Si de plus l'application $\boldsymbol{u}$ est bijective, on dit que $\boldsymbol{u}$ est un **isomorphisme de $\mathbb{K}$-algèbres**, les $\mathbb{K}$-algèbres $\mathcal{A}$ et $\mathcal{B}$ sont alors dites **isomorphes**.*

0.6 Matrices

Dans cette section, on désigne par $\mathbb{K}$ un corps commutatif. Toutes les matrices considérées sont à coefficients dans $\mathbb{K}$.

Notation Soit M une matrice à m lignes et n colonnes. Si a_{ij} désigne le coefficient de M situé sur la i-ième ligne et la j-ième colonne, on pourra écrire $M = (a_{ij})_{1 \leq i \leq m,\, 1 \leq j \leq n}$, ou plus simplement $M = (a_{ij})$ s'il n'y a pas de confusion possibles quant à m et n.
Chaque colonne de M est identifiée à un vecteur de $\mathbb{K}^m$.
On rappelle les définitions et résultats suivants.

Définition 0.19 *Le rang d'une matrice M à m lignes et n colonnes est la dimension du sous-espace vectoriel de $\mathbb{K}^m$ engendré par les n colonnes de M.*

Définition 0.20 *Si $M = (a_{ij})_{1 \leq i \leq m,\, 1 \leq j \leq n}$ est une matrice à m lignes et n colonnes, la matrice transposée de M, notée ${}^tM$ est la matrice à n lignes et m colonnes définie par*

$${}^tM = (b_{ij})_{1 \leq i \leq n,\, 1 \leq j \leq m}, \quad \text{où, pour tout } (i, j), \quad b_{ij} = a_{ji}.$$

Proposition 0.25 *Soit M une matrice. Le rang de M est égal*
– au nombre maximum de colonnes de M linéairement indépendantes dans $\mathbb{K}^m$,
– au rang de la matrice ${}^tM$,
– au nombre maximum de lignes de M linéairement indépendantes dans $\mathbb{K}^n$.
– à la dimension de la plus grande matrice carrée inversible contenue dans M.

Proposition 0.26 *On ne modifie pas le rang d'une matrice M*
– en permutant deux lignes,
– en permutant deux colonnes,
– en multipliant tous les éléments d'une ligne ou d'une colonne par un scalaire non nul,
– en ajoutant à une ligne une combinaison linéaire des autres lignes,
– en ajoutant à une colonne une combinaison linéaire des autres colonnes.

0.7 L'anneau des polynômes $\mathcal{A}[X]$

Soit $\mathcal{A}$ un anneau commutatif, on rappelle qu'un polynôme P à une variable à coefficients dans l'anneau $\mathcal{A}$ est la donnée d'une suite $P = (a_0, a_1, \ldots, a_n, \ldots)$ d'éléments de $\mathcal{A}$, dont tous les termes sont nuls à partir d'un certain rang.
L'ensemble de ces polynômes est noté $\mathcal{A}[X]$ (on verra tout de suite ce qu'est X).

Opérations sur les polynômes et notations

Soit $P = (a_0, a_1, \ldots, a_n, \ldots)$ et $Q = (b_0, b_1, \ldots, b_n, \ldots)$ deux polynômes de $\mathcal{A}[X]$.
On définit la somme et le produit de P et Q respectivement par

$$P + Q = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots) \tag{1}$$

$$PQ = (c_0, c_1, \ldots, c_n, \ldots), \tag{2}$$

où pour chaque indice $i \geq 0$, $$c_i = \sum_{k=0}^{i} a_k b_{i-k}.$$

Un polynôme dont les termes a_i sont nuls pour tout $i \geq 1$ est appelé *polynôme constant*.
On identifie tout élément $a \in \mathcal{A}$ au polynôme constant $(a, 0, 0, \ldots)$, ce qui permet d'écrire

$$aP = (aa_0, aa_1, \ldots, aa_n, \ldots).$$

Il est clair que le polynôme $1 = (1, 0, 0, \ldots)$ est l'élément neutre de la multiplication et le polynôme $0 = (0, 0, 0, \ldots)$ celui de l'addition.

Définition 0.21 *Soit $P = (a_0, a_1, \ldots, a_n, \ldots) \in \mathcal{A}[X]$.*
- *Si tous les a_i sont nuls, on convient, pour rendre cohérente la proposition 0.28 ci-dessous, de poser $\deg(P) = -\infty$, sinon le degré $\deg(P)$ de P est le plus grand entier k tel que $a_k \neq 0$.*
- *Le coefficient a_0 est le **terme constant** de P, et si $\deg(P) = n \geq 0$, a_n est le **coefficient dominant** de P.*
- *Le polynôme P est dit **unitaire** si son coefficient dominant est égal à 1.*

Attention, les polynômes de degré 0 sont les polynômes constants **non nuls**, le polynôme constant nul est de degré $-\infty$.

Retour à l'écriture classique $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$.
Si on pose

$$X = (0, 1, 0, 0 \ldots),$$

il résulte de (2) qu'on a alors

$$\begin{array}{rcl} X^2 & = & (0, 0, 1, 0, 0 \ldots) \\ X^3 & = & (0, 0, 0, 1, 0 \ldots) \\ \ldots & = & \ldots \\ \forall n \geq 1,\ X^n & = & \underbrace{(0, \ldots, 0, 1, 0, 0 \ldots)}_{1 \text{ en } (n+1)\text{-ième position}} . \end{array}$$

Il en résulte que si le polynôme $P = (a_0, a_1, \ldots, a_n, \ldots)$ est de degré $n \geq 0$, on a $a_n \neq 0$ et

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n.$$

Il arrivera aussi que l'on écrive $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$. On démontrera les trois propositions qui suivent à titre d'exercice.

Proposition 0.27 *Les opérations définies ci-dessus font de $\mathcal{A}[X]$ un anneau commutatif. Si l'anneau $\mathcal{A}$ est intègre, il en est de même de $\mathcal{A}[X]$.*

Proposition 0.28 *Si l'anneau $\mathcal{A}$ est intègre, pour tous polynômes P et $Q \in \mathcal{A}[X]$, on a*

$$\deg(P+Q) \leq \max(\deg(P), \deg(Q)),$$

$$\textit{si } \deg(P) \neq \deg(Q), \quad \deg(P+Q) = \max(\deg(P), \deg(Q)),$$

$$\deg(PQ) = \deg(P) + \deg(Q),$$

avec la convention que si k est un entier ≥ 0 ou si $k = -\infty$, on a

$$-\infty \leq k \quad \textit{et} \quad k + (-\infty) = (-\infty) + k = -\infty.$$

Proposition 0.29 *Si $\mathbb{K}$ est un corps commutatif, l'anneau $\mathbb{K}[X]$ est une $\mathbb{K}$-**algèbre**. Les seuls éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls, qu'on identifie aux éléments non nuls de $\mathbb{K}$. En d'autres termes, $\mathbb{K}[X]^* = \mathbb{K}^*$.*

Chapitre 1

La division euclidienne dans l'anneau $\mathbb{Z}$ et ses conséquences

(Euclide vécut à Alexandrie au III^e siècle avant J.C.)

Dans tout ce qui suit, on dira qu'un entier n est **positif** si $n \geq 1$, et **positif ou nul** si $n \geq 0$.

1.1 La division euclidienne

Théorème 1.1 (Division euclidienne) *Soit a et b deux éléments de $\mathbb{Z}$, avec $b > 0$.*
Il existe un couple unique $(q, r) \in \mathbb{Z}^2$ vérifiant

$$\begin{cases} a = bq + r \\ 0 \leq r < b. \end{cases}$$

*On dit que q est le **quotient** et r le **reste** de la division euclidienne de a par b.*

Preuve :

- *Existence.* L'ensemble $A = \{a - bk \,|\, k \in \mathbb{Z}\} \cap \mathbb{N}$ n'est pas vide, en effet si $a \geq 0$, on prend $k = 0$, et si $a \leq -1$ il suffit de prendre $k = a$, de sorte que $a - bk = a(1 - b) \geq 0$.
  Il résulte alors de la propriété fondamentale de $\mathbb{N}$ (page 6) que A possède un plus petit élément r.
  Par définition de A, il existe $q \in \mathbb{Z}$ tel que $r = a - bq$.
  Supposons $r \geq b$, on écrit alors

$$0 \leq r - b = a - bq - b = a - b(q + 1) \in A,$$

  mais on a $0 \leq r - b < r$, ce qui contredit le fait que r est le plus petit élément de A.
- *Unicité.* Supposons $a = bq_1 + r_1 = bq_2 + r_2$, avec $0 \leq r_1 < b$ et $0 \leq r_2 < b$.
  Si $q_1 \neq q_2$, supposons $q_1 - q_2 \geq 1$ par exemple, on écrit

$$b \leq b(q_1 - q_2) = r_2 - r_1 \leq r_2,$$

  ce qui contredit l'hypothèse $r_2 < b$.
  On en déduit $q_1 = q_2$ et il s'en suit que $r_1 = r_2$. □

Exemples

- Division euclidienne de 17 par 5 : $17 = 5 \times 3 + 2$, $q = 3$ et $r = 2$.
- Division euclidienne de -17 par 5 : $-17 = 5 \times (-4) + 3$, $q = -4$ et $r = 3$.

On peut étendre la division euclidienne au cas où $b \neq 0$ est de signe quelconque.

Théorème 1.2 *Soit a et b deux éléments de $\mathbb{Z}$, avec $b \neq 0$, il existe un couple unique $(q, r) \in \mathbb{Z}^2$ vérifiant*

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \,. \end{cases}$$

Preuve : Si $b < 0$, on effectue la division euclidienne de a par $-b$ selon le théorème 1.1

$$a = (-b)q + r, \quad 0 \leq r < -b,$$

puis on remplace b par $-b$ et q par $-q$, le reste r est inchangé. □

Remarque importante Dans tous les cas, **le reste r est positif ou nul**.

Exemples
- Division euclidienne de 18 par -4 : $18 = 4 \times 4 + 2 = (-4) \times (-4) + 2$.
- Division euclidienne de -15 par -4 : $-15 = 4 \times (-4) + 1 = (-4) \times 4 + 1$.

1.2 Les sous-groupes de $\mathbb{Z}$

La première conséquence de la division euclidienne dans $\mathbb{Z}$ concerne la forme spécifique des sous-groupes de $\mathbb{Z}$.

Soit $n \in \mathbb{Z}$, on sait que l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. Nous allons démontrer la réciproque de ce résultat, réciproque qui aura des conséquences importantes par la suite.

Théorème 1.3 *Soit H un sous-groupe de $\mathbb{Z}$, il existe un entier unique $n \geq 0$ tel que*

$$H = n\mathbb{Z}.$$

Preuve : Si $H = \{0\}$, on écrit $H = 0\mathbb{Z}$.
Si $H \neq \{0\}$, on pose

$$A = \{x \in H \mid x \geq 1\} = H \cap \mathbb{N}^*.$$

Soit x un élément non nul de H, alors ou bien $x \geq 1$, ou bien $-x \geq 1$, donc $A \neq \emptyset$.
Soit $n \geq 1$ le plus petit élément de A, (propriété fondamentale de $\mathbb{N}$), montrons que $H = n\mathbb{Z}$.
Comme $n \in H$, il résulte du théorème 0.10 (page 11) que $n\mathbb{Z} \subseteq H$.
Réciproquement, soit $m \in H$, effectuons la division euclidienne de m par n

$$m = nq + r, \qquad 0 \leq r < n.$$

De $m \in H$ et $n \in H$, il résulte, H étant un sous-groupe de $\mathbb{Z}$, que $r = m - nq \in H$.
D'où $r = 0$, sinon r serait un élément de A strictement plus petit que n.
On a donc $m = nq \in n\mathbb{Z}$. D'où $H \subseteq n\mathbb{Z}$. On en déduit $H = n\mathbb{Z}$.
Unicité Si $n\mathbb{Z} = m\mathbb{Z}$, m est multiple de n, et n est multiple de m, d'où $m = \pm n$. □

Corollaire 1.4 *Les idéaux de $\mathbb{Z}$ sont les sous-groupes de $\mathbb{Z}$.*

Preuve : Tout idéal d'un anneau en est par définition un sous-groupe. Réciproquement, pour tout entier $n \geq 0$, il est clair que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. □

1.3 Diviseurs, nombres premiers

Définition 1.1 *Soit a et b deux entiers, avec $b \neq 0$.*

1. *Lorsque le reste de la division euclidienne de a par b est nul, on dit que a est* ***multiple*** *de b, que b est un* ***diviseur*** *de a ou que b* ***divise*** *a.*
2. *Lorsque $a \neq 0$, un diviseur b de a est un* ***diviseur propre*** *de a si $b \neq \pm 1$ et $b \neq \pm a$.*
3. *Un entier p est* ***premier****, ou est un* ***nombre premier****, si $p \geq 2$ et si p n'admet pas de diviseur propre.*

Remarques

1. **Le nombre 1 n'est pas premier**.
2. Remarquons que (b divise a) équivaut à (($-b$) divise a), on se ramènera donc le plus souvent au cas où $b > 0$.
3. Tout entier $b \neq 0$ divise 0 puisque $0 = b \times 0$.

Proposition 1.5 *Soit a, b et c dans $\mathbb{Z}$, alors*

$$\left.\begin{array}{l} c \text{ divise } a \\ c \text{ divise } b \end{array}\right\} \Longrightarrow \quad \left(\forall\,(m,n) \in \mathbb{Z}^2, \quad c \text{ divise } (am+bn)\right).$$

Preuve : Soit q_1 et q_2 deux entiers tels que $a = q_1 c$ et $b = q_2 c$, alors

$$am + bn = q_1 cm + q_2 cn = (q_1 m + q_2 n)c. \qquad \square$$

Soit un entier $a \geq 0$, **on désigne par $D(a)$ l'ensemble des diviseurs positifs de a.**
On voit facilement que

1. *Si $a > 0$, $D(a)$ est fini, son plus grand élément est a et son plus petit élément est 1.*
2. *$D(0) = \mathbb{N}^*$.*
3. *Si $b \in D(a)$, $D(b) \subseteq D(a)$.*

Dire qu'un entier $a \geq 2$ est premier équivaut donc à dire que $D(a) = \{1, a\}$.
L'énoncé suivant est un bel exemple de théorème d'existence, on en déduit en effet l'existence d'une infinité de nombres premiers. Notons que c'est encore une conséquence directe de la propriété fondamentale de $\mathbb{N}$ (théorème 0.1 page 6).

Théorème 1.6 *Soit un entier $a \geq 2$, le plus petit diviseur de a strictement supérieur à 1 est premier. Cela implique que tout entier $a \geq 2$ admet au moins un diviseur premier.*

Preuve : Désignons par $\widetilde{D}(a)$ l'ensemble des éléments de $D(a)$ strictement supérieurs à 1, comme $a > 1$, $a \in \widetilde{D}(a)$ donc $\widetilde{D}(a) \neq \emptyset$.
Soit p le plus petit élément de $\widetilde{D}(a)$. Si p n'est pas premier il possède un un diviseur propre q, on a donc $1 < q < p$ et $q \in \widetilde{D}(p) \subseteq \widetilde{D}(a)$, ce qui contredit le fait que p est le plus petit élément de $\widetilde{D}(a)$. $\square$

Corollaire 1.7 *L'ensemble des nombres premiers est infini.*

Preuve : Par l'absurde, supposons cet ensemble fini égal à $\{p_1, p_2, \ldots, p_q\}$.
L'entier $a = p_1 p_2 \ldots p_q + 1$ n'est divisible par aucun des p_i mais admet un diviseur premier d'après le théorème 1.6, d'où contradiction. $\square$

1.4 Plus grand commun diviseur ou pgcd

Soit a et b deux entiers **non tous deux nuls** (cf. remarque 1. ci-dessous), il est facile de vérifier que l'ensemble

$$H(a,b) = \{au + bv \,|\, (u,v) \in \mathbb{Z}^2\}$$

est un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$.
Il existe donc d'après le théorème 1.3 (page 22) un entier unique $d \geq 1$ tel que

$$H(a,b) = \{au + bv \,|\, (u,v) \in \mathbb{Z}^2\} = d\,\mathbb{Z}. \tag{1}$$

Cet entier d est **appelé le plus grand commun diviseur** ou **pgcd** de a et b.

Étant donné un entier $k \in \mathbb{Z}$, on a donc l'équivalence suivante

$$\boxed{(\exists (u,v) \in \mathbb{Z}^2,\ k = au + bv) \iff (k \textit{ est un } \textbf{\textit{multiple}} \textit{ du } \text{pgcd} \textit{ de } a \textit{ et } b).}$$

Les notations usuelles pour le pgcd sont $\text{pgcd}\,(a,b)$ ou $(a \wedge b)$ ou $(a \vee b)$, ou encore (a,b) lorsqu'il n'y a pas de confusion possible. Nous adopterons la notation $\text{pgcd}\,(a,b)$.

Remarques

1. Si $a = b = 0$, le sous-groupe $H(a,b)$ est réduit à $\{0\}$. Certain manuels conviennent donc de dire que $\text{pgcd}\,(0,0) = 0$, avec la convention que 0 divise 0. Or tout entier positif divise 0, il n'y a donc pas à proprement parler de *plus grand* diviseur de 0. Au contraire, 0 apparaît comme le *plus petit* diviseur ≥ 0 de lui-même. C'est pourquoi nous ne retiendrons pas cette convention, qui par ailleurs ne présente pas beaucoup d'intérêt.
2. Il résulte de la définition que si $a > 0$, on a $\text{pgcd}\,(a,0) = a$.
3. Il est clair que $H(a,b) = H(\pm a, \pm b)$, il en résulte que $\text{pgcd}\,(a,b) = \text{pgcd}\,(\pm a, \pm b)$.

On peut caractériser le pgcd de deux entiers de la façon suivante.

Théorème 1.8 (Propriété caractéristique du pgcd) *Soit a et b deux entiers non tous deux nuls. Un entier positif d est le* pgcd *de a et b si et seulement si les deux conditions suivantes sont satisfaites :*

1. *d est un diviseur commun de a et b,*
2. *tout diviseur commun de a et b divise d.*

Preuve : Soit d le pgcd de a et b, alors $H(a,b) = d\,\mathbb{Z}$.

1. Comme $a \in H(a,b)$ et $b \in H(a,b)$, d divise a et b.
2. Comme $d \in H(a,b)$, il existe deux entiers u et v de $\mathbb{Z}$ tels que $d = au + bv$, donc tout entier c divisant a et b divise d d'après la proposition 1.5 (page 23).

Réciproquement, soit d' un entier positif vérifiant les conditions 1. et 2., la condition 1. implique d'après ce qui précède que d' divise d, et la condition 2. implique que d divise d', d'où $d' = d$.□

On voit donc que $(\text{pgcd}\,(a,b) = d)$ équivaut à $(D(a) \cap D(b) = D(d))$, c'est-à-dire que d est le plus grand élément de $D(a) \cap D(b)$. Cela justifie l'appellation de plus grand commun diviseur de a et b.

Définition 1.2 *On dit que deux entiers a et b sont* ***premiers entre eux*** *si leur seul diviseur commun positif est* 1*, autrement dit si leur* pgcd *est égal à* 1.

Remarquons qu'il résulte de cette définition que l'entier 1 est premier avec tout autre entier.

Le théorème suivant, dû au mathématicien français **Étienne Bézout** (1730-1783), synthétise ce qui précède.

Théorème 1.9 (Bézout) *Soit a, et b deux entiers.*

1. *Soit $d \geq 1$ un* ***diviseur commun*** *de a et b, alors d est le* pgcd *de a et b si et seulement s'il existe deux entiers u et v tels que*

   (1) $$au + bv = d.$$

2. *Les entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que*

   (2) $$au + bv = 1.$$

   Cette relation est appelée identité de Bézout.

Preuve : Remarquons d'abord que les relations (1) et (2) impliquent chacune que a et b ne sont pas tous deux nuls.

1. Si $d = \text{pgcd}\,(a, b)$, l'existence de u et v vient de la définition de d. (Cf. démonstration du théorème 1.8 page 24).

   Réciproquement, si d divise a et b et vérifie (1), tout diviseur commun de a et b divise d d'après la proposition 1.5 (page 23), donc $d = \text{pgcd}\,(a, b)$ d'après le théorème 1.8.
2. Il en résulte que la condition (2) est nécessaire. Elle est suffisante car elle implique que tout diviseur commun $c > 0$ de a et b divise 1 donc $c = 1$, ce qui veut dire que $\text{pgcd}\,(a, b) = 1$.

Remarque Si $a \neq 0$ et $b \neq 0$, le couple (u, v) vérifiant (1) n'est pas unique. Par exemple si $a = 4$ et $b = 6$, on a $d = 2$ et on peut écrire

$$2 = (-1) \times 4 \ + \ 1 \times 6 = (-4) \times 4 \ + \ 3 \times 6 = 2 \times 4 \ + \ (-1) \times 6, \text{ etc.}$$

La proposition qui suit n'est autre que la "*règle de réduction d'une fraction*" apprise à l'école.

Proposition 1.10 *Soit a et b deux entiers, et soit $d \geq 1$ un diviseur commun de a et b. Si on écrit*

(1) $$a = da_1 \ \ \text{et} \ \ b = db_1,$$

alors $d = \text{pgcd}\,(a, b)$ si et seulement si $\text{pgcd}\,(a_1, b_1) = 1$.

Preuve : Soit u et v deux entiers, on a l'équivalence

$$(d = au + bv) \Longleftrightarrow (1 = a_1 u + b_1 v). \qquad \square$$

Proposition 1.11 *Soit p un nombre premier et soit $a \in \mathbb{Z}$. Alors ou bien p et a sont premiers entre eux, ou bien p divise a.*

Preuve : Soit $d = \text{pgcd}\,(a, p)$. Puisque d divise p et p est premier, d est égal à 1 ou à p.
– Si $d = 1$, p et a sont premiers entre eux.
– Si $d = p$, p divise a. $\square$

Exercice 14 — Avec les notations du théorème de Bézout, montrer que les entiers u et v sont premiers entre eux.

Exercice 15 — Existe-t-il des entiers premiers avec 0 ? Si oui, lesquels ?

Exercice 16 — Montrer que si $d = \text{pgcd}\,(a,b)$ et si le couple $(u_0, v_0) \in \mathbb{Z}^2$ vérifie $au_0 + bv_0 = d$, les autres couples (u,v) vérifiant $au + bv = d$ sont les couples (u_k, v_k) définis pour chaque $k \in \mathbb{Z}^*$ par

$$\begin{cases} u_k = u_0 + kb_1, \\ v_k = v_0 - ka_1 \end{cases}$$

où a_1 et b_1 sont définis par $a = da_1$ et $b = db_1$.

Exercice 17 — Résoudre dans $\mathbb{Z}^2$ l'équation $5x - 18y = 4$.

Exercice 18 — Résoudre dans $\mathbb{Z}^2$ l'équation $6x + 15y = 28$.

Exercice 19 — Soit a, b, c et d quatre entiers, démontrer les implications suivantes.

1. $\big(\text{pgcd}\,(a,b) = d\big) \Longleftrightarrow \big(\text{pgcd}\,(ac,bc) = dc\big)$.
2. $\begin{cases} \text{pgcd}\,(a,b) = 1 \\ \text{pgcd}\,(a,c) = 1 \end{cases} \Longrightarrow \big(\text{pgcd}\,(a,bc) = 1\big)$.
3. $(\text{pgcd}\,(a,b) = 1) \Longrightarrow (\forall m \geq 2,\ \forall n \geq 2, \quad \text{pgcd}\,(a^m, b^n) = 1)$.
4. $\big(\text{pgcd}\,(a,b) = 1\big) \Longrightarrow \big(\text{pgcd}\,((a+b), ab) = 1\big)$.
5. $(\text{pgcd}\,(a,b) = d) \Longrightarrow (\forall n \geq 2, \quad \text{pgcd}\,(a^n, b^n) = d^n)$.

La proposition qui suit va nous permettre de construire un algorithme de calcul du pgcd de deux entiers, appelé algorithme d'Euclide.

Proposition 1.12 *Soit a et b deux entiers, avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b, on a*

$$\text{pgcd}\,(a,b) = \text{pgcd}\,(b,r).$$

Preuve : Si $a = bq + r$, (la double inégalité $0 \leq r < b$ ne nous servira pas ici), les diviseurs communs de a et b sont les diviseurs communs de b et r. □

1.5 L'algorithme d'Euclide

Cet algorithme a été établi et baptisé ainsi par Étienne Bézout, il est basé sur la proposition 1.12 et permet de calculer le pgcd de deux entiers a et b en effectuant un nombre fini de divisions euclidiennes.

Soit a et b deux entiers positifs, on pose $r_0 = a$ et $r_1 = b$, et tant que $r_i > 0$ on effectue les divisions euclidiennes successives suivantes.

$$(DE) \qquad \begin{cases} r_0 = r_1 q_1 + r_2, & \text{où} & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3, & \text{où} & 0 \leq r_3 < r_2 \\ \qquad \ldots & \ldots & \\ r_{k-2} = r_{k-1} q_{k-1} + r_k, & \text{où} & 0 \leq r_k < r_{k-1} \\ r_{k-1} = r_k q_k + r_{k+1}, & \text{où} & 0 \leq r_{k+1} < r_k \end{cases}$$

Il résulte de la proposition 1.12 que pour chaque $k \geq 0$, on a $\text{pgcd}\,(a,b) = \text{pgcd}\,(r_k, r_{k+1})$.
La suite des restes $(r_1, r_2, r_3, \ldots)$ étant une suite strictement décroissante d'entiers positifs, on obtient nécessairement un reste nul au bout d'un nombre fini de divisions.

Soit r_n le dernier reste non nul. On a $r_{n+1} = 0$, ce qui signifie que

$$\text{pgcd}\,(a,b) = \text{pgcd}\,(r_n, r_{n+1}) = \text{pgcd}\,(r_n, 0) = r_n.$$

D'où **l'algorithme d'Euclide** : On effectue les divisions euclidiennes successives décrites ci-dessus jusqu'à obtenir un reste nul, **le pgcd de a et b est le dernier reste non nul.**
L'algorithme d'Euclide peut être décrit formellement comme suit.

Algorithme d'Euclide

Entrées *: entiers a et b positifs.* ***Sortie*** : $\text{pgcd}\,(a,b)$.

Règle :

$$\begin{cases} \textit{si } v > 0, & (u,v) & \longrightarrow & (v, u - [u \textit{ div } v]v), \\ \textit{si } v = 0, & (u,v) & \longrightarrow & u. \end{cases}$$

Algorithme d'Euclide étendu

L'algorithme d'Euclide **étendu** permet de déterminer $d = \text{pgcd}\,(a, b)$ ainsi que deux entiers u et v vérifiant

$$d = au + bv.$$

Reprenons la suite (DE) des divisions euclidiennes et à chaque étape $k \geq 0$, calculons deux entiers u_k et v_k tels que

$$r_k = au_k + bv_k.$$

Un coup d'œil à (DE) montre que $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ et $v_1 = 1$.
De la relation $(r_{k-1} = r_k q_k + r_{k+1})$, qu'on écrit

$$r_{k+1} = r_{k-1} - r_k q_k,$$

on déduit que pour $k \geq 1$, on a $\begin{cases} u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k. \end{cases}$

Si $d = r_n$ est le dernier reste non nul, on a $u = u_n$ et $v = v_n$.
D'où **l'algorithme d'Euclide étendu** :
Soit deux entiers positifs a et b. Pour déterminer $d = \text{pgcd}\,(a, b)$, ainsi que deux entiers u et v tels que $d = au + bv$,

on écrit $\begin{cases} r_0 = a, \\ u_0 = 1, \\ v_0 = 0, \end{cases} \quad \begin{cases} r_1 = b, \\ u_1 = 0, \\ v_1 = 1, \end{cases} \quad \text{et} \quad \forall k \geq 1, \quad \begin{cases} r_{k+1} = r_{k-1} - r_k q_k, \\ u_{k+1} = u_{k-1} - u_k q_k, \\ v_{k+1} = v_{k-1} - v_k q_k, \end{cases}$

jusqu'à obtenir un reste nul.

Si r_n est le dernier reste non nul, on a $\begin{cases} d = r_n, \\ u = u_n, \\ v = v_n. \end{cases}$

Cela se formalise comme suit.
Entrées *: entiers a et b positifs.* ***Sortie*** *: entiers d, u, v, avec $d = \text{pgcd}\,(a, b) = au + bv$.*

Règle *:* $(a, b) \longrightarrow (b, 0, 1, a, 1, 0)$, *puis*

$$\begin{cases} \textit{si } t > 0, & (t, x, y, d, u, v) \longrightarrow (d - qt, u - qx, v - qy, t, x, y), \quad \textit{avec } q = d \text{ div } t, \\ \textit{si } t = 0, & (t, x, y, d, u, v) \longrightarrow (d, u, v). \end{cases}$$

1.6 Le lemme de Gauss

Parmi les corollaires les plus importants du théorème de Bézout figure le résultat suivant, connu sous le nom de lemme de Gauss.

Théorème 1.13 (Lemme Gauss) *(Carl Friedrich Gauss, 1777-1855) Soit a, b et c trois entiers. Si a divise le produit bc et si a est premier avec b, a divise c.*

Preuve : Soit $k \in \mathbb{Z}$ tel que $bc = ka$, et soit $(u, v) \in \mathbb{Z}^2$ tel que $1 = au + bv$. Multipliant les deux membres de cette égalité par c, on obtient $c = cau + cbv$, puis remplaçant $cb = bc$ par ka, il vient

$$c = cau + kav = acu + akv = a(cu + kv). \qquad \square$$

Attention Si a et b ne sont pas premiers entre eux, la conclusion du lemme de Gauss est **fausse** ; par exemple, 6 divise 3×4 mais ne divise ni 3 ni 4.

Corollaire 1.14 *Soit a, m et n trois entiers. Si m et n sont premiers entre eux et divisent a, leur produit mn divise a.*

Preuve : On écrit $a = km = \ell n$. Comme n divise km et est premier avec m, n divise k. □

Proposition 1.15 *Soit p un nombre premier, et soit k un entier compris entre 1 et $(p-1)$. Le coefficient binomial $\mathcal{C}_k^p$ est divisible par p.*

Preuve : On a $k!(p-k)\mathcal{C}_k^p = p!$, donc p divise $k!(p-k)\mathcal{C}_k^p$. Si k est compris entre 1 et $(p-1)$, l'entier $k!(p-k)$ est premier avec p, le résultat découle alors du lemme de Gauss. □

1.7 Plus petit commun multiple ou ppcm

Soit a et b deux entiers, on sait que l'intersection des sous-groupes $a\mathbb{Z}$ et $b\mathbb{Z}$ de $\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Il existe donc d'après le théorème 1.3 (page 22) un unique entier $m \geq 0$ tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}. \tag{1}$$

Cet entier m est **appelé le plus petit commun multiple** ou **ppcm** de a et b, on le note $m = \text{ppcm}\,(a,b)$. La caractérisation qui suit résulte directement de la définition.

Proposition 1.16 (Propriété caractéristique du ppcm) *Soit a et b deux entiers. Un entier $m \geq 0$ est le ppcm de a et b si et seulement si les deux conditions suivantes sont satisfaites :*

1. *m est un multiple commun de a et b,*
2. *tout multiple commun de a et b est un multiple de m.*

La proposition suivante ramène le calcul du ppcm à celui du pgcd.

Proposition 1.17 *Soit a et b deux entiers non tous deux nuls et soit d leur* pgcd *. Si on pose $a = da_1$, $b = db_1$, alors ppcm $(a,b) = d|a_1b_1|$. En particulier, on a l'égalité*

$$\text{pgcd}\,(a,b) \times \textit{ppcm}\,(a,b) = |ab|.$$

Preuve : Supposons pour simplifier que a et b sont non négatifs, et soit $m_1 = da_1b_1$. Les entiers a_1 et b_1 sont premiers entre eux d'après la proposition 1.10 (page 25).
Soit M un multiple commun de $a = da_1$ et $b = db_1$. Si on pose $M = dM_1$, alors M_1 est un multiple commun de a_1 et b_1, donc, d'après le corollaire 1.14 ci-dessus du lemme de Gauss, un multiple du produit a_1b_1. Il en résulte que $M = dM_1$ est un multiple de $m_1 = da_1b_1$. Il est clair d'autre part que m_1 est lui-même un multiple commun de a et b. On a donc prouvé, d'après la proposition 1.16, que $m_1 = \text{ppcm}\,(a,b)$. Il est clair enfin que $dm_1 = da_1db_1 = ab$. □

1.8 Décomposition d'un entier en facteurs premiers

Proposition 1.18 *Soit p un nombre premier. Si p divise un produit $q_1q_2\ldots q_n$ de n entiers, il existe au moins un indice $i \in \{1,2,\ldots,n\}$ tel que p divise q_i.*

Preuve : Par récurrence. Supposons $k = 2$ et p divise q_1q_2.
Ou bien p divise q_2 ou bien p est premier avec q_2 donc divise q_1 d'après le lemme de Gauss.
Supposons le résultat établi pour $n-1$, si p divise $q_1q_2\ldots q_n$, alors ou bien p divise q_n ou bien p est premier avec q_n donc divise $q_1q_2\ldots q_{n-1}$ d'après le lemme de Gauss, le résultat découle alors de l'hypothèse de récurrence. □

Corollaire 1.19 *Soit p un nombre premier. Si p divise un produit $p_1 p_2 \dots p_n$ de n nombres premiers, il existe un indice $i \in \{1, 2, \dots, n\}$ tel que $p = p_i$.*

Le théorème 1.6 (page 23) et le corollaire 1.19 ci-dessus vont permettre de démontrer l'important résultat suivant, appelé "Théorème fondamental de l'arithmétique".

Théorème 1.20 ***Théorème fondamental de l'arithmétique*** *Tout entier $a > 1$ s'écrit de façon unique*

(D) $$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

où $$\begin{cases} \text{les entiers } p_i \text{ sont premiers et vérifient } p_1 < p_2 < \dots < p_n, \\ \text{les entiers } \alpha_i \text{ sont positifs.} \end{cases}$$

Preuve :

1. *Existence.* Soit p_1 le plus petit diviseur premier de a (théorème 1.6 page 23).
   L'ensemble des entiers positifs α tels que (p_1^α divise a) est fini, soit α_1 son plus grand élément, alors α_1 est l'unique entier positif tel que
   $$(p_1^{\alpha_1} \text{ divise a }) \quad \text{et} \quad (p_1^{\alpha_1+1} \text{ ne divise pas a}),$$
   on écrit $a = p_1^{\alpha_1} a_1$.
   Si $a_1 = 1$, c'est terminé. Si $a_1 > 1$, on recommence.
   Soit p_2 le plus petit diviseur premier de a_1, et $\alpha_2 \geq 1$ le plus grand entier tel que $p_2^{\alpha_2}$ divise a_1. On pose $a = p_1^{\alpha_1} p_2^{\alpha_2} a_2$, et on remarque que $p_2 > p_1$ et que $a > a_1 > a_2 \geq 1$.
   On recommence l'opération jusqu'à obtenir un quotient $a_n = 1$, ce qui arrive au bout d'un nombre fini d'opérations puisque
   $$a > a_1 > a_2 > \dots > a_k > \dots \geq 1.$$

2. *Unicité.* Supposons
   (1) $$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} = {p'_1}^{\beta_1} {p'_2}^{\beta_2} \dots {p'_m}^{\beta_m},$$
   où les p_i et les p'_i sont premiers et vérifient
   $$p_1 < p_2 < \dots < p_n \quad \text{et} \quad p'_1 < p'_2 < \dots < p'_m,$$
   et où les α_i et les β_i sont des entiers ≥ 1. Il faut montrer que
   (a) $m = n$,
   (b) $\forall i = 1, 2, \dots, n, \;\; p_i = p'_i$,
   (c) $\forall i = 1, 2, \dots, n, \;\; \alpha_i = \beta_i$.

   (a) D'après le corollaire 1.19 (page 29), chaque p_i est égal à l'un des p'_i et chaque p'_i est égal à l'un des p_i. La famille des p_i coïncide donc avec celle des p'_i, d'où $m = n$.

   (b) Comme de plus les p_i et les p'_i sont rangés par ordre croissant, on a $p_i = p'_i$ pour chaque $i = 1, 2, \dots, n$.

   (c) Supposons qu'il existe un indice i tel que $\alpha_i \neq \beta_i$, par exemple $\alpha_i < \beta_i$. En divisant les deux membres de (1) par $p_i^{\alpha_i}$, on en déduit que p_i divise un produit de nombres premiers tous différents de lui-même, ce qui est impossible d'après le corollaire 1.19.□

L'égalité (D) constitue la *décomposition de l'entier a en facteurs premiers*. Si le théorème précédent en démontre l'existence pour tout entier a, la décomposition effective d'un "grand" entier (de plusieurs centaines de chiffres) en facteurs premiers est jusqu'à ce jour, malgré les moyens informatiques dont on dispose, un processus très lent. En amont de ce problème figure déjà celui de savoir si un entier donné est premier ou non. Des tests probabilistes de primalité et de non primalité des grand entiers existent mais sont d'autant plus longs à aboutir qu'on leur demande une fiabilité plus grande.

Chapitre 2

Groupes finis

Dans toute la suite du cours, on désigne par $\#E$ le nombre des éléments d'un ensemble fini E. Si G est un groupe fini, on rappelle que l'entier $\#G$ est appelé **ordre** de G.

2.1 Les groupes quotients $\mathbb{Z}/n\mathbb{Z}$

Définition 2.1 *Soit n un entier positif. On dit que deux entiers a et b sont **congrus modulo** n si leur différence $(b-a)$ est multiple de n, c'est à dire si $(b-a) \in n\mathbb{Z}$. Cette relation est notée*

$$a \equiv b \pmod{n}.$$

La notion de congruence modulo n a été introduite par Gauss.

Proposition 2.1 *Soit n un entier positif. La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. Soit $a \in \mathbb{Z}$, la classe d'équivalence $\overline{a}$ de a modulo n est appelée **classe de** a **modulo** n, et on a*

$$\overline{a} = \{a + nk \,|\, k \in \mathbb{Z}\}.$$

Preuve : On retrouve la relation d'équivalence associée au sous-groupe $n\mathbb{Z}$. (Cf. page 12). □

Proposition 2.2 *Soit n un entier positif et soit $a \in \mathbb{Z}$. Le reste r de la division euclidienne de a par n est le seul entier vérifiant*

$$\begin{cases} r \equiv a \pmod{n}, \\ 0 \leq r < n. \end{cases} \tag{1}$$

Il en résulte que deux entiers a et b sont congrus modulo n si et seulement si le reste de la division euclidienne de a par n est égal au reste de la division euclidienne de b par n.

Preuve : Il est clair que $r \equiv a \pmod{n}$. Soit r_1 un entier vérifiant (1), alors $r - r_1$ est multiple de n et $|r - r_1| < n$, ce qui montre que $r - r_1 = 0$. □

Rappelons que l'addition du groupe quotient $\mathbb{Z}/n\mathbb{Z}$ est définie, si a et b sont deux entiers, par

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Proposition 2.3 *Le groupe $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n, plus précisément, on a*

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

Preuve : Soit $a \in \mathbb{Z}$, il résulte de la proposition 2.2 que $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{(n-1)}\,\}$ et que les classes $\overline{0}$, $\overline{1}, \ldots, \overline{(n-1)}$ sont toutes distinctes. On remarque que $\overline{n} = \overline{0}$, $\overline{(n+1)} = \overline{1}$, etc. □

Proposition 2.4 *Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique (additif), engendré par $\overline{1}$.*

Preuve : Conséquence directe de la définition de l'addition de $\mathbb{Z}/n\mathbb{Z}$. □

2.2 Généralités sur les groupes finis

Du théorème 0.11 (page 12), on déduit une propriété essentielle des groupes finis :

Théorème 2.5 (Lagrange) *Dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe.*

Preuve : Soit G un groupe fini et H un sous-groupe de G. On sait d'après le théorème 0.11 (page 12) que les classes d'équivalence modulo H possèdent toutes le même nombre d'éléments que H et constituent une partition de G. L'ensemble G étant fini, il n'y a qu'un nombre fini m de classes, on en déduit que l'ordre de G est égal à m fois l'ordre de H. □

L'étude d'un groupe comporte l'étude de tous ses sous-groupes, le théorème précédent permet de cerner la recherche des sous-groupes, un groupe d'ordre 8 par exemple ne possédera pas de sous-groupe d'ordre 3, 5 ou 7. De même qu'un groupe d'ordre premier ne possédera que ses deux sous-groupes triviaux.

Définition 2.2 *Soit G un groupe fini et soit $x \in G$. On appelle* ***ordre de*** *x l'ordre du sous-groupe $\langle x\rangle = \{x^k \mid k \in \mathbb{Z}\}$ de G engendré par x.*

Notons que le seul élément de G d'ordre 1 est l'unité 1.

Théorème 2.6 *Soit G un groupe fini, soit $x \in G$ et soit m l'ordre de x. Alors*

1. *m divise l'ordre de G.*
2. *m est le plus petit entier positif tel que $x^m = 1$.*
3. *Les éléments $1, x, x^2, \ldots, x^{m-1}$ sont tous distincts dans G.*
4. *$\langle x\rangle = \{1, x, x^2, \ldots, x^{m-1}\}$.*

Preuve :

1. Résulte du théorème de Lagrange.
2. Si $m = 1$, c'est évident. On suppose $m \geq 2$, la démonstration se fait en deux étapes.
   (a) On montre qu'il existe au moins un entier ℓ, $1 \leq \ell \leq m$ tel que $x^\ell = 1$.

   Soit $$A = \{x, x^2, \ldots, x^m, x^{m+1}\} \subseteq \langle x\rangle,$$

   comme l'ordre de $\langle x\rangle$ est égal à m, il existe au moins deux éléments égaux dans A,

   $$\exists k,\ \exists \ell,\ \ 1 \leq k \leq m,\ \ 1 \leq k + \ell \leq m + 1 \text{ vérifiant } x^k = x^{k+\ell},$$

   on en déduit $$1 \leq \ell \leq m \quad \text{et} \quad x^\ell = 1.$$

   (b) Soit n le plus petit entier positif tel que $x^n = 1$, il résulte de (a) que $(n \leq \ell \leq m)$. Montrons que $\langle x\rangle \subseteq \{1, x, x^2, \ldots, x^{n-1}\}$. Soit en effet $k \in \mathbb{Z}$, la division euclidienne de k par n s'écrit $k = nq + r$, $\quad 0 \leq r \leq n - 1$, ce qui donne

   $$x^k = x^{nq}x^r = (x^n)^q x^r = 1^q x^r = x^r \in \{1, x, x^2, \ldots, x^{n-1}\},$$

   il en résulte $m = \#\langle x\rangle \leq \#\{1, x, x^2, \ldots, x^{n-1}\} \leq n$, c'est-à-dire , en vertu de (a),

   $$m = \#\langle x\rangle = \#\{1, x, x^2, \ldots, x^{m-1}\} = n.$$

   Cela démontre 2. et 4.
3. Résulte de l'égalité $m = \#\{1, x, x^2, \ldots, x^{m-1}\}$. □

Il découle du théorème 2.6 un chapelet de corollaires tous aussi importants les uns que les autres.

Corollaire 2.7 *Soit G un groupe fini d'ordre n, alors on a $x^n = 1$ pour tout $x \in G$.*

Preuve : Soit m l'ordre de x, et soit $k \geq 1$ l'entier tel que $n = mk$, alors

$$x^n = x^{mk} = (x^m)^k = 1^k = 1. \qquad \square$$

Corollaire 2.8 *Tout groupe fini G d'ordre premier p est cyclique et engendré par l'un quelconque de ses éléments distincts de 1.*

Preuve : Soit $x \in G$, $x \neq 1$. Comme $x \in \langle x \rangle$ et $1 \in \langle x \rangle$, l'ordre m de x est ≥ 2 et divise p, d'où $m = p$, c'est-à-dire $\langle x \rangle = G$. $\square$

Corollaire 2.9 *Soit G un groupe d'ordre n. Pour chaque entier positif k, soit $\alpha_G(k)$ le nombre des éléments d'ordre k de G, alors on a*

$$n = \sum_{d/n} \alpha_G(d).$$

Preuve : On sait que si k ne divise pas n, on a $\alpha_G(k) = 0$. Si d divise n, soit $\Omega_G(d)$ l'ensemble des éléments d'ordre d de G, alors $\alpha_G(d) = \#\Omega_G(d)$ et tout élément de G appartient à un $\Omega_G(d)$ et un seul. $\square$

Le théorème suivant est très utile pour déterminer l'ordre des éléments d'un groupe fini.

Théorème 2.10 *Soit G un groupe fini, soit $x \in G$ et soit m l'ordre de x.*

1. *Pour tout entier positif q, on a l'équivalence*

$$\boxed{(x^q = 1) \iff (m \text{ divise } q).}$$

2. *Pour tout entier positif k,*

$$\boxed{x^k \text{ est d'ordre } m/d, \text{ où } d = \operatorname{pgcd}(m, k).}$$

Preuve :

1. Si m divise q, posons $q = mq'$, alors

$$x^q = x^{mq'} = (x^m)^{q'} = 1^{q'} = 1.$$

Réciproquement, si $x^q = 1$, soit $q = mq' + r$, $0 \leq r < m$, la division euclidienne de q par m. Alors

$$1 = x^q = x^{mq'+r} = x^{mq'}x^r = x^r.$$

On déduit du point 2. du théorème 2.6 (page 32) que $r = 0$.

2. On écrit $m = dm'$ et $k = dk'$, de sorte que $\operatorname{pgcd}(m', k') = 1$.

Soit α l'ordre de x^k, de l'égalité $(x^k)^\alpha = x^{k\alpha} = 1$, on déduit que m divise $k\alpha$, c'est-à-dire dm' divise $dk'\alpha$, d'où m' divise $k'\alpha$ et m' divise α d'après le lemme de Gauss.

Réciproquement, $(x^k)^{m'} = x^{km'} = x^{dk'm'} = x^{mk'} = (x^m)^{k'} = 1$, donc α divise m' et finalement $\alpha = m'$. $\square$

Attention Bien comprendre le point 1. du théorème 2.10 : si $x \in G$ et si q est un entier > 1,

l'égalité $(x^q = 1)$ **n'implique pas que** x **est d'ordre** q
mais seulement que **l'ordre de** x **divise** q.

En particulier, soit G un groupe d'ordre n ; d'après le corollaire 2.7 ci-dessus, *tous les éléments* de G vérifient $x^n = 1$, mais ces éléments ne sont pas tous *d'ordre* n. Mieux, si G n'est pas cyclique, *aucun* de ses éléments n'est d'ordre n.
L'important corollaire suivant résulte du point 2. du théorème 2.10.

Corollaire 2.11 *Soit G un groupe fini, soit $x \in G$ et soit k un entier positif.*
L'ordre de x^k est égal à l'ordre de x si et seulement si k est premier avec l'ordre de x.

Exercice 20 — Soit G un groupe fini *commutatif* et soit x et y deux éléments de G, d'ordres respectifs p et q. Montrer que

1. Si p et q sont premiers entre eux, le produit $z = xy$ est d'ordre pq et le sous-groupe de G engendré par z contient x et y.
2. Il existe un élément $t \in G$ dont l'ordre est égal au ppcm de p et q.

2.3 Groupes cycliques et indicatrice d'Euler

On rappelle qu'un groupe G est cyclique s'il est fini et s'il existe un élément $g \in G$, appelé générateur de G, tel que $G = \langle g \rangle$, ce qui équivaut à l'égalité

$$(\text{ordre de } g) = (\text{ordre de } G).$$

On rappelle également que *tout groupe cyclique est commutatif.*
L'énoncé suivant est une conséquence directe du théorème 2.6 (page 32).

Théorème 2.12 *Soit G un groupe cyclique d'ordre n, et soit $g \in G$ un générateur de G.*

1. *g est d'ordre n.*
2. *Tous les éléments g^k sont distincts pour $k = 0, 1, \ldots, n-1$.*
3. *$G = \{g^k \mid k \geq 0\} = \{1, g, \ldots, g^{n-1}\}$.*
4. *En notation additive, cela s'écrit $G = \{kg \mid k \geq 0\} = \{0, g, \ldots, (n-1)g\}$.*

Corollaire 2.13 *Deux groupes cycliques de même ordre sont isomorphes.*

Preuve : Soit G_1 et G_2 deux groupes cycliques d'ordre n, de générateurs respectifs g_1 et g_2. L'application u de G_1 sur G_2 définie par

$$\forall k \geq 0, \quad \begin{cases} u(g_1^k) = g_2^k & \text{si } G_1 \text{ et } G_2 \text{ sont multiplicatifs,} \\ u(kg_1) = kg_2 & \text{si } G_1 \text{ et } G_2 \text{ sont additifs,} \\ u(kg_1) = g_2^k & \text{si } G_1 \text{ est additif et } G_2 \text{ multiplicatif,} \end{cases}$$

est un isomorphisme de G_1 sur G_2. □

Corollaire 2.14 *Tout groupe cyclique d'ordre $n \geq 1$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : On a vu, proposition 2.4 page 31, que le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n. □

Exercice 21 — Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ sont commutatifs, d'ordre 4, mais non isomorphes.

Définition 2.3 ***Indicatrice d'Euler*** *(Leonhard Euler, 1707-1783) Soit n un entier positif, l'indicatrice d'Euler de n, notée $\varphi(n)$, est définie comme étant égale au nombre des entiers k vérifiant*

$$(1) \qquad (1 \leq k \leq n) \ \text{ et } \ (\text{pgcd}\,(k,n) = 1).$$

Notons que pour tout entier positif n, on a $\text{pgcd}\,(1,n) = 1$, ce qui fait que $\varphi(n) \geq 1$.

Exemples

1. Il est clair que $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$. Etc.
2. Si $n = 10$, les entiers vérifiant (1) sont 1, 3, 7 et 9, il y en a 4, donc $\varphi(10) = 4$. Remarquons que $\varphi(9) = 6$, la fonction φ n'est pas croissante.

Nous verrons plus loin (page 41), que l'indicatrice d'Euler $\varphi(n)$ se calcule à partir de la décomposition de l'entier n en facteurs premiers. La première étape est le résultat suivant.

Proposition 2.15 *Soit p un nombre premier. Pour tout entier positif n, on a*

$$\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1} = p^n\left(1 - \frac{1}{p}\right).$$

En particulier, $\varphi(p^n)$ est pair dès que $p > 2$.

Preuve : Parmi les p^n entiers k tels que $1 \leq k \leq p^n$, il y a p^{n-1} multiples de p, les autres sont premiers avec p d'après la proposition 1.11 (page 25). □

Théorème 2.16 *Un groupe cyclique G d'ordre n possède $\varphi(n)$ générateurs distincts. Plus précisément, si g est un générateur de G, les $\varphi(n)$ générateurs de G sont les éléments g^k, où $1 \leq k \leq n$ et $\text{pgcd}\,(n,k) = 1$.*

Preuve : Il résulte du théorème 2.12 (page 34) que tous les éléments g^k sont distincts pour $1 \leq k \leq n$, puis du corollaire 2.11 (page 34) que si $k \geq 1$, g^k est générateur de G si et seulement si $\text{pgcd}\,(k,n) = 1$. □

Transcrit en notation additive, le théorème précédent permet de déterminer les générateurs du groupe (additif) $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 2.17 (Générateurs de $\mathbb{Z}/n\mathbb{Z}$) *Les $\varphi(n)$ générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ sont les classe $\overline{k}$ modulo n, où $1 \leq k \leq n$ et $\text{pgcd}\,(k,n) = 1$.*

Preuve : Résulte du fait que $\overline{1}$ est générateur $\mathbb{Z}/n\mathbb{Z}$. □

Théorème 2.18 *Soit G un groupe cyclique d'ordre n. Pour chaque diviseur d de n, l'ensemble*

$$U_d = \{x \in G \,|\, x^d = 1\}$$

est un sous-groupe d'ordre d de G. C'est le seul sous-groupe d'ordre d de G. Ce sous-groupe est cyclique. Il en résulte que G possède exactement $\varphi(d)$ éléments d'ordre d, et que tout sous-groupe d'un groupe cyclique est cyclique.

Preuve : Le groupe G étant commutatif, U_d est un sous-groupe de G. Il résulte ensuite du corollaire 2.7 (page 33) que tout sous-groupe d'ordre d de G est contenu dans U_d.

Posons $n = dn'$ et soit g un générateur de G, on a l'équivalence, pour tout entier $k \geq 1$,

$$\left((g^k)^d = g^{kd} = 1\right) \iff (kd \text{ est multiple de } n = dn') \iff (k \text{ est multiple de } n').$$

Les éléments de U_d sont donc $g^{n'}$, $g^{2n'}, \ldots,$ $g^{dn'} = g^n = 1$.

Ces éléments sont tous distincts car $in' \leq n$ pour tout $i = 1, \ldots, d$.

Le sous-groupe U_d est donc cyclique d'ordre d, engendré par $g^{n'}$, il possède par conséquent $\varphi(d)$ générateurs qui sont les seuls éléments d'ordre d de U_d donc de G.

D'après le corollaire 2.11 (page 34), ces éléments sont les $g^{n'k}$, où k est premier avec d. □

Exercice 22 — Déterminer les éléments d'ordre 8 du groupe $\mathbb{Z}/32\,\mathbb{Z}$.

Exercice 23 — **Contrexemple** Soit G le groupe (additif) $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$.

1. Quel est l'ordre de G ?
2. Déterminer $U_3 = \{x \in G \,|\, 3x = 0\}$.
3. Déterminer l'ensemble des éléments d'ordre 3 de G. En déduire que les conclusions du théorème 2.18 ci-dessus ne s'appliquent pas à un groupe non cyclique, même s'il est commutatif.

Corollaire 2.19 *Pour chaque entier positif n, on a*

$$n = \sum_{d/n} \varphi(d). \tag{1}$$

Preuve : Résulte du théorème 2.18 appliqué au groupe $\mathbb{Z}/n\mathbb{Z}$, et du corollaire 2.9 (page 33).□

Le théorème suivant donne une **caractérisation** très pratique des groupes cycliques, dont nous ferons usage au chapitre 5.

Théorème 2.20 *Soit G un groupe d'ordre n. Pour chaque diviseur d de n, soit*

$$\begin{cases} U_d = \{x \in G \,|\, x^d = 1\}, \\ \alpha_G(d) \text{ le nombre d'éléments d'ordre } d \text{ de } G. \end{cases}$$

Les conditions suivantes sont équivalentes.

1. *Pour chaque diviseur d de n, $\#U_d \leq d$.*
2. *Pour chaque diviseur d de n, $\alpha_G(d) \leq \varphi(d)$.*
3. *Pour chaque diviseur d de n, $\alpha_G(d) = \varphi(d)$.*
4. *G est cyclique.*
5. *Pour chaque diviseur d de n, $\#U_d = d$.*

Preuve : Notons que si G n'est pas commutatif, U_d n'est pas nécessairement un sous-groupe.
$1 \Longrightarrow 2$. Si $\alpha_G(d) \geq 1$, il existe un élément $x \in G$ d'ordre d, donc $x \in U_d$, et il résulte du théorème 2.7 (page 33) que $\langle x \rangle \subseteq U_d$, d'où $\#\langle x \rangle = d \leq \#U_d$. Sous l'hypothèse 1., on en déduit $d = \#U_d$, donc $\langle x \rangle = U_d$.
Le sous-groupe $\langle x \rangle$ possède $\varphi(d)$ générateurs d'après le théorème 2.16 (page 35), et l'égalité $\langle x \rangle = U_d$ implique que ce sont les seuls éléments d'ordre d de G. On en déduit $\alpha_G(d) = \varphi(d)$. Autrement dit, ou bien $\alpha_G(d) = 0$ ou bien $\alpha_G(d) = \varphi(d)$, d'où $\alpha_G(d) \leq \varphi(d)$.
$2 \Longrightarrow 3$. Le corollaire 2.9 (page 33) et le corollaire 2.19 ci-dessus impliquent l'égalité

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

De cette égalité et de la condition 2., on déduit que pour tout diviseur d de n, on a

$$\alpha_G(d) = \varphi(d).$$

$3 \Longrightarrow 4$. Pour $d = n$, on déduit de 3. que $\alpha_G(n) = \varphi(n) \geq 1$, le groupe G possède donc un élément d'ordre n, il est cyclique.
$4 \Longrightarrow 5$. C'est le théorème 2.18 (page 35).
$5 \Longrightarrow 1$. Évident. □

Chapitre 3

Arithmétique des congruences

3.1 Les anneaux quotients $\mathbb{Z}/n\mathbb{Z}$

La proposition suivante permet de définir une multiplication sur l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$.

Proposition 3.1 *Soit a et b deux entiers, et soit n un entier positif, alors on a dans $\mathbb{Z}/n\mathbb{Z}$,*

$$\left.\begin{array}{l}\overline{a}=\overline{a'}\\ \overline{b}=\overline{b'}\end{array}\right\} \quad\Longrightarrow\quad \left(\overline{ab}=\overline{a'b'}\right)$$

Preuve : Il existe q_1 et q_2 dans $\mathbb{Z}$ tels que $a=a'+q_1n$ et $b=b'+q_2n$, ce qui donne

$$ab=a'b'+n(a'q_2+b'q_1+nq_1q_2).$$ □

Ceci justifie la définition suivante.

Définition 3.1 *Étant données deux classes α et $\beta\in\mathbb{Z}/n\mathbb{Z}$, on **définit la classe produit** $\alpha\beta\in\mathbb{Z}/n\mathbb{Z}$ comme suit.*

1. *On **choisit** un représentant $a\in\alpha$ et un représentant $b\in\beta$, c'est à dire deux entiers a et b vérifiant $\overline{a}=\alpha$ et $\overline{b}=\beta$.*
2. *On **pose** $\alpha\beta=\overline{ab}$.*

Proposition 3.2 *La multiplication définie ci-dessus fait du groupe quotient $\mathbb{Z}/n\mathbb{Z}$ un anneau commutatif d'élément neutre $\overline{0}$ et d'élément unité $\overline{1}$.*

Preuve : On sait que l'addition fait de $\mathbb{Z}/n\mathbb{Z}$ un groupe commutatif. On vérifie facilement que la multiplication définie ci-dessus est commutative, distributive par rapport à l'addition, et que la classe $\overline{1}$ en est l'élément neutre. □

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est appelé **anneau quotient** de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

Rappelons que $(\mathbb{Z}/n\mathbb{Z})^*$ désigne l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ inversibles pour la multiplication. On sait que $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif (proposition 0.16 page 14).

Théorème 3.3 *Soit n un entier positif, soit $q\in\mathbb{Z}$ et soit $\overline{q}$ la classe de q modulo n.*

1. *On a l'équivalence*
$$\left(\overline{q}\in(\mathbb{Z}/n\mathbb{Z})^*\right)\Longleftrightarrow\left(\operatorname{pgcd}(q,n)=1\right).$$
On dit alors que l'entier q est inversible modulo n.
2. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. On le désigne alors par $\mathbb{F}_n$.*

Preuve : Soit $\overline{q}$ un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, il existe $\ell \in \mathbb{Z}$ tel que $\overline{q}\,\overline{\ell} = \overline{1}$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $q\ell = 1 + nk$, ce qui implique $\text{pgcd}\,(q, n) = 1$.
Réciproquement, si $\text{pgcd}\,(q, n) = 1$, il existe d'après le théorème de Bézout deux entiers u et v vérifiant $qu + nv = 1$, d'où, modulo n, $\overline{q}\,\overline{u} + \overline{n}\,\overline{v} = \overline{1}$, mais $\overline{n} = \overline{0}$, d'où $\overline{q}\,\overline{u} = \overline{1}$, c'est-à-dire que $\overline{q}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.
Enfin, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si pour tout $q \in \{1, \ldots, n-1\}$, $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^*$, c'est-à-dire $\text{pgcd}\,(q, n) = 1$, ce qui signifie que n est premier. □

Important

1. La démonstration précédente montre que si q est inversible modulo n, son inverse peut être calculé à l'aide de l'algorithme d'Euclide étendu.
2. Les éléments inversibles de **l'anneau** $\mathbb{Z}/n\mathbb{Z}$ ne sont autres que les générateurs du **groupe** $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 3.4 *Soit n un entier positif, le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est d'ordre $\varphi(n)$, où φ désigne l'indicatrice d'Euler.*

Convention Soit $a \in \{1, 2, \ldots, n-1\}$ un entier premier avec n.
On dira que l'entier b est **l'inverse de** a **modulo** n si $ab \equiv 1 \pmod{n}$ et si $b \in \{1, 2, \ldots, n-1\}$.

Exercice 24 — Déterminer l'inverse de 5 modulo 12, de 8 modulo 27 et de 14 modulo 25.

Exercice 25 — Dresser la table de multiplication de l'anneau $\mathbb{Z}/4\mathbb{Z}$ et du corps $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.

3.2 Théorèmes de Fermat et d'Euler

Théorème 3.5 ***Petit théorème de Fermat*** *(Pierre de Fermat, 1601-1665) Étant donné un nombre premier p et un entier $a \in \mathbb{Z}$, on a*

$$a^p \equiv a \pmod{p}.$$

Preuve : Soit $a \in \mathbb{Z}$. On sait d'après la proposition 1.11 (page 25) qu'ou bien a est multiple de p ou bien a est premier avec p. Soit $\overline{a}$ la classe de a modulo p.
– Si a est multiple de p, a^p est aussi multiple de p, on a donc $a^p \equiv a \equiv 0 \pmod{p}$.
– Si $\text{pgcd}\,(a, p) = 1$, alors $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ d'après le théorème 3.3 (page 37).
Or $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $p-1$ donc $\overline{a}^{\,p-1} = \overline{1}$ d'après le corollaire 2.7 (page 33).
Ceci s'écrit $a^{p-1} \equiv 1 \pmod{p}$, il en résulte $a^p \equiv a \pmod{p}$. □

Théorème 3.6 (Euler) *Soit n un entier positif, et soit $a \in \mathbb{Z}$ un entier premier avec n, alors*

$$a^{\,\varphi(n)} \equiv 1 \pmod{n}.$$

Preuve : Soit $\overline{a}$ la classe de a modulo n. On a $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ et $(\mathbb{Z}/n\mathbb{Z})^*$ est d'ordre $\varphi(n)$, on applique le corollaire 2.7 (page 33). □

3.3 Systèmes de congruences. Théorème chinois

Un système de congruences est un système de la forme

$$(SC) \qquad \begin{cases} x \equiv a_1 & (\text{mod } m_1), \\ x \equiv a_2 & (\text{mod } m_2), \\ \dots & \dots \\ x \equiv a_k & (\text{mod } m_k). \end{cases}$$

où les a_i, et les m_i sont des entiers donnés. Résoudre le système (SC) consiste à déterminer tous les entiers $x \in \mathbb{Z}$ vérifiant le système.

Lorsque les entiers m_i sont premiers entre eux deux à deux, nous allons voir que le système (SC) admet toujours des solutions. Ce résultat est connu sous le nom de Théorème chinois parce que les Chinois en utilisaient des cas particuliers pour déterminer les dates de certains événements astronomiques.

D'après Michel Demazure (Cours d'algèbre, Éditions Cassini, 1997), le théorème chinois apparaît pour la première fois dans le traité appelé *Juzhang suhanshu* écrit entre 280 et 473 de notre ère. Le problème y était posé de la façon suivante.

Nous avons des choses dont nous ne connaissons pas le nombre ;
– si nous les comptons par paquets de 3, le reste est 2,
– si nous les comptons par paquets de 5, le reste est 3,
– si nous les comptons par paquets de 7, le reste est 2.
Combien y a-t-il de choses ? Réponse 23.

Nous allons voir qu'il suffit de savoir résoudre un système de deux congruences.

Théorème 3.7 (Théorème chinois) *Soit m et n deux entiers **premiers entre eux**.*

1. *Pour tout couple d'entiers $(a, b) \in \mathbb{Z}^2$, il existe $c \in \mathbb{Z}$ tel que l'on ait l'équivalence*

$$(SC) \qquad \begin{cases} x \equiv a & (\text{mod } m), \\ x \equiv b & (\text{mod } n). \end{cases} \iff (x \equiv c \pmod{mn}).$$

   Le système (SC) admet donc une infinité de solutions dans $\mathbb{Z}$, ce sont tous les entiers de la forme $x = c + kmn$, où $k \in \mathbb{Z}$. Deux solutions distinctes sont congrues modulo mn.

2. *Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ sont isomorphes et l'application*

$$\psi : \quad \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

   définie par $\qquad \forall x \in \mathbb{Z}, \quad \psi(\overline{x} \ (\text{mod } mn)) = (\overline{x} \ (\text{mod } m), \overline{x} \ (\text{mod } n))$

   réalise un isomorphisme entre ces anneaux.

Preuve :

1. Soit u et v deux entiers tels que $un + vm = 1$. L'entier c défini par l'égalité

$$(S) \qquad c = aun + bvm$$

   est solution de (SC) puisque

$$\begin{cases} c &= a(1 - vm) + bvm &= a + vm(b - a) &\equiv a & (\text{mod } m), \\ c &= aun + b(1 - un) &= b + un(a - b) &\equiv b & (\text{mod } n). \end{cases}$$

   Il est facile de vérifier que pour tout entier $k \in \mathbb{Z}$, l'entier $x = c + kmn$ est aussi solution de (SC).

   Réciproquement, soit x une solution de (SC), alors $x - c$ est congru à 0 modulo m et modulo n, donc m et n divisent $x - c$ donc mn divise $x - c$ puisque $\text{pgcd}\,(m, n) = 1$.

2. On vérifie facilement que ψ réalise un morphisme d'anneaux. Il résulte de la question précédente que ψ est surjective, donc bijective puisque les deux anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ont même nombre mn d'éléments.

   Remarque L'isomorphisme réciproque de ψ s'obtient en résolvant le système (SC). Soit en effet $(a, b) \in \mathbb{Z}^2$, la relation $\psi^{-1}(\overline{a}, \overline{b}) = \overline{x} \in \mathbb{Z}/mn\mathbb{Z}$ signifie que x est solution du système (SC).

   En particulier, il résulte de (S) que $\psi^{-1}(\overline{a}, \overline{b}) = \overline{x}$ ***se calcule à l'aide du théorème de Bézout, c'est-à-dire de l'algorithme d'Euclide étendu.*** □

Le théorème chinois nous dit qu'un système de deux congruences équivaut, lorsque m et n sont premiers entre eux, à une seule congruence. Pour résoudre un système (SC) à $k > 2$ congruences, où les m_i sont premiers entre eux deux à deux, il suffit donc de résoudre le système des deux premières congruences en les remplaçant par une unique congruence, ce qui ramène le système à $k - 1$ congruences, etc. Pour finalement aboutir à deux.

Exemple Déterminer la plus petite solution positive x_0 du système

$$(SC) \qquad \begin{cases} x \equiv 9 & (\text{mod } 14), \\ x \equiv 13 & (\text{mod } 31). \end{cases}$$

– *Première méthode :* partant de la relation de Bézout

$$1 = (-11) \times 14 + 5 \times 31,$$

l'égalité (S) s'écrit

$$c = 13 \times (-11) \times 14 + 9 \times 5 \times 31 = -607.$$

La solution cherchée est $x_0 = 261$ puisque $261 \equiv -607 \pmod{14 \times 31}$ et $1 \leq 261 \leq 14 \times 31$.

– *Deuxième méthode :* on écrit le système (SC) dans $\mathbb{Z}$ puis dans l'un des deux groupes $\mathbb{Z}/14\mathbb{Z}$ ou $\mathbb{Z}/31\mathbb{Z}$. Dans $\mathbb{Z}/14\mathbb{Z}$ par exemple, cela donne

$$\begin{cases} x &= 9 + 14k, \\ x &= 13 + 31\ell, \end{cases} \implies \begin{cases} \overline{x} &= \overline{9} \\ \overline{x} &= \overline{13} + \overline{31}\,\overline{\ell} \;=\; \overline{13} + \overline{3}\,\overline{\ell}, \end{cases}$$

d'où l'on tire $\qquad \overline{3}\,\overline{\ell} = \overline{9} - \overline{13} = -\overline{4} = \overline{10}.$

Comme 14 et 31 sont premiers entre eux, 14 et 3 le sont, donc 3 est inversible modulo 14. L'inverse de $\overline{3}$ dans $\mathbb{Z}/14\mathbb{Z}$ est $\overline{5}$, ce qui donne $\overline{\ell} = \overline{50} = \overline{8}$. Posant $\ell = 8 + 14\ell'$, on obtient

$$x = 13 + 31\ell = 13 + 31 \times 8 + (14 \times 31)\ell' = 261 + (14 \times 31)\ell'.$$

Exercice 26 — Refaire les calculs précédents dans $\mathbb{Z}/31\,\mathbb{Z}$.

Corollaire 3.8 *Soit G_1 et G_2 deux groupes cycliques d'ordres respectifs m et n. Le groupe produit $G_1 \times G_2$ est cyclique si et seulement si m et n sont premiers entre eux.*

Preuve : Les groupes G_1 et G_2 sont respectivement isomorphes aux groupes $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ d'après le corollaire 2.14 (page 34), la condition est donc suffisante d'après le théorème chinois. Elle est nécessaire car si $\text{pgcd}\,(m, n) = d > 1$, on pose $m = dm_1$ et $n = dn_1$, et soit

$$q = \text{ppcm}(m, n) = dm_1n_1 = n_1m = m_1n.$$

Comme $mn = qd$, on a $q < mn$, et tout élément $(x, y) \in G_1 \times G_2$ vérifie

$$(x, y)^q = (x^q, y^q) = (x^{n_1m}, y^{m_1n}) = (1, 1).$$

Il n'existe donc pas dans $G_1 \times G_2$ d'élément d'ordre mn, ainsi $G_1 \times G_2$ n'est pas cyclique. □

Exercice 27 — Décrire l'isomorphisme de $\mathbb{Z}/12\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Corollaire 3.9 *Soit m et n deux entiers premiers entre eux, les groupes multiplicatifs*

$$(\mathbb{Z}/mn\mathbb{Z})^* \quad \text{et} \quad (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

sont isomorphes.

Preuve : Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ étant isomorphes, les groupes $(\mathbb{Z}/mn\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^*$ le sont, il est facile de voir que $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. □

Exercice 28 — Montrer que que si $m > 2$ et $n > 2$ sont deux entiers premiers entre eux, le groupe $(\mathbb{Z}/mn\mathbb{Z})^*$ n'est pas cyclique.

3.3.1 Retour à l'indicatrice d'Euler

Théorème 3.10 *Soit φ l'indicatrice d'Euler (définie page 35).*

1. *Si m et n sont deux entiers positifs premiers entre eux, alors*

$$\varphi(mn) = \varphi(m)\,\varphi(n).$$

2. *Si $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_q^{\alpha_q}$ est la décomposition en facteurs premiers d'un entier $a \geq 2$, alors*

$$\varphi(a) = \prod_{i=1}^{q} \varphi(p_i^{\alpha_i}) = a \prod_{i=1}^{q} \left(1 - \frac{1}{p_i}\right).$$

En particulier, $\varphi(a)$ est paire dès que $a > 2$.

Preuve :

1. On sait d'après le corollaire 3.4 (page 38) que $\#(\mathbb{Z}/k\mathbb{Z})^* = \varphi(k)$ pour tout entier $k > 0$. On a donc

$$\varphi(mn) = \#(\mathbb{Z}/mn\mathbb{Z})^* = \#(\mathbb{Z}/m\mathbb{Z})^* \times \#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(m)\,\varphi(n).$$

   en vertu du corollaire 3.9 ci-dessus.

2. On en déduit par récurrence sur q, et compte tenu de la proposition 2.15 (page 35),

$$\varphi(a) = \prod_{i=1}^{q} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{q} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = a \prod_{i=1}^{q} \left(1 - \frac{1}{p_i}\right).$$

Si $a > 2$, $\varphi(a)$ est paire d'après la proposition 2.15 page 35. □

Notons que pour calculer $\varphi(a)$ selon la formule ci-dessus, il faut connaître la décomposition en facteurs premiers de a.

3.4 Application à la cryptographie, l'algorithme RSA

La cryptographie, du grec *kryptos* qui signifie caché, et *graphein* écriture, est l'art de transformer un message pour tenter de le rendre illisible par toute autre personne que son destinataire.
Depuis l'antiquité, la nécessité de faire parvenir des messages qui ne puissent être lus par "l'ennemi" a suscité quantité de techniques de cryptage de textes. Jules César fut le premier responsable militaire à crypter ses messages. Le *chiffre de César* consistait à remplacer chaque lettre de l'alphabet par la lettre venant trois places après. Un tel algorithme de cryptage, où chaque lettre est remplacée par une autre, est appelé **chiffre de substitution**.
Dans le cas du chiffre de César, le destinataire remplaçait chaque lettre par la lettre venant trois places avant dans l'alphabet et retrouvait ainsi le message, il avait **la clé** du chiffrage, c'est-à-dire l'information lui permettant d'effectuer le **déchiffrage**.
Un mot ou une suite de mots peut servir à fabriquer un chiffre de substitution plus efficace.
Soit par exemple la suite de mots LE ROI AGAMEMNON. On commence par ôter les lettres qui se répètent et à coller les mots, ce qui donne LEROIAGMN. Utilisant ces lettres comme début de l'alphabet chiffré, les autres lettres suivant normalement, on obtient l'alphabet chiffré suivant :

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
l	e	r	o	i	a	g	m	n	p	q	s	t	u	v	w	x	y	z	b	c	d	f	h	j	k

Un indiscret, interceptant le message SIZTLBMRIZBLTCZLUB, s'il ne possède pas la clé, c'est-à-dire la phrase "LE ROI AGAMEMNON", devra essayer toutes les permutations possibles de l'alphabet, il y en a 26!, c'est dire qu'il peut en avoir pour des années, noter par exemple que 20! secondes représentent plus de 77 milliards d'années, c'est-à-dire plus de 5 fois l'âge de l'univers.
Les chiffres de substitution restèrent inviolés durant plus de quinze siècles.
Ce sont les Arabes qui les premiers ont "cassé" ces chiffres, grâce à leur science des langues, utilisant des méthodes statistiques très fines basées sur la fréquence moyenne d'utilisation de telle ou telle lettre dans telle ou telle langue.
On a retrouvé en 1987, dans les archives ottomanes à Istanbul, un traité intitulé "*Manuscrit sur le déchiffrement des messages cryptés*", écrit par le célèbre philosophe arabe Abou Youssouf **Al Kindi**, qui vécut de la fin du VIII^{e} siècle au milieu du IX^{e} et qui écrivit 290 ouvrages de médecine, d'astronomie, de mathématiques, de linguistique et de musicologie. C'est le premier ouvrage connu de **cryptanalyse**, ou l'art de décrypter un message sans en connaître la clé.
L'histoire de la cryptographie ne fut depuis qu'une longue joute entre cryptographes et cryptanalystes, les mêmes individus jouant souvent les deux rôles, joute dont on pourra lire les épisodes et les détails dans le passionnant ouvrage de Simon **Singh** "*Histoire des codes secrets*" (JC Lattes, 1999).
Les algorithmes modernes de cryptage ne sont plus des chiffres de substitution, c'est-à-dire que la même lettre, "e" par exemple, sera, au fur et à mesure de ses apparitions dans le texte, remplacée par des symboles différents entre eux, ce qui rend caduques les analyses basées sur la fréquence moyenne d'occurrence d'une lettre dans une langue donnée.
Jusqu'aux années 1970, des centaines de "fonctionnaires" de toutes nationalités parcouraient le monde, une petite mallette attachée au poignet, pour transmettre les fameuses clés.
Ce n'est qu'en 1976 que deux chercheurs américains, Whitfield **Diffie** et Martin **Hellman** démontrèrent que ce qui passait pour un rêve fou était possible : deux correspondants, (appelés traditionnellement Alice et Bernard en français), pouvaient se fabriquer une clé secrète au vu et au su de tous les espions du monde, représentés par Eve (voir plus loin le protocole d'échange de clés de Diffie-Hellman). Ces travaux ouvraient en même temps la voie à la cryptographie à clé publique.

Parmi les problèmes majeurs auxquels s'attaque la cryptographie aujourd'hui, citons le problème de la **génération de clés** de chiffrage, celui de la **confidentialité** et celui de **l'authentification** de l'expéditeur d'un message, message qui peut être secret ou non.

L'algorithme à clé publique RSA

Imaginé par les trois chercheurs américains Ronald **Rivest**, Adi **Shamir** et Leonard **Adleman** en 1977, dans la foulée de la découverte de Diffie et Hellman, l'algorithme RSA, nommé d'après leurs initiales, a révolutionné le domaine de la cryptographie.
Le plus étonnant de l'affaire réside dans le fait que le protocole de Diffie-Hellman et l'algorithme RSA reposent sur des propriétés mathématiques connues depuis le XVIII^e siècle, voire depuis Fermat au XVII^e siècle. Mais il est vrai que la puissance de calcul nécessaire à la mise en œuvre de ces algorithmes n'était pas disponible à cette époque.
L'algorithme RSA est un algorithme de cryptage qui permet aussi de signer un message, c'est-à-dire de rendre possible l'authentification de l'expéditeur. Il repose sur le fait qu'en l'état actuel du savoir et de la technique, on ne sait effectuer rapidement aucune des deux opérations suivantes :
– Décomposer un "grand" entier en facteurs premiers.
– Étant donné un grand entier n et un entier e, *inverser* la fonction

$$\psi_e : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \quad \text{définie par} \quad \psi_e(x) = x^e,$$

c'est-à-dire retrouver $x \pmod n$ à partir de $x^e \pmod n$, ceci dans les cas, bien entendu, où cette fonction est injective.

Convention Étant donné un entier positif n et deux entiers a et b, il nous arrivera d'écrire $a = b \pmod n$ pour signifier que $a \equiv b \pmod n$ **et** que $0 \leq b < n$.
Cela revient à dire que b est le reste de la division euclidienne de a par n.
L'algorithme RSA est basé sur le résultat arithmétique suivant, corollaire du théorème d'Euler, qui permet sous certaines conditions d'inverser rapidement la fonction ψ_e ci-dessus.

Lemme 3.11 *Soit p et q deux nombres premiers distincts, et soit $n = pq$. Pour tout entier positif t tel que $t \equiv 1 \pmod{\varphi(n)}$, on a*

$$\forall a \in \mathbb{Z}, \quad a^t \equiv a \pmod n, \qquad \textit{c'est-à-dire} \qquad \forall x \in \mathbb{Z}/n\mathbb{Z}, \quad x^t = x.$$

Preuve : On sait que $\varphi(n) = (p-1)(q-1)$.
Posons $t = 1 + k\varphi(n)$, avec $k \in \mathbb{N}$, et soit $a \in \mathbb{Z}$. Trois cas sont possibles.

1. $(\text{pgcd}\,(a,p) = 1)$ et $(\text{pgcd}\,(a,q) = 1)$, ce qui équivaut à $(\text{pgcd}\,(a,n) = 1)$.
2. $(\text{pgcd}\,(a,p) = 1)$ et a est multiple de q. (resp $(\text{pgcd}\,(a,q) = 1)$ et a est multiple de p).
3. a est multiple de $pq = n$.

– Dans le premier cas, on a $a^{\varphi(n)} \equiv 1 \pmod n$ d'après le théorème d'Euler, donc

$$a^t = a^{1+k\varphi(n)} = a\left(a^{\varphi(n)}\right)^k \equiv a \pmod n.$$

– Dans le second cas, $a^{p-1} = a^{\varphi(p)} \equiv 1 \pmod p$ d'après le théorème d'Euler, donc

$$a^t = a^{1+k(p-1)(q-1)} = aa^{k(p-1)(q-1)} = a\left(a^{(p-1)}\right)^{k(q-1)} \equiv a \pmod p. \tag{1}$$

Comme de plus a est multiple de q, on a

$$a^t \equiv a \equiv 0 \pmod q. \tag{2}$$

On déduit de (1) et (2) que $a^t - a$ est multiple de p et q donc de n, c'est-à-dire $a^t \equiv a \pmod n$.

– Dans le troisième cas, on a $a \equiv 0 \pmod{n}$ donc $a^t \equiv a \equiv 0 \pmod{n}$. □

Corollaire 3.12 *Soit p et q deux nombres premiers distincts et soit $n = pq$. Soit e un entier positif premier avec $\varphi(n)$ et soit d l'inverse de e modulo $\varphi(n)$.*

1. *L'application ψ_e définie sur $\mathbb{Z}/n\mathbb{Z}$ par $\psi_e(x) = x^e$ est une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur lui-même, et la bijection réciproque est l'application ψ_d définie par $\psi_d(x) = x^d$*
2. *On en déduit que les applications π_e et π_d définies sur l'ensemble $\{2, 3, \ldots, n-1\}$ par*

$$\pi_e(a) = a^e \pmod{n} \quad et \quad \pi_d(a) = a^d \pmod{n}$$

sont des bijections réciproques de $\{2, 3, \ldots, n-1\}$.

Preuve : Pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $\psi_d \circ \psi_e(x) = \psi_e \circ \psi_d(x) = x^{ed} = x$ puisque $ed \equiv 1 \pmod{\varphi(n)}$. Pour le point 2., on remarque que $\psi_d(0) = \psi_e(0) = 0$ et $\psi_d(1) = \psi_e(1) = 1$. □

Chaque élément d'information à transmettre, chiffre, lettre, etc., est représenté par un entier appartenant à un ensemble $\{2, 3, \ldots, C\}$, où $C \in \mathbb{N}$, c'est ce qu'on appelle un **encodage**, cet encodage est connu de tous. Chaque utilisateur du cryptosystème RSA procède comme suit.

– Il choisit (ou achète sur le marché) deux "grands" nombres premiers p et q. Il calcule le produit $n = pq$ et et l'indicatrice d'Euler $\varphi(n) = (p-1)(q-1)$. Remarquons que l'on a toujours $n > C$.
– Il choisit un entier $d > 1$ **premier avec** $\varphi(n)$ et calcule son inverse e modulo $\varphi(n)$.
– Il publie le couple (e, n), qui est donc appelé sa **clé publique**, et conserve le couple $(d, \varphi(n))$ qui est sa **clé secrète**.

Remarquons que, connaissant la clé publique (e, n), quiconque voudrait reconstituer la clé secrète $(d, \varphi(n))$ devrait calculer $\varphi(n) = (p-1)(q-1)$, donc connaître p et q, c'est-à-dire la décomposition de n en facteurs premiers.

– **Encryptage** Si Alice veut envoyer le message secret $m \in \{2, 3, \ldots, C\}$ à Bernard, elle prend connaissance de la clé publique (e, n) de ce dernier (dont la clé secrète est $(d, \varphi(n))$), puis calcule l'entier $M = m^e \pmod{n}$. C'est le message crypté, qu'elle envoie à Bernard.
– **Décryptage** Bernard calcule $M^d \pmod{n}$ et récupère m puisque

$$M^d \equiv m^{ed} \pmod{n} = m \pmod{n}.$$

– **Signature** L'algorithme RSA permet en outre à Alice de **signer** un message m de façon à ce que Bernard soit certain que c'est bien elle qui l'a envoyé. Si (e_1, n_1) est sa clé publique et $(d_1, \varphi(n_1))$ sa clé secrète, Alice calcule l'entier $s = m^{d_1} \pmod{n_1}$ et fait parvenir à Bernard le couple (m, s) qui est le **message signé**.
– **Vérification** Recevant (m, s), Bernard calcule $s^{e_1} \pmod{n_1}$. Si $s^{e_1} = m$, il est certain que le message vient d'Alice puisque seule Alice connaît l'inverse d_1 de e_1 modulo $\varphi(n_1)$, c'est-à-dire la bijection réciproque π_{d_1} de la bijection π_{e_1} de l'ensemble $\{2, 3, \ldots, n_1 - 1\}$ dans lui-même.
– **Commentaire** Dans notre cas, le message signé par RSA n'est pas secret, mais il est *authentifié*.

L'algorithme RSA est dit **asymétrique** au sens où

– pour chiffrer, Alice utilise la clé publique du destinataire Bernard,
– pour déchiffrer, Bernard utilise sa propre clé secrète.

Exemple Soit $n = 7 \times 11 = 77$. Alors $\varphi(77) = 6 \times 10 = 60$. Bernard choisit $e = 13$, il utilise l'algorithme d'Euclide étendu pour calculer d, et obtient $1 = 13 \times 37 + 60 \times (-8)$, c'est-à-dire $d = 37$. Sa clé publique est donc $(77, 13)$ et sa clé privée $(60, 37)$.

Pour envoyer à Bernard le message $m = 9$, Alice calcule $M = 9^{13} \pmod{77}$ en utilisant **un algorithme de calcul rapide des puissances** basé sur l'écriture en binaire de 13,

$$13 = 2^3 + 2^2 + 1 = 1101.$$

Pour calculer $x^{13} = x \times x^4 \times x^8$, il lui suffit de calculer successivement

$$x \longrightarrow x^2 \longrightarrow x^4 \longrightarrow x^8 \longrightarrow x^{12} = x^4 \times x^8 \longrightarrow x^{13} = x \times x^{12},$$

ce qui ne fait que 5 multiplications au lieu de 12. Pour cet algorithme de calcul rapide des puissances, le nombre des multiplications nécessaires pour calculer a^n est majoré par $2\log_2 n$. Chacune des opérations est effectuée modulo 77, ce qui évite les trop grands nombres.

$$\begin{array}{lcccl}
9^2 = 81 & & & = & 4 \pmod{77}, \\
9^4 & \equiv & 4^2 & = & 16 \pmod{77}, \\
9^8 & \equiv & 16^2 = 256 & = & 25 \pmod{77}, \\
9^{12} = 9^8 \times 9^4 & \equiv & 25 \times 16 = 400 & = & 15 \pmod{77}, \\
9^{13} = 9^{12} \times 9 & \equiv & 15 \times 9 = 135 & = & 58 \pmod{77}.
\end{array}$$

Recevant $M = 58$, Bernard calcule $58^{37} \pmod{77}$ de la façon suivante

$$\begin{array}{lcccl}
58^2 = 3364 & & & = & 53 \pmod{77}, \\
58^4 & \equiv & 53^2 = 2809 & = & 37 \pmod{77}, \\
58^8 & \equiv & 37^2 = 1369 & = & 60 \pmod{77}, \\
58^{16} & \equiv & 60^2 = 3600 & = & 58 \pmod{77}, \\
58^{32} & \equiv & 58^2 = 3364 & = & 53 \pmod{77}, \\
58^{36} = 58^{32} \times 58^4 & \equiv & 53 \times 37 = 1961 & = & 36 \pmod{77}, \\
58^{37} = 58^{36} \times 58 & \equiv & 36 \times 58 = 2088 & = & 9 \pmod{77},
\end{array}$$

et récupère $m = 9$ (en effectuant 7 multiplications au lieu de 36).

Chapitre 4

La division euclidienne dans l'algèbre $\mathbb{K}[X]$ et ses conséquences

Dans tout ce chapitre, $\mathbb{K}$ désigne un corps commutatif.

4.1 Généralités

Théorème 4.1 (Division euclidienne) *Soit A et B deux polynômes de $\mathbb{K}[X]$ tels que $B \neq 0$. Il existe un couple unique $(Q, R) \in \mathbb{K}[X]^2$ vérifiant*

$$\textit{(DE)} \qquad \begin{cases} A = BQ + R \\ \deg(R) < \deg(B). \end{cases}$$

*On dit que Q est le **quotient** et R le **reste** de la division euclidienne de A par B.*

La démonstration est basée sur le lemme suivant, qui justifie la technique de la *division des polynômes suivant les puissances décroissantes.*

Lemme 4.2 *Soit U et V deux polynômes non nuls de $\mathbb{K}[X]$ tels que $\deg(U) \geq \deg(V)$. Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $\deg(U - VQ) < \deg(U)$.*

Preuve : Soit a_k le coefficient dominant de U et b_q celui de V. Par hypothèse, on a $k \geq q$. On "tue" le monôme $a_k X^k$ en posant $\gamma = a_k (b_q)^{-1}$ et $Q = \gamma X^{k-q}$, de sorte que le coefficient dominant de VQ soit a_k et qu'ainsi $\deg(U - VQ) < k$. □

Preuve du théorème 4.1.

– *Existence.* Considérons l'ensemble $\mathcal{A} = \{A - BQ \,|\, Q \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$, et soit r le plus petit des degrés des polynômes de $\mathcal{A}$. Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$\deg(A - BQ) = r.$$

Supposons $r \geq \deg(B) \geq 0$. D'après le lemme 4.2, il existe $Q' \in \mathbb{K}[X]$ tel que le polynôme

$$(A - BQ) - BQ' = A - B(Q + Q')$$

soit de degré $r' < r$, ce qui est impossible puisque $A - B(Q + Q') \in \mathcal{A}$.
On a donc $-\infty \leq r < \deg(B)$.

– *Unicité.* Soit Q et $Q_1 \in \mathbb{K}[X]$ deux polynômes vérifiant les inégalités

$$\begin{cases} \deg(A - BQ) < \deg(B), \\ \deg(A - BQ_1) < \deg(B). \end{cases}$$

On en déduit $\deg((A-BQ)-(A-BQ_1)) = \deg(B(Q_1-Q)) < \deg(B)$,

ce qui n'est possible que si $Q_1 - Q = 0$.

L'unicité du polynômes Q implique celle du polynôme $R = A - BQ$. □

Retenons que dans la pratique, la division euclidienne des polynômes correspond à la division suivant les puissances décroissantes.

Définition 4.1 *Soit A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$.*

1. *On dit que B est un **diviseur** ou un facteur de A, ou que B divise A, ou que A **est divisible par** B, lorsque le reste de la division euclidienne de A par B est nul.*
2. *On dit que B est un **diviseur propre** de A si B divise A et si $1 \leq \deg(B) < \deg(A)$.*

Proposition 4.3 *Soit A et B deux polynômes non nuls de $\mathbb{K}[X]$. On a l'équivalence*

$$\{(A \text{ divise } B) \text{ et } (B \text{ divise } A)\} \Longleftrightarrow (\exists \lambda \in \mathbb{K}^*,\ A = \lambda B).$$

Preuve : Soit Q et Q' les deux polynômes non nuls tels que $A = QB$ et $B = Q'A$, cela donne $A = Q'QA$, l'anneau $\mathbb{K}[X]$ étant intègre, on en déduit $Q'Q = 1$, d'où $\deg(Q) = 0$. c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda \in \mathbb{K}^*$. □

Définition 4.2 *Soit $P = c_0 + c_1X + \cdots + c_kX^k$ un polynôme de $\mathbb{K}[X]$. Pour chaque $a \in \mathbb{K}$, la **valeur** de P en a est définie par*

$$P(a) = c_0 + c_1a + \cdots + c_ka^k \in \mathbb{K}.$$

*On dit qu'un un élément $a \in \mathbb{K}$ est **racine** de P si $P(a) = 0 \in \mathbb{K}$.*

Le résultat suivant est une première conséquence de la division euclidienne dans $\mathbb{K}[X]$.

Proposition 4.4 *Le polynôme $P \in \mathbb{K}[X]$ admet $a \in \mathbb{K}$ comme racine si et seulement s'il est divisible par le polynôme $(X - a)$.*

Preuve : Effectuons la division euclidienne dans $\mathbb{K}[X]$ de P par $B = X - a$. Il existe un couple unique de polynômes $(Q, R) \in \mathbb{K}[X]^2$ vérifiant $P = BQ + R$, et $\deg(R) < \deg(X - a) = 1$. Le polynôme R est donc constant. Comme $B(a) = 0$, on a $P(a) = 0$ si et seulement si $R = 0$. □

On en déduit le théorème suivant, qui joue un rôle essentiel dans la théorie des corps finis.

Théorème 4.5 *Soit $P \in \mathbb{K}[X]$ et $a_1, a_2, \ldots, a_k$ des racines **distinctes** de P dans $\mathbb{K}$, alors P est divisible par le polynôme $(X - a_1)(X - a_2)\ldots(X - a_k)$ de degré k.*
Il en résulte qu'un polynôme de degré n de $\mathbb{K}[X]$ possède au plus n racines distinctes dans $\mathbb{K}$.

Preuve : Par récurrence. La propriété est vraie pour $k = 1$ d'après la proposition 4.4 ci-dessus. Supposons-la vérifiée pour $k - 1$, alors

$$P(X) = (X - a_1)\ldots(X - a_{k-1})Q(X).$$

Comme $P(a_k) = (a_k - a_1)\ldots(a_k - a_{k-1})Q(a_k) = 0$, **l'intégrité** de $\mathbb{K}$ implique $Q(a_k) = 0$ donc $Q(X) = (X - a_k)Q_1(x)$, d'où le résultat. □

Le théorème 4.5 reste vrai si le corps $\mathbb{K}$ est remplacé par un anneau intègre.

Contrexemple Dans l'anneau $(\mathbb{Z}/6\mathbb{Z})[X]$, on a l'égalité $(X - 2)(X - 3) = X(X - 5)$.
Le polynôme $P = (X - 2)(X - 3)$ possède donc 4 racines distinctes dans l'anneau non intègre $\mathbb{Z}/6\mathbb{Z}$. Pour chacune des racines $a_i = 0,\ 2,\ 3$ ou 5, P est divisible par $(X - a_i)$. Mais P n'est pas divisible par le produit des $(X - a_i)$, qui est de degré 4.

4.2 Les idéaux de $\mathbb{K}[X]$

Soit $A \in \mathbb{K}[X]$, on voit facilement que l'ensemble $\langle A \rangle = \{AQ \,|\, Q \in \mathbb{K}[X]\}$ est un idéal de $\mathbb{K}[X]$.
Nous allons voir que réciproquement, comme dans le cas de $\mathbb{Z}$, la division euclidienne dans $\mathbb{K}[X]$ implique que tout idéal de $\mathbb{K}[X]$ est de cette forme.
Rappelons qu'un polynôme $A \in \mathbb{K}[X]$ est dit **unitaire** si son coefficient dominant est égal à 1.

Théorème 4.6 *Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$, et soit $r \geq 0$ **le plus petit des degrés** des polynômes non nuls appartenant à $\mathcal{I}$.*

1. *Pour tout polynôme $A \in \mathcal{I}$ de degré r, on a $\mathcal{I} = \langle A \rangle$.*
2. *Il existe un polynôme unitaire **unique** $U \in \mathcal{I}$ tel que $\mathcal{I} = \langle U \rangle$.*
3. *$\mathcal{I}$ est un idéal propre de $\mathbb{K}[X]$ si et seulement si $r \geq 1$.*

Preuve : L'entier r existe d'après la propriété fondamentale de $\mathbb{N}$ (page 6).

1. Soit $A \in \mathcal{I}$ de degré $r \geq 0$, et soit $P \in \mathcal{I}$. La division euclidienne de P par A s'écrit $P = AQ + R$, avec $\deg(R) < \deg(A) = r$.

   On voit que $R = P - AQ \in \mathcal{I}$, et comme $\deg(R) < r$, on a $R = 0$ et $P = AQ$. Cela montre que $\mathcal{I} \subseteq \langle A \rangle$. Réciproquement, il est clair que $\langle A \rangle \subseteq \mathcal{I}$.
2. Divisant A par son coefficient dominant, on obtient un polynôme unitaire $U \in \mathcal{I}$ tel que $\mathcal{I} = \langle U \rangle$. Ce polynôme est unique car si $U' \in \mathcal{I}$ est un polynôme unitaire tel que $\mathcal{I} = \langle U \rangle = \langle U' \rangle$, chacun des deux polynômes U et U' divise l'autre, il existe $\lambda \in \mathbb{K}^*$ tel que $U = \lambda U'$ (cf. proposition 4.3 page 48), les polynômes U et U' étant unitaires, on a nécessairement $\lambda = 1$ donc $U = U'$.
3. Si $\deg(U) = 0$, $U = 1 \in \mathcal{I}$, ce qui équivaut à $\mathcal{I} = \mathbb{K}[X]$. □

Remarquons que si $\mathcal{I} = \{0\}$, on peut écrire $\mathcal{I} = \langle 0 \rangle$, ce qui montre que tout idéal $\mathcal{I}$ de $\mathbb{K}[X]$ est de la forme $\mathcal{I} = \langle A \rangle$.
On pourra comparer la démonstration qui précède à celle du théorème 1.3 (page 22), et le rôle dans les deux cas de la propriété fondamentale de $\mathbb{N}$ (page 6).

4.3 Polynômes irréductibles

Définition 4.3 *Un polynôme **irréductible** est un polynôme non constant qui n'admet pas de diviseur propre. Un polynôme non irréductible est aussi dit **réductible**.*

Par exemple, tous les polynômes de degré 1 sont irréductibles. Lorsque $\mathbb{K} = \mathbb{C}$, ce sont les seuls. Lorsque $\mathbb{K} = \mathbb{R}$, il y a aussi les polynômes de degré 2 de discriminant négatif. Pour d'autres corps, nous verrons qu'il existe des polynômes irréductibles de degré arbitrairement grand.
On démontre l'exact équivalent du théorème 1.6 page 23 :

Théorème 4.7 *Soit P un polynôme de degré $n \geq 1$, et soit $\mathcal{D} \subset \mathbb{N}$ l'ensemble des degrés des diviseurs non constants de P. Alors $\mathcal{D} \neq \emptyset$ puisque $n \in \mathcal{D}$.*
Soit r le plus petit élément de $\mathcal{D}$ et soit A un diviseur de P de degré r, alors A est irréductible.
Cela signifie que tout polynôme de degré positif admet un facteur irréductible.

Attention Il est **faux de penser qu'un polynôme est irréductible si et seulement s'il n'a pas de racine**. Ainsi

1. Tout polynôme de degré 1 admet une racine, mais est irréductible.

2. Le polynôme $(X^2+1)^2$, de degré 4, n'a pas de racine dans $\mathbb{R}$ mais est réductible dans $\mathbb{R}[X]$, le polynôme $(X^2+X+1)^3$, de degré 6, n'a pas de racine dans $\mathbb{F}_2$ mais est réductible dans $\mathbb{F}_2[X]$, etc.

On a cependant l'équivalence suivante **dans les seuls cas des polynômes de degré 2 ou 3**.

Proposition 4.8 *Un polynôme de degré* 2 *ou* 3 *est irréductible dans* $\mathbb{K}[X]$ *si et seulement s'il n'admet pas de racine dans* $\mathbb{K}$.

Preuve : Un polynôme P est réductible si et seulement s'il possède un diviseur propre, c'est-à-dire un diviseur A vérifiant $1 \leq \deg(A) < \deg(P)$, cela implique $\deg(P) \geq 2$.
Si on écrit $P = AB$, alors on a $(1 \leq \deg(B) \leq \deg(P) - 1)$ et $(\deg(A) + \deg(B) = \deg(P))$.
Si $\deg(P) \leq 3$, on en déduit $(\deg(A) = 1)$ ou $(\deg(B) = 1)$, donc P admet une racine. □

Exercice 29 — Montrer que dans $\mathbb{F}_2[X]$, le seul polynôme irréductible de degré 2 est X^2+X+1, les seuls polynômes irréductibles de degré 3 sont X^3+X^2+1 et X^3+X+1.

Exercice 30 — Montrer que dans $\mathbb{F}_3[X]$, les seuls polynômes irréductibles unitaires de degré 2 sont X^2+1, X^2+X+2, et X^2+2X+2.

4.4 Pgcd de deux polynômes

Soit A et B deux polynômes non tous deux nuls de $\mathbb{K}[X]$, on vérifie facilement que l'ensemble

$$\mathcal{I}(A,B) = \{AU + BV \mid (U,V) \in \mathbb{K}[X]^2\}$$

est un idéal de $\mathbb{K}[X]$. Comme A et B sont éléments de $\mathcal{I}(A,B)$, cet idéal n'est pas réduit à $\{0\}$. Il existe d'après le théorème 4.6 (page 49) un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que

$$\mathcal{I}(A,B) = \langle D \rangle.$$

Définition 4.4 *On appelle plus grand commun diviseur de* A *et* B, *ou* pgcd *de* A *et* B, *et on désigne par* $\operatorname{pgcd}(A,B)$ *l'unique polynôme unitaire* $D \in \mathbb{K}[X]$ *tel que* $\mathcal{I}(A,B) = \langle D \rangle$.

La démonstration des énoncés qui suivent est quasi-identique à celle des énoncés qui leur correspondent dans le cas de l'anneau $\mathbb{Z}$.

Théorème 4.9 (Propriété caractéristique du pgcd) *(Cf. théorème 1.8 page 24)*
Soit A *et* B *deux polynômes de* $\mathbb{K}[X]$ *non tous deux nuls. Le* pgcd *de* A *et* B *est l'unique polynôme unitaire* $D \in \mathbb{K}[X]$ *tel que*

1. D *est un diviseur commun de* A *et* B.
2. *Tout diviseur commun de* A *et* B *divise* D.

On dira que deux polynômes A et B sont **premiers entre eux** si leur seul diviseur unitaire commun est le polynôme 1, autrement dit si leur pgcd est le polynôme 1.

Théorème 4.10 (Théorème de Bézout) *(Cf. théorème 1.9 page 25)*
Soit A *et* B *deux polynômes de* $\mathbb{K}[X]$.

1. *Soit* D *un* ***diviseur commun*** *unitaire de* A *et* B. *Alors* D *est le* pgcd *de* A *et* B *si et seulement s'il existe deux polynômes* U *et* V *dans* $\mathbb{K}[X]$ *tels que*

$$AU + BV = D. \tag{1}$$

2. *En particulier, les polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V dans $\mathbb{K}[X]$ tels qu'on ait*

$$AU + BV = 1. \tag{2}$$

Proposition 4.11 *(Cf. proposition 1.12 page 26) Soit A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$, et soit R le reste de la division euclidienne de A par B, alors*

$$\operatorname{pgcd}(A, B) = \operatorname{pgcd}(B, R).$$

Ce résultat débouche sur **l'algorithme d'Euclide** et **l'algorithme d'Euclide étendu** pour les polynômes, respectivement identiques à leurs homonymes pour les entiers.
Comme dans le cas des entiers, le lemme de Gauss pour les polynômes et la décomposition en facteurs irréductibles résultent du théorème de Bézout.

Théorème 4.12 (Lemme de Gauss) *(Cf. théorème 1.13 page 27) Soit A, B et C trois polynômes de $\mathbb{K}[X]$. Si A divise le produit BC et est premier avec B, A divise C.*

4.5 Décomposition d'un polynôme en facteurs irréductibles

L'énoncé suivant se déduit du théorème 4.7 (page 49) d'existence d'un facteur irréductible de la même façon que le Théorème fondamental de l'arithmétique (page 29) se déduit du théorème 1.6 (page 23).

Théorème 4.13 *(Cf. Théorème fondamental de l'arithmétique 1.20 page 29)*
Tout polynôme non nul $A \in \mathbb{K}[X]$ s'écrit d'une façon unique à une permutation près

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n},$$

où
$$\begin{cases} \lambda \in \mathbb{K}^*, \\ \text{les polynômes } P_i \text{ sont irréductibles, unitaires et tous distincts,} \\ \text{les entiers } \alpha_i \text{ sont positifs.} \end{cases}$$

Exercice 31 — Décomposer en facteurs irréductibles dans $\mathbb{F}_2[X]$ le polynôme

$$A = X^5 + X^4 + X^3 + X^2 + X + 1.$$

4.6 La $\mathbb{K}$-algèbre quotient $\mathbb{K}[X]/\langle P \rangle$

Soit $P \in \mathbb{K}[X]$ un polynôme non constant ($\deg(P) \geq 1$). Comme dans le cas de $\mathbb{Z}$, la relation d'équivalence **modulo** P est définie par

$$\forall (A, A') \in \mathbb{K}[X]^2, \quad (A \equiv A' \pmod{P}) \text{ si et seulement si } (A' - A \in \langle P \rangle). \tag{1}$$

Pour chaque polynôme $A \in \mathbb{K}[X]$, on désigne par $\overline{A}$ sa classe d'équivalence modulo P :

$$\overline{A} = \{A' \in \mathbb{K}[X] \mid A \equiv A' \pmod{P}\} = \{A + PQ \mid Q \in \mathbb{K}[X]\}.$$

On désigne par $\mathbb{K}[X]/\langle P \rangle$ l'ensemble quotient de $\mathbb{K}[X]$ par la relation d'équivalence (1), c'est-à-dire l'ensemble des classes modulo P.

Proposition 4.14 *(Cf. proposition 3.2 page 37) L'addition, la multiplication et la multiplication par un scalaire, définies sur l'ensemble quotient* $\mathbb{K}[X]/\langle P\rangle$ *par*

$$\forall (A,B)\in\mathbb{K}[X]^2,\qquad \begin{cases} \overline{A}+\overline{B} &= \overline{A+B},\\ \overline{A}\,\overline{B} &= \overline{AB},\\ \forall a\in\mathbb{K},\quad a\,\overline{A} &= \overline{aA}, \end{cases}$$

font de $\mathbb{K}[X]/\langle P\rangle$ *une* $\mathbb{K}$*-algèbre dans laquelle l'élément neutre de l'addition est* $\overline{0}$*, classe du polynôme* $0\in\mathbb{K}[X]$*, et l'élément neutre de la multiplication est* $\overline{1}$*, classe du polynôme* $1\in\mathbb{K}[X]$*.*

Théorème 4.15 *(Cf. théorème 3.3 page 37) Soit* $P\in\mathbb{K}[X]$ *un polynôme non constant.*
- *La classe* $\overline{A}\in\mathbb{K}[X]/\langle P\rangle$ *d'un polynôme* $A\in\mathbb{K}[X]$ *est inversible dans* $\mathbb{K}[X]/\langle P\rangle$ *si et seulement si* A *est premier avec* P*.*
- *Il en résulte que l'anneau* $\mathbb{K}[X]/\langle P\rangle$ *est un corps si et seulement si le polynôme* P *est irréductible dans* $\mathbb{K}[X]$*.*

4.7 Représentation de la $\mathbb{K}$-algèbre $\mathbb{K}[X]/\langle P\rangle$

Soit $q\in\mathbb{Z}$ et soit n un entier positif. On a vu que la façon la plus simple de décrire la classe $\overline{q}$ dans $\mathbb{Z}/n\mathbb{Z}$ consiste à écrire $\overline{q}=\overline{r}$, où r est le reste de la division euclidienne de q par n. On peut dire dans ce sens que l'entier $r\in\{0,1,\ldots,n-1\}$ *représente* la classe $\overline{q}$ modulo n.

On procède de la même façon dans l'anneau $\mathbb{K}[X]/\langle P\rangle$, grâce à la proposition suivante.

Proposition 4.16 *Soit* A *et* P *deux éléments de* $\mathbb{K}[X]$*, on suppose* $\deg(P)\geq 1$*. Le reste* R *de la division euclidienne de* A *par* P *est le seul polynôme de* $\mathbb{K}[X]$ *tel que*

$$\begin{cases} R\equiv A \pmod P,\\ \deg(R) < \deg(P). \end{cases}$$

Preuve : Il est clair que $R\equiv A \pmod P$.

L'unicité vient de ce que si $R'\equiv R \pmod P$ avec $\deg(R')<\deg(P)$, le polynôme $R'-R$ est divisible par P et $\deg(R'-R)<\deg(P)$, ce qui implique $R'-R=0$. □

Notation Pour chaque entier positif n, désignons par $\mathbb{K}[X]^{(n)}$ le sous-espace vectoriel de $\mathbb{K}[X]$ constitué des polynômes $Q\in\mathbb{K}[X]$ tels que $\deg(Q)<n$.

Dans ce qui suit, on pose $n=\deg(P)\geq 1$.

La proposition 4.16 énonce alors que pour tout $A\in\mathbb{K}[X]$, la classe $\overline{A}\in\mathbb{K}[X]/\langle P\rangle$ contient **un seul** polynôme appartenant à $\mathbb{K}[X]^{(n)}$, ce polynôme est le reste de la division euclidienne de A par P.

Dans la suite de ce chapitre, on désigne par α **la classe du polynôme** X **dans la** $\mathbb{K}$**-algèbre quotient** $\mathbb{K}[X]/\langle P\rangle$.

Pour chaque polynôme $A=a_0+a_1X+\cdots+a_kX^k\in\mathbb{K}[X]$, posons

$$A(\alpha)=a_0+a_1\alpha+\cdots+a_k\alpha^k\in\mathbb{K}[X]/\langle P\rangle,$$

de sorte que $A(\alpha)=\overline{A} \pmod P$, et qu'en particulier on a $P(\alpha)=0$. Cela permet d'écrire

$$\mathbb{K}[X]/\langle P\rangle=\{\overline{A}\,|\,A\in\mathbb{K}[X]\}=\{A(\alpha)\,|\,A\in\mathbb{K}[X]\}.$$

Soit $A=PQ+R$ la division euclidienne de A par P, de la relation $P(\alpha)=0$ il résulte que

$$A(\alpha)=R(\alpha).$$

On en déduit

$$\mathbb{K}[X]/\langle P\rangle = \{R(\alpha)\,|\,R\in\mathbb{K}[X]^{(n)}\} = \{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}\,|\,a_i\in\mathbb{K}\}. \tag{1}$$

De plus, il résulte de la proposition 4.16 que si R_1 et $R_2\in\mathbb{K}[X]^{(n)}$, on a l'équivalence

$$(R_1(\alpha)=R_2(\alpha))\Longleftrightarrow(R_1=R_2). \tag{2}$$

On déduit de (1) et (2) que la famille $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]/\langle P\rangle$. On a ainsi démontré l'important théorème suivant.

Théorème 4.17 *Soit $P\in\mathbb{K}[X]$ un polynôme de degré $n\geq 1$.*

1. *Tout élément $x\in\mathbb{K}[X]/\langle P\rangle$ s'écrit d'une façon et d'une seule sous la forme*
$$x=R(\alpha),\ \text{où } R\in\mathbb{K}[X]^{(n)}.$$
2. *En tant que $\mathbb{K}$-algèbre, $\mathbb{K}[X]/\langle P\rangle$ est un $\mathbb{K}$-espace vectoriel de dimension n et la famille*
$$\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$$
en constitue une base, qu'on appelle la ***base canonique*** *de $\mathbb{K}[X]/\langle P\rangle$.*

Exercice 32 — Montrer que le corps $\mathbb{C}$ des nombres complexes n'est autre que le corps quotient $\mathbb{R}[X]/\langle X^2+1\rangle$. A quoi correspond dans $\mathbb{C}$ la classe α de X dans $\mathbb{R}[X]/\langle X^2+1\rangle$? La base $\{1,\alpha\}$?

4.8 Règles de calculs dans $\mathbb{K}[X]/\langle P\rangle$

Sous les hypothèses du théorème 4.17 ci-dessus, chaque élément $x\in\mathbb{K}[X]/\langle P\rangle$ s'écrit de façon unique $x=R(\alpha)$, avec $R\in\mathbb{K}[X]^{(n)}$. L'addition ne pose pas de problème puisque la somme de deux polynômes de $\mathbb{K}[X]^{(n)}$ appartient à $\mathbb{K}[X]^{(n)}$. Pour la multiplication, on procède comme suit.

Règle de calcul pour la multiplication *Pour multiplier les deux éléments $R_1(\alpha)$ et $R_2(\alpha)$ dans $\mathbb{K}[X]/\langle P\rangle$, on calcule le reste R de la division euclidienne dans $\mathbb{K}[X]$ du polynôme produit R_1R_2 par P et on écrit*

$$R_1(\alpha)R_2(\alpha)=R(\alpha).$$

Exemple Supposons par exemple $\mathbb{K}=\mathbb{Q}$ et $P=X^3-X+1$.

$$\mathbb{Q}[X]/\langle P\rangle=\{a\alpha^2+b\alpha+c\,|\,a,b,c\in\mathbb{Q}\}.$$

Soit à effectuer le produit de $(\alpha^2+\alpha)$ par (α^2+1), on écrit

$$(\alpha^2+\alpha)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha^2+\alpha, \tag{1}$$

puis
$$X^4+X^3+X^2+X=(X^3-X+1)(X+1)+\underbrace{2X^2+X-1}_{R},$$

on en déduit
$$(\alpha^2+\alpha)(\alpha^2+1)=R(\alpha)=2\alpha^2+\alpha-1.$$

On peut aussi réduire l'expression obtenue dans (1) en utilisant la relation

$$P(\alpha)=\alpha^3-\alpha+1=0,$$

c'est-à-dire
$$\alpha^3=\alpha-1,$$

ce qui donne, en remplaçant autant de fois qu'il le faut α^3 par $\alpha-1$,

$$(\alpha^2+\alpha)(\alpha^2+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha(\alpha-1)+\alpha-1+\alpha^2+\alpha=2\alpha^2+\alpha-1.$$

Chapitre 5

Corps finis

Pour chaque nombre premier p, nous connaissons déjà le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ à p éléments.
Nous allons voir comment, à partir des corps $\mathbb{F}_p$, appelés **corps premiers**, on peut construire d'autres corps finis, et nous en étudierons les principales propriétés.
Nous admettrons le résultat suivant.

Théorème 5.1 (Wedderburn 1882-1948) *Tout corps fini est commutatif.*

Rappelons d'autre part que deux corps $\mathbb{K}$ et $\mathbb{K}'$ sont **isomorphes** s'il existe un **isomorphisme de corps** u de $\mathbb{K}$ sur $\mathbb{K}'$, c'est-à-dire une application bijective u de $\mathbb{K}$ sur $\mathbb{K}'$ vérifiant

$$\forall(x,\ y) \in \mathbb{K}^2, \quad u(x+y) = u(x) + u(y) \quad \text{et} \quad u(xy) = u(x)u(y).$$

Un **automorphisme** d'un corps $\mathbb{K}$ est un isomorphisme de $\mathbb{K}$ sur lui-même.

Lemme 5.2 *Soit $\mathbb{K}$ un corps fini et $\mathbb{L}$ un sous-corps de $\mathbb{K}$. Alors $\mathbb{K}$ est un espace vectoriel de dimension finie n sur $\mathbb{L}$, ce qui implique que $\mathbb{K}$ possède $(\#\mathbb{L})^n$ éléments.*

Preuve : On a vu, (proposition 0.19 page 16) que $\mathbb{K}$ est un espace vectoriel sur $\mathbb{L}$. Cet espace vectoriel est nécessairement de dimension finie puisque $\mathbb{K}$ est fini. Soit n cette dimension, on sait qu'il existe une base $\{b_1, b_2, \ldots, b_n\}$ de $\mathbb{K}$ sur $\mathbb{L}$. Tout élément $x \in \mathbb{K}$ s'écrit de façon unique

$$x = \alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n, \quad \alpha_i \in \mathbb{L}$$

et chaque α_i, pour $i = 1, 2, \ldots, n$, peut prendre $\#\mathbb{L}$ valeurs distinctes. □

5.1 Exemple d'un corps à 4 éléments

Soit $P = X^2 + X + 1$ le seul polynôme irréductible de degré 2 de l'algèbre $\mathbb{F}_2[X]$.
On sait, (théorème 4.15 page 52), que $\mathbb{F}_2[X]/\langle P\rangle$ est un corps et que si α désigne la classe d'équivalence du polynôme X dans $\mathbb{F}_2[X]/\langle P\rangle$, alors, (théorème 4.17 page 53),

$$\mathbb{F}_2[X]/\langle P\rangle = \{a + b\alpha \,|\, a,\ b \in \mathbb{F}_2\} = \{0,\ 1,\ \alpha,\ 1+\alpha\}.$$

La table de multiplication de $\mathbb{F}_2[X]/\langle P\rangle$ s'écrit, compte tenu de l'égalité $P(\alpha) = 0$, c'est-à-dire $\alpha^2 = 1 + \alpha$,

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

On y voit par exemple que l'inverse de α est $(1 + \alpha)$.

5.2 Construction des corps finis

Nous admettrons le résultat suivant, qui est démontré dans la section facultative 5.7 page 62.

Théorème 5.3 *Pour tout nombre premier p et tout entier positif n, il existe un polynôme irréductible de degré n dans l'anneau $\mathbb{F}_p[X]$.*

On en déduit, pour tout nombre premier p et tout entier positif n, l'existence d'un corps à p^n éléments. Le théorème suivant, reprenant le théorème 4.17 (page 53), décrit ce corps.

Théorème 5.4 (Existence de corps finis) *Soit n un entier positif et soit p un nombre premier, il existe un corps à p^n éléments. Plus précisément, soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n et soit $\mathbb{K}$ le corps $\mathbb{F}_p[X]/\langle P\rangle$, on désigne par α la classe d'équivalence du polynôme X dans $\mathbb{K}$.*

1. *Le corps $\mathbb{K}$ est constitué des éléments de la forme $R(\alpha)$, où R décrit l'espace vectoriel $\mathbb{F}_p[X]^{(n)}$ des polynômes de degré $\leq n-1$ de $\mathbb{F}_p[X]$.*
2. *Si $\beta \in \mathbb{K}$, il existe **un seul** polynôme $R \in \mathbb{F}_p[X]^{(n)}$ tel que $\beta = R(\alpha)$.*
3. *La famille $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ est une base de l'espace vectoriel $\mathbb{K}$ sur $\mathbb{F}_p$.*
4. *$\#\mathbb{K} = p^n$.*

Preuve :

1. 2. et 3. résultent du théorème 4.17 (page 53).
4. Résulte de 3, (cf. démonstration du lemme 5.2 page 55). □

5.3 Élément primitif

La propriété suivante des corps finis joue un rôle important en cryptographie ainsi que pour la construction de certains codes correcteurs d'erreurs.

Théorème 5.5 *Si $\mathbb{K}$ est un corps fini, le groupe multiplicatif $\mathbb{K}^*$ est cyclique.*

Preuve : Soit d un diviseur de l'ordre du groupe $\mathbb{K}^*$. L'ensemble $U_d = \{x \in \mathbb{K}^* \mid x^d = 1\}$ coïncide avec l'ensemble des racines distinctes du polynôme $X^d - 1$. On déduit du théorème 4.5 (page 48) que $\#U_d \leq d$, puis on applique le théorème 2.20 (page 36). □

Il en résulte que si $\mathbb{K}$ est un corps à q éléments, le groupe cyclique $\mathbb{K}^*$, d'ordre $q-1$, possède $\varphi(q-1)$ générateurs. Ces générateurs du groupe $\mathbb{K}^*$ sont appelés **éléments primitifs** de $\mathbb{K}$.

L'importance d'un élément primitif $a \in \mathbb{K}^*$ tient au fait qu'on peut décrire tous les éléments du groupe $\mathbb{K}^*$ en termes des $(q-1)$ premières puissances positives de a.

Cela *implique* que si un sous-corps $\mathbb{L}$ de $\mathbb{K}$ contient un élément primitif a, alors $\mathbb{L} = \mathbb{K}$. C'est par cette dernière propriété qu'on définit un élément primitif dans la plupart des traités d'algèbre, définition *qui n'est pas équivalente* à celle donnée ici, qui est propre aux "codeurs" et aux cryptographes. Ce que nous appelons ici élément primitif est appelé par les algébristes "racine primitive de l'unité".

Pour la non équivalence des deux définitions, voir l'exemple du corps construit en 5.5 page 59.

Exercice 33 — Déterminer les éléments primitifs du corps construit en 5.1 (page 55).

5.4 Caractéristique d'un corps fini

Soit $\mathbb{K}$ un corps fini d'élément unité 1, et soit $\psi : \mathbb{Z} \mapsto \mathbb{K}$ le morphisme de groupes défini par

$$\forall n \in \mathbb{Z} \qquad \psi(n) = n.1.$$

Le corps $\mathbb{K}$ étant fini, l'application ψ ne peut être injective, elle n'est pas non plus identiquement nulle. Son noyau est donc un sous-groupe non trivial de $\mathbb{Z}$, de la forme $p\mathbb{Z}$, avec $p \geq 2$.
L'entier p est le plus petit entier positif tel que $p.1 = 0$, supposons $p = p_1 p_2$, avec $1 < p_1 < p$, on aurait alors $0 = p.1 = (p_1.1)(p_2.1)$, avec $p_1.1 \neq 0$ et $p_2.1 \neq 0$, ce qui est impossible puisque $\mathbb{K}$ est intègre. L'entier p est donc premier.
Ce nombre premier p est appelé la **caractéristique** du corps $\mathbb{K}$.
Si $\mathbb{K}$ est un corps de caractéristique p, tout sous-corps de $\mathbb{K}$ contient l'unité 1, donc contient $\psi(\mathbb{Z})$, donc est de caractéristique p.

Proposition 5.6 *Soit $\mathbb{K}$ un corps fini de caractéristique p et d'élément unité 1. L'ensemble $\mathbb{L} = \psi(\mathbb{Z}) = \{n.1 \,|\, n \in \mathbb{Z}\}$ est un sous-corps de $\mathbb{K}$, isomorphe à $\mathbb{F}_p$.*

Preuve : On vérifie facilement que $\mathbb{L}$ est un anneau. Par définition de p, on a $(m.1 = n.1)$ si et seulement si $(m - n) \in p\mathbb{Z}$, on en déduit que $\mathbb{L} = \{0, 1, 2.1, \ldots, (p-1).1\}$.
On définit une bijection u de $\mathbb{L}$ sur $\mathbb{F}_p$ en posant, pour chaque $n \in \{0, 1, \ldots, p-1\}$,

$$u(n.1) = \overline{n} \in \mathbb{F}_p.$$

On vérifie facilement que, pour tout $(x, y) \in \mathbb{L}^2$

$$\begin{cases} u(x+y) & = & u(x) + u(y) \\ u(x\,y) & = & u(x)\,u(y) \end{cases}$$

Il en résulte que u est un isomorphisme d'anneaux. L'anneau $\mathbb{F}_p$ étant un corps, il en est donc de même de l'anneau $\mathbb{L}$. □

Soit $\mathbb{K}$ un corps fini de caractéristique p, on identifie le corps $\mathbb{F}_p$ au sous-corps de $\mathbb{K}$ défini par

$$\mathbb{L} = \{0, 1, 2.1, \ldots, (p-1).1\}.$$

Il en résulte que $\mathbb{K}$, ainsi que tous ses sous-corps, admettent $\mathbb{F}_p$ comme sous-corps.
Cela justifie l'appellation de corps *premier* pour $\mathbb{F}_p$.
Réciproquement, tout corps fini contenant le corps $\mathbb{F}_p$ est de caractéristique p, en particulier les corps $\mathbb{K} = \mathbb{F}_p[X]/\langle P \rangle$ décrits en section 5.2, et le corps $\mathbb{F}_p$ lui-même.
La proposition suivante donne des **règles de calcul** dans un corps fini de caractéristique p.

Proposition 5.7 *Soit $\mathbb{K}$ un corps fini de caractéristique p.*

1. $\forall (x, y) \in \mathbb{K}^2$, $(x + y)^p = x^p + y^p$.
2. $\forall (x, y) \in \mathbb{K}^2$, $\forall i \geq 2$, $(x + y)^{p^i} = x^{p^i} + y^{p^i}$.
3. $\mathbb{F}_p = \{x \in \mathbb{K} \,|\, x = x^p\}$.
4. *Soit $Q \in \mathbb{K}[X]$, on a l'équivalence*

$$(Q \in \mathbb{F}_p[X]) \iff ([Q(X)]^p = Q(X^p)).$$

Preuve :

1. On développe $(x+y)^p$ par la formule du binôme de Newton, puis on remarque que pour tout entier $k = 1, \ldots, p-1$, le coefficient binomial $\mathcal{C}_k^p$ est divisible par p, (proposition 1.15 page 28), donc est nul dans $\mathbb{F}_p$.
2. Par récurrence sur i à partir de la question précédente.
3. Le groupe $\mathbb{F}_p^*$ est d'ordre $p-1$, tout élément $x \in \mathbb{F}_p^*$ vérifie donc $x^{p-1} = 1$, d'où $x^p = x$, relation aussi vérifiée par 0, donc $\mathbb{F}_p \subseteq \{x \in \mathbb{K} \,|\, x = x^p\}$.

   Réciproquement, le polynôme $X^p - X$ possédant au plus p racines dans $\mathbb{K}$, (théorème 4.5 page 48), on a l'inégalité $\#\{x \in \mathbb{K} \,|\, x = x^p\} \leq p$, d'où l'égalité $\mathbb{F}_p = \{x \in \mathbb{K} \,|\, x = x^p\}$.
4. Soit $Q(X) = a_0 + a_1 X + \cdots + a_n X^n$. D'après 1. on a $[Q(X)]^p = a_0^p + a_1^p X^p + \cdots + a_n^p (X^p)^n$, le résultat découle alors de 3. ci-dessus. □

Exercice 34 — Soit $\mathbb{K}$ un corps fini de caractéristique p. Montrer que l'application u de $\mathbb{K}$ dans lui-même définie par $u(x) = x^p$ est un automorphisme de $\mathbb{K}$, c'est-à-dire un isomorphisme de corps de $\mathbb{K}$ dans lui-même.

Le théorème qui suit nous permettra d'effectuer des calculs pratiques dans un corps fini.

Théorème 5.8 *Soit $\mathbb{K}$ un corps fini à q éléments, de caractéristique p.*

1. *Si n est la dimension de l'espace vectoriel $\mathbb{K}$ sur $\mathbb{F}_p$, on a $q = p^n$.*
2. *Tout $x \in \mathbb{K}^*$ vérifie $x^{q-1} = 1$, ce qui implique $x^{-1} = x^{q-2}$.*
3. *Tout $x \in \mathbb{K}$ vérifie $x^q = x$.*
4. *Dans l'anneau $\mathbb{K}[X]$, on a l'égalité*

$$X^{q-1} - 1 = \prod_{a \in \mathbb{K}^*} (X - a).$$

5. *Soit a un élément primitif de $\mathbb{K}$. La famille*

$$\mathcal{B} = \{1, a, a^2, \ldots, a^{n-1}\}$$

est une base de l'espace vectoriel $\mathbb{K}$ sur $\mathbb{F}_p$, c'est-à-dire que tout élément $x \in \mathbb{K}$ s'écrit d'une façon unique

$$x = R(a), \quad \text{avec} \quad R \in \mathbb{F}_p[X]^{(n)}.$$

Preuve :

1. Conséquence du lemme 5.2 (page 55).
2. et 3. Le groupe $\mathbb{K}^*$ est d'ordre $q-1$ donc tout $x \in \mathbb{K}^*$ vérifie $x^{q-1} = 1 = x\, x^{q-2}$, d'où $x^q = x$, relation qui est aussi vérifiée par 0.
4. Résulte de 2. et du théorème 4.5 page 48.
5. Le corps $\mathbb{K}$ étant un espace vectoriel de dimension n sur $\mathbb{F}_p$, il suffit de montrer que la famille $\mathcal{B} = \{1, a, a^2, \ldots, a^{n-1}\}$ est libre.

   Supposons le contraire, une relation linéaire non identiquement nulle entre les a^i équivaut à l'existence d'un polynôme non constant $P \in \mathbb{F}_p[X]^{(n)}$ tel que $P(a) = 0$.

   Soit B le sous $\mathbb{F}_p$-espace vectoriel de $\mathbb{K}$ engendré par la famille $\mathcal{B}$. D'après notre hypothèse, $\dim(B) < n$ donc B est strictement inclus dans $\mathbb{K}$. On en déduit que $B \backslash \{0\}$ est strictement inclus dans $\mathbb{K}^*$.

   Si on montre que B est un anneau, comme $B \setminus \{0\}$ contient a, $B \setminus \{0\}$ contiendra toutes les puissances positives de a et cela prouvera que a n'est pas un générateur de $\mathbb{K}^*$.

Par définition de B, on peut écrire

$$B = \{R(a) \,|\, R \in \mathbb{F}_p[X]^{(n)}\}. \tag{1}$$

Soit $A = \{Q(a) \,|\, Q \in \mathbb{F}_p[X]\}$, montrons que $B = A$, ce qui prouvera que B est un anneau. Or il résulte de (1) que $B \subseteq A$. Réciproquement, soit $Q \in \mathbb{F}_p[X]$, et soit $Q = PQ_1 + R_1$, avec $R_1 \in \mathbb{F}_p[X]^{(n)}$, la division euclidienne de Q par P, on a d'une part $Q(a) = R_1(a)$ puisque $P(a) = 0$, et d'autre part $R_1(a) \in B$ puisque $R_1 \in \mathbb{F}_p[X]^{(n)}$, ce qui prouve que $A \subseteq B$ et l'égalité. □

Exercice 35 — Montrer que deux corps finis ayant même nombre d'éléments ont même caractéristique.

5.5 Calculs dans un corps fini - Table de logarithmes

Le théorème 5.8 (page 58) fournit un moyen efficace pour effectuer des calculs dans un corps fini $\mathbb{K}$ de caractéristique p, si on en connaît un élément primitif a.
Soit $q = p^n$ le nombre d'éléments de $\mathbb{K}$. On sait en effet que chaque élément de $x \in \mathbb{K}^*$ s'écrit de façon unique sous chacune des deux formes suivantes :

(1) $x = R(a)$, où $R \in \mathbb{F}_p[X]^{(n)}$. On sait additionner deux éléments donnés sous cette forme.

(2) $x = a^i$, où $i \in \{0, 1, 2, \ldots, q-2\}$. La multiplication de deux éléments donnés sous cette forme s'effectue en additionnant les exposants modulo $(q-1)$.

La question est de pouvoir passer de la première à la seconde forme et réciproquement, c'est-à-dire d'établir la **table des logarithmes de base** a.
Le plus instructif est de donner un exemple.
On sait que le polynôme $P = X^2 + 1$ est irréductible dans $\mathbb{F}_3[X]$.
Le corps $\mathbb{K} = \mathbb{F}_3[X]/\langle P\rangle$ possède 9 éléments, le groupe $\mathbb{K}^*$ est d'ordre 8.
La classe α de X dans $\mathbb{K}$ vérifie $P(\alpha) = \alpha^2 + 1 = 0$, c'est-à-dire $\alpha^2 = -1 = 2$.
On voit que α n'est pas un élément primitif puisque $\alpha^4 = 1$ (remarquons qu'au sens des traités d'algèbre, au sens des générateur de $\mathbb{K}$ sur $\mathbb{F}_p$, α est un élément primitif d'après le théorème 5.4 page 56.)
Par contre, l'élément $a = \alpha + 2$ est primitif puisque $a^2 = \alpha^2 + 4\alpha + 4 = 2 + \alpha + 1 = \alpha$, et que $a^4 = \alpha^2 = -1$. Remarquons que a vérifie la relation

$$a^2 = 1 + a,$$

relation qu'on utilisera pour le calcul des puissances successives de a dans la base $\{1, a\}$ de $\mathbb{K}$.
La table de logarithmes de base a s'écrit :

$$\begin{cases} a^0 &= 1, \\ a^1 &= a, \\ a^2 &= 1+a, \\ a^3 &= 1+2\,a, \\ a^4 &= 2, \\ a^5 &= 2\,a, \\ a^6 &= 2+2\,a, \\ a^7 &= 2+a, \end{cases} \quad \text{c'est-à-dire} \quad \begin{cases} \log_a(1) &= 0, \\ \log_a(a) &= 1, \\ \log_a(1+a) &= 2, \\ \log_a(1+2\,a) &= 3, \\ \log_a(2) &= 4, \\ \log_a(2\,a) &= 5, \\ \log_a(2+2\,a) &= 6, \\ \log_a(2+a) &= 7. \end{cases}$$

Connaissant la table des logarithmes de base a, **multiplier** entre eux deux éléments donnés sous la forme (1) revient à effectuer une *addition modulo* 8. Par exemple, pour calculer le produit $(2+a)(2+2a)$, on consulte la table de logarithmes, on y trouve $2+a=a^7$ et $2+2a=a^6$, d'où

$$(2+a)(2+2a) = a^{7+6} = a^{13} = a^5 = 2a.$$

Additionner deux éléments donnés sous la forme (2) se fait de façon symétrique, par exemple

$$a^3 + a^2 = (1+2a) + (1+a) = 2 = a^4.$$

Inverser un élément $x \neq 0$ donné sous la forme (1) est aussi automatique, compte tenu de ce que sous la forme (2), on a $(a^k)^{-1} = a^{8-k}$. Par exemple

$$(1+2a)^{-1} = (a^3)^{-1} = a^{8-3} = a^5 = 2a.$$

Remarquons que dans un corps $\mathbb{K}$ à q éléments, on peut toujours, en l'absence de table de logarithmes, écrire que $x^{-1} = x^{q-2}$ puisque $x^{q-1} = 1$.

Dans un corps de très grande taille, d'élément primitif a, il existe des méthodes rapides, étant donné un entier $m \geq 2$, pour calculer l'élément a^m. Mais il est beaucoup plus difficile, en l'absence de table de logarithmes, d'effectuer le calcul inverse : connaissant $x \in \mathbb{K}$ sous la forme (1), déterminer l'entier $m = \log_a(x)$ tel que $x = a^m$.

Ce problème est connu sous le nom de **problème du logarithme discret** (ce logarithme ne prenant que des valeurs entières).

Certains algorithmes de cryptographie sont basés sur la difficulté à résoudre le problème du logarithme discret.

Exercice 36 — Déterminer tous les éléments primitifs du corps $\mathbb{K}$ défini ci-dessus.

5.6 Applications à la cryptographie

5.6.1 Protocole d'échange de clés de Diffie-Hellman

Le problème ici est lié à la génération de clés. Il s'agit pour deux personnes d'obtenir une clé qu'ils seront les seuls à posséder, clé qui leur servira à chiffrer leur correspondance en utilisant un chiffrement à clé secrète.

Ce protocole est basé sur la difficulté à résoudre le problème du logarithme discret dans des corps de grande taille lorsque certaines conditions sont remplies.

Le protocole d'échange de clés de Diffie-Hellman permet, à partir d'une clé publique, à deux personnes désirant communiquer secrètement, de se fabriquer une clé secrète.

Soit $\mathbb{F}_q$ un corps à q éléments dans lequel le problème du logarithme discret est difficile, et soit g un élément primitif de $\mathbb{F}_q$, le couple $(\mathbb{F}_q, g)$ est public.

Voici le protocole que doivent suivre Alice et Bernard pour se confectionner une clé secrète au vu et au su de tout le monde :

- Alice choisit un entier a vérifiant $1 < a < q-1$ et transmet sa clé publique g^a à Bernard.
- Bernard choisit un entier b vérifiant $1 < b < q-1$ et transmet sa clé publique g^b à Alice.
- Alice élève g^b à la puissance a, obtenant $\gamma = g^{ab}$.
- Bernard élève g^a à la puissance b, obtenant $\gamma = g^{ab}$, qui sera leur clé secrète commune.

Alice et Bernard sont les seuls à connaître γ car Eve peut intercepter g^a et g^b mais ne peut en déduire $\gamma = g^{ab}$ qu'en connaissant a ou b, c'est-à-dire en ayant résolu le problème du logarithme discret de base g dans $\mathbb{F}_q$.

Vulnérabilité du protocole de Diffie-Hellman - Nécessité d'une signature

Le protocole de Diffie-Hellman est vulnérable à l'attaque suivante : Eve choisit un entier c tel que $1 < c < q-1$ et calcule g^c. Elle intercepte la clé publique g^a envoyée par Alice à Bernard, lui substitue la clé g^c qu'elle envoie à Bernard, lequel croit recevoir la clé publique d'Alice.

Lorsque Bernard envoie à Alice sa clé publique g^b, Eve l'intercepte et envoie g^c à Alice.

La clé "secrète" d'Alice est donc $\alpha = g^{ac}$ et celle de Bernard $\beta = g^{bc}$, Eve les connaît puisque qu'il lui suffit d'élever chacune des clés publiques d'Alice et Bernard à la puissance c.

Eve intercepte alors tous les messages d'Alice à Bernard, est capable de les déchiffrer, de les modifier avec la clé α puis de les envoyer à Bernard en les chiffrant avec la clé β.

Elle procède de même avec les messages envoyés par Bernard à Alice, qu'elle déchiffre avec la clé β et renvoie à Alice en les rechiffrant à l'aide de la clé α.

La vulnérabilité du protocole de Diffie-Hellman réside dans le fait qu'il ne permet pas d'authentifier les participants.

5.6.2 Algorithme de chiffrement à clé publique d'El Gamal

C'est un exemple de chiffrement à clé publique basé sur le problème du logarithme discret.

Soit $\mathbb{F}_q$ une corps à q éléments et soit g un élément primitif de $\mathbb{F}_q$. On suppose que le problème du logarithme discret de base g dans $\mathbb{F}_q$ est difficile. Le **couple** $(\mathbb{F}_q, g)$ **est public**. Rappelons que pour tout $x \in \mathbb{F}_q$, on a $x^{-1} = x^{q-2}$ puisque $x^{q-1} = 1$.

L'encodage consiste à assigner à chaque élément de message un élément de $\mathbb{F}_q^*$ de façon injective.

- **Clé secrète, clé publique** Si Bernard veut permettre à un tiers de lui envoyer des messages secrets, il choisit un entier a tel que $1 < a < q$, qui sera sa **clé secrète**. Il calcule $\alpha = g^a$, qu'il publie, et qui sera sa **clé publique**.
- **Encryptage** Pour envoyer à Bernard le message $m \in \mathbb{F}_q$, Alice **choisit aléatoirement** un entier x tel que $1 < x < q$, et lui transmet le couple

$$(\beta, \gamma) = (g^x, m\,\alpha^x) = (g^x, m\,g^{ax})$$

  qui est le message crypté ou chiffré.
- **Décryptage** Bernard, grâce à sa clé secrète a, peut calculer l'inverse $\delta = g^{-ax}$ de g^{ax}, en effet

$$\delta = g^{-ax} = g^{ax(q-2)} = (g^x)^{a(q-2)} = \beta^{a(q-2)},$$

  il en déduit $$m = (m\,g^{ax})\,g^{-ax} = \gamma\,\delta.$$

Comme l'algorithme RSA, cet algorithme est **asymétrique**.

L'introduction de l'aléa x est un avantage au sens où le même message envoyé plusieurs fois ne sera pas codé de la même façon à chaque fois.

Signature d'El Gamal (♮)

La signature d'El Gamal équipe le logiciel *GNU Privacy Guard (GPG)* qui est une déclinaison libre du logiciel de cryptage PGP. Les signatures de ce type, dites **signatures numériques**, ont valeur légale en France depuis le mois de mars 2000.

On considère un corps premier $\mathbb{F}_p$ et un élément primitif g de $\mathbb{F}_p$. On identifie chaque élément de $\mathbb{F}_p$ à un entier compris entre 0 et $p-1$. Les entiers p et g sont choisis de telle sorte que le problème du logarithme discret de base g soit difficile à résoudre dans $\mathbb{F}_p$. Le couple $(\mathbb{F}_p, g)$ est public.

- **Signature** Soit a_1 la clé secrète d'Alice et $\alpha_1 = g^{a_1}$ sa clé publique. Pour signer le message m, elle procède comme suit.
  - Elle **choisit aléatoirement** un entier positif e premier avec $p-1$ et calcule son inverse d modulo $p-1$.
  - Elle calcule l'entier $s_1 = g^e \pmod p$ et l'entier $s_2 = d(m - a_1 s_1)$, c'est-à-dire tel que

    $$m = es_2 + a_1 s_1 \pmod{p-1}. \tag{1}$$

  - Le message signé est le triplet (m, s_1, s_2).
- **Vérification** Recevant le triplet (m, s_1, s_2), Bernard calcule $s_1^{s_2}\ \alpha_1^{s_1}$ et vérifie l'égalité suivante dans $\mathbb{F}_p$

  $$g^m = \alpha_1^{s_1}\ s_1^{s_2}, \tag{2}$$

  qui résulte de l'égalité (1) puisque $g^m = g^{es_2 + a_1 s_1} = a_1^{s_2}\alpha_1^{s_1}$.
- **Justification** Étant donné que Bernard connaît la clé publique α_1 d'Alice, pour authentifier son message, celle-ci doit prouver à Bernard qu'elle connaît l'entier $a_1 = \log_g(\alpha_1)$ qui est sa clé secrète. La façon la plus simple serait de lui communiquer a_1, ce qui constituerait une signature mais obligerait Alice à changer de clé, celle-ci n'étant plus secrète.

  C'est ce qui se passerait si elle avait choisi $e = d = 1$, puisqu'à ce moment là, on aurait $s_1 = g$ et $s_2 = m - a_1$, d'où on déduit immédiatement a_1. L'entier e est donc une clé secrète destinée à protéger la clé secrète a_1. Connaissant $s_1 = g^e$, Eve ne peut en déduire e, donc d. Connaissant $s_2 = d(m - a_1 s_1)$, elle ne peut donc en déduire a_1.

  Mais comment l'égalité (2) peut-elle prouver à Bernard qu'Alice connaît a_1 ?

  Remarquons que (2) équivaut à l'égalité (1) des logarithmes de base g :

  $$m = es_2 + a_1 s_1 \pmod{p-1}.$$

  Il en résulte qu'Alice, connaissant s_1, s_2, e et m, connaît nécessairement a_1.

  Eve, ne connaissant que s_1 sans connaître e, et ignorant a_1, ne peut pas déterminer d'entier s_2 vérifiant (1), même si elle connaît m ou $m - a_1 s_1$.

  Des aléas e différents sont utilisés pour deux signatures consécutives.

5.7 Compléments facultatifs sur les corps finis (♮)

5.7.1 Structure générale d'un corps fini

Nous utiliserons le résultat d'arithmétique élémentaire suivant.

Lemme 5.9 *Soit a, m et n trois entiers positifs, avec $a \geq 2$. Alors*

$$(a^m - 1) \textit{ divise } (a^n - 1) \textit{ si et seulement si } m \textit{ divise } n.$$

Preuve : Si m divise n, on pose $n = mq$ et on écrit

$$a^n - 1 = a^{mq} - 1 = (a^m)^q - 1 = (a^m - 1)(a^{m(q-1)} + a^{m(q-2)} + \cdots + 1) = (a^m - 1)\, b.$$

Dans le cas général, la division euclidienne de n par m s'écrit $n = mq + r$, $0 \leq r < m$, d'où

$$a^n - 1 = a^{mq+r} - 1 = (a^{mq} - 1)a^r + (a^r - 1) = (a^m - 1)ba^r + (a^r - 1),$$

comme $(a^r - 1) < (a^m - 1)$, le reste de la division euclidienne de $(a^n - 1)$ par $(a^m - 1)$ est $(a^r - 1)$, ce qui démontre le lemme. □

La structure générale d'un corps fini de caractéristique p est décrite par le théorème suivant.

Théorème 5.10 *Soit $\mathbb{K}$ un corps de caractéristique p, à $q = p^n$ éléments.*

1. *Le nombre d'éléments de tout sous-corps de $\mathbb{K}$ est de la forme p^r, où r divise n.*
2. *Réciproquement, pour tout diviseur r de n, $\mathbb{K}$ possède un unique sous-corps à p^r éléments, c'est l'ensemble des $a \in \mathbb{K}$ vérifiant $a^{p^r} = a$.*

Preuve :

1. Le nombre d'éléments d'un sous-corps $\mathbb{L}$ de $\mathbb{K}$ est de la forme p^r d'après le théorème 5.8 (page 58). D'après le lemme 5.2 (page 55), p^n est une puissance de p^r donc r divise n.
2. Soit r un diviseur de n. Le groupe multiplicatif $\mathbb{K}^*$ est cyclique d'ordre $p^n - 1$, et $(p^r - 1)$ divise $(p^n - 1)$ d'après le lemme 5.9 ci-dessus. Il résulte alors du théorème 2.18 (page 35) que les éléments de $\mathbb{K}^*$ vérifiant $a^{p^r-1} = 1$ forment un sous-groupe d'ordre $(p^r - 1)$ de $\mathbb{K}^*$. En ajoutant 0, on en déduit que l'ensemble $\mathbb{L} = \{a \in \mathbb{K} \,|\, a^{p^r} = a\}$ possède p^r éléments. Comme $\mathbb{L} \setminus \{0\}$ est un groupe multiplicatif, il reste à montrer que $\mathbb{L}$ est un groupe additif, or $\mathbb{L}$ est stable pour l'addition d'après le point 2 de la proposition 5.7 (page 57), et $0 \in \mathbb{L}$. Soit $a \in \mathbb{L}$, montrons que $-a \in \mathbb{L}$.
   – Si $p = 2$, on a $-a = a$ donc $-a \in \mathbb{L}$.
   – Si $p > 2$, p^r est impair donc $(-a)^{p^r} = -a^{p^r} = -a$, c'est-à-dire $-a \in \mathbb{L}$.
   Ainsi $\mathbb{L}$ est bien un corps. L'unicité vient du fait que si $\mathbb{L}_1$ est un sous-corps à p^r éléments de $\mathbb{K}$, le groupe $\mathbb{L}_1^*$ est d'ordre $(p^r - 1)$ donc tout élément $a \in \mathbb{L}_1$ vérifie $a^{p^r} = a$, ce qui fait que $\mathbb{L}_1 \subset \mathbb{L}$ donc $\mathbb{L}_1 = \mathbb{L}$. □

5.7.2 Polynôme minimal

Soit $\mathbb{K}$ un corps de caractéristique p, à $q = p^n$ éléments, et soit $a \in \mathbb{K}$. Il est facile de voir que l'ensemble

$$\mathcal{I} = \{Q \in \mathbb{F}_p[X] \,|\, Q(a) = 0\}$$

est un idéal de $\mathbb{F}_p[X]$. Le polynôme $\Pi = X^q - X$ appartient à $\mathbb{F}_p[X]$, et $\Pi(a) = 0$ d'après le théorème 5.10 (page 63), ce qui fait que $\Pi \in \mathcal{I}$ donc $\mathcal{I} \neq \{0\}$.

Il existe d'après le théorème 4.6 (page 49) un polynôme unitaire unique $P \in \mathbb{F}_p[X]$ tel que $\mathcal{I} = \langle P \rangle$. On rappelle que P est le polynôme unitaire de degré minimum de $\mathcal{I}$.

Le polynôme P est appelé **polynôme minimal de a sur le corps $\mathbb{F}_p$**, ou simplement polynôme minimal de a, son degré d est appelé **degré algébrique** de a sur $\mathbb{F}_p$.

Le polynôme P est **irréductible** dans $\mathbb{F}_p[X]$ puisque $\mathbb{K}$ est intègre.

> **Exercice 37** — Soit $\mathbb{K}$ un corps fini de caractéristique p et soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible unitaire. Montrer que si P possède une racine $a \in \mathbb{K}$, alors P est le polynôme minimal de a. En déduire la proposition suivante.

Proposition 5.11 *Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible unitaire, si α désigne la classe de X dans le corps $\mathbb{F}_p[X]/\langle P \rangle$, alors P est le polynôme minimal de α.*

Soit $\mathbb{K}$ un corps fini et soit $a \in \mathbb{K}^*$. Désignons par $\mathbb{F}_p(a)$ **le plus petit** sous-corps de $\mathbb{K}$ contenant a, ou **sous-corps engendré** par a. (La notation $\mathbb{F}_p(a)$ rappelle que ce sous-corps contient le corps premier $\mathbb{F}_p$.) Le corps $\mathbb{F}_p(a)$ est décrit par le théorème suivant.

Théorème 5.12 *Soit $\mathbb{K}$ un corps fini de caractéristique p, soit $a \in \mathbb{K}^*$ un élément de degré algébrique $r \geq 1$, et soit P le polynôme minimal de a.*

1. *Le corps $\mathbb{F}_p(a)$ est constitué de l'ensemble des éléments de $\mathbb{K}$ de la forme $Q(a)$, où Q décrit l'anneau $\mathbb{F}_p[X]$.*

2. *La famille* $\{1, a, a^2, \ldots, a^{r-1}\}$ *est une base de l'espace vectoriel* $\mathbb{F}_p(a)$ *sur* $\mathbb{F}_p$*, c'est-à-dire que tout élément* $x \in \mathbb{F}_p(a)$ *s'écrit d'une manière et d'une seule*

$$x = R(a), \quad \textit{avec} \quad R \in \mathbb{F}_p^{(r)}[X].$$

3. $\#\mathbb{F}_p(a) = p^r$.
4. *Il existe un isomorphisme de corps* ψ *de* $\mathbb{F}_p(a)$ *sur* $\mathbb{F}_p[X]/\langle P\rangle$ *tel que* $\psi(a) = \overline{X}$.

Preuve :

1. Soit A l'ensemble des éléments de $\mathbb{K}$ de la forme $Q(a)$, où Q décrit $\mathbb{F}_p[X]$. On vérifie aisément que $a \in A$ et que A est un anneau contenu dans $\mathbb{F}_p(a)$.
   Si on montre que A est un corps, l'égalité $A = \mathbb{F}_p(a)$ résultera de la définition de $\mathbb{F}_p(a)$.
   Soit $x = Q(a)$ un élément non nul de A, montrons que $x^{-1} \in A$.
   Comme $Q(a) \neq 0$, Q n'est pas multiple de P, donc $\operatorname{pgcd}(P, Q) = 1$ dans $\mathbb{F}_p[X]$ puisque P est irréductible. Il résulte du théorème de Bézout qu'il existe deux polynômes U et V de $\mathbb{F}_p[X]$ tels que $PU + QV = 1$, ce qui donne $Q(a)V(a) = x\,V(a) = 1$ et démontre que A est un corps.
2. Soit $x = Q(a) \in \mathbb{F}_p(a)$, la division euclidienne $Q = P\,Q_1 + R$ dans $\mathbb{F}_p[X]$ montre, puisque $P(a) = 0$, que $Q(a) = R(a)$, avec $R \in \mathbb{F}_p^{(r)}[X]$.
   Soit R_1 et $R_2 \in \mathbb{F}_p^{(r)}[X]$ deux polynômes tels que $R_1(a) - R_2(a) = (R_1 - R_2)(a) = 0$, le polynôme P divise alors le polynôme $R_1 - R_2$, avec $\deg(R_1 - R_2) < \deg(P)$, d'où $R_1 - R_2 = 0$.
3. Résulte de 2.
4. Si Q_1 et Q_2 sont deux polynômes de $\mathbb{F}_p[X]$, on a les équivalences

$$(Q_1(a) = Q_2(a)) \Longleftrightarrow ((Q_1 - Q_2) \text{ multiple de } P) \Longleftrightarrow \left(\overline{Q_1} = \overline{Q_2} \text{ dans } \mathbb{F}_p[X]/\langle P\rangle\right).$$

   Cela permet, d'après 1., de définir une application *surjective* ψ de $\mathbb{F}_p(a)$ dans $\mathbb{F}_p[X]/\langle P\rangle$ par

$$\psi(Q(a)) = \overline{Q},$$

   de sorte que $\psi(a) = \overline{X}$. L'application ψ est bijective puisque les corps $\mathbb{F}_p(a)$ et $\mathbb{F}_p[X]/\langle P\rangle$ ont même nombre d'éléments, elle est compatible avec l'addition et la multiplication, ψ est donc un isomorphisme de corps. □

Corollaire 5.13 *Soit* $\mathbb{K}$ *un corps fini de caractéristique* p*, et soit* a *un élément primitif de* $\mathbb{K}$*. Si* $P \in \mathbb{F}_p[X]$ *est le polynôme minimal de* a*, les corps* $\mathbb{K}$ *et* $\mathbb{F}_p[X]/\langle P\rangle$ *sont isomorphes.*

Preuve : Si a est un élément primitif de $\mathbb{K}$, on a $\mathbb{F}_p(a) = \mathbb{K}$. □

Le polynôme minimal d'un élément primitif de $\mathbb{K}$ est appelé **polynôme primitif**.

5.7.3 Décomposition du polynôme minimal

Théorème 5.14 *Soit* $\mathbb{K}$ *un corps fini de caractéristique* p*, soit* $a \in \mathbb{K}^*$ *un élément de degré algébrique* $r \geq 1$*,* P *le polynôme minimal de* a *et* $\mathbb{F}_p(a)$ *le sous-corps de* $\mathbb{K}$ *engendré par* a*.*

1. *L'entier* r *est le plus petit entier positif tel que* $a^{p^r} = a$.
2. *Les racines de* P *dans le corps* $\mathbb{K}$ *sont les* r *éléments* $a^{p^i} \in \mathbb{F}_p(a)$*, pour* $i = 0, 1, \ldots, r-1$*, elles sont toutes distinctes.*
3. *On a l'égalité dans* $\mathbb{F}_p[X]$

$$P = (X - a)(X - a^p)\ldots(X - a^{p^{r-1}}). \tag{1}$$

Preuve :

1. On sait (théorème 5.12 page 63), que $\#\mathbb{F}_p(a) = p^r$, le groupe $\mathbb{F}_p(a)^*$ est donc d'ordre $p^r - 1$, ce qui implique $a^{p^r-1} = 1$, c'est-à-dire $a^{p^r} = a$.
   Soit s le plus petit entier positif tel que $a^{p^s} = a$, alors $a^{p^s-1} = 1$, cela implique que $p^s - 1$ divise $p^r - 1$ donc que s divise r d'après le lemme 5.9 (page 62).
   Il résulte alors du théorème 5.10 (page 63) que l'ensemble $\mathbb{L} = \{x \in \mathbb{F}_p(a) \,|\, x^{p^s} = x\}$ est le sous-corps de $\mathbb{F}_p(a)$ à p^s éléments. Comme $a \in \mathbb{L}$, on en déduit $\mathbb{L} = \mathbb{F}_p(a)$ donc $s = r$.
2. Supposons $a^{p^i} = a^{p^j}$ avec $0 \leq i < j \leq r-1$, on en déduit
   $$a^{p^{r-j+i}} = (a^{p^i})^{p^{r-j}} = (a^{p^j})^{p^{r-j}} = a^{p^r} = 1,$$
   ce qui est impossible puisque $1 \leq j - i \leq r - 1$, donc $1 \leq r - j + i \leq r - 1$.
   Comme $P \in \mathbb{F}_p[X]$, on sait d'après le théorème 5.7 (page 57) que $[P(X)]^p = P(X^p)$, on en déduit $0 = [P(a)]^p = P(a^p) = P(a^{p^2}) = \cdots = P(a^{p^i})$ pour tout $i \geq 2$. Comme P est de degré r, les r éléments a^{p^i}, $i = 0, 1, \ldots, r-1$, sont les seules racines de P dans $\mathbb{K}$, et P étant unitaire on a l'égalité (1) dans $\mathbb{K}[X]$.
3. Montrer que l'égalité (1) a lieu dans $\mathbb{F}_p[X]$ revient à montrer que le polynôme
   $$Q = (X - a)(X - a^p) \ldots (X - a^{p^{r-1}})$$
   appartient à $\mathbb{F}_p[X]$. Pour cela, il faut et il suffit que $[Q(X)]^p = Q(X^p)$. Or
   $$[Q(X)]^p = (X-a)^p(X-a^p)^p \ldots (X-a^{p^{r-1}})^p = (X^p-a^p)(X^p-a^{p^2}) \ldots (X^p-a) = Q(X^p).$$
   □

Les éléments $a^p, a^{p^2}, \ldots, a^{p^{r-1}}$ sont appelés les **conjugués** de a.

5.7.4 Existence de corps finis

Théorème 5.15 *Soit p un nombre premier et n un entier positif. On pose*

$$\Pi_n = X^{p^n} - X \in \mathbb{F}_p[X].$$

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible unitaire de degré r. Alors

1. *P divise Π_n si et seulement si r divise n.*
2. *Le polynôme P^2 ne divise pas Π_n.*

Preuve : Soit $\mathbb{K} = \mathbb{F}_p[X]/\langle P\rangle$ et soit $\alpha = \mathrm{Cl}(X)$. On sait que $\#\mathbb{K} = p^r$, que P est le polynôme minimal de α et que $\alpha^{p^r-1} = 1$.

– Si r divise n, $(p^r - 1)$ divise $(p^n - 1)$ donc $\alpha^{p^n-1} = 1$ donc $\alpha^{p^n} = \alpha$, c'est-à-dire $\Pi_n(\alpha) = 0$.
  Par définition du polynôme minimal, cela implique que P divise Π_n.
– Réciproquement, si P divise Π_n, alors $\Pi_n(\alpha) = 0$, c'est-à-dire $\alpha^{p^n} = \alpha$.
  Mais l'ensemble $A = \{a \in \mathbb{K} \,|\, a^{p^n} = a\}$ est un sous-anneau de $\mathbb{K}$ (Cf. la démonstration du théorème 5.10 page 63). Comme A contient α, A contient toutes les puissances de α, donc $A = \mathbb{K}$. Ainsi tout élément de $\mathbb{K}^*$ vérifie $a^{p^n-1} = 1$.
  Or $\mathbb{K}^*$ contient un élément d'ordre $(p^r - 1)$, donc $(p^r - 1)$ divise $(p^n - 1)$ donc que r divise n.
– Si P^2 divisait Π_n, P diviserait $\Pi_n' = p^n X^{p^n-1} - 1 = -1$. □

Le théorème ci-dessus va nous servir à démontrer l'important résultat suivant.

Théorème 5.16 *Pour tout nombre premier p et tout entier positif n, il existe un polynôme irréductible de degré n dans l'anneau $\mathbb{F}_p[X]$.*

Preuve : Pour chaque entier positif n, désignons par $N_p(n)$ le nombre de polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$.

– Pour $n = 1$, $N_p(1) = p$.

– Pour $n = 2$, un polynôme unitaire de degré 2 s'écrit $P = X^2 + aX + b$, où $a,\ b \in \mathbb{F}_p$, il en existe p^2. Un tel polynôme est irréductible si et seulement s'il n'est pas d'une des deux formes

(1) $P = (X - \alpha)(X - \beta)$, où $\alpha,\ \beta \in \mathbb{F}_p,\ \ \alpha \neq \beta$,

(2) $P = (X - \alpha)^2$ où $\alpha \in \mathbb{F}_p$.

Or il existe $p(p-1)/2$ polynômes de la forme (1) et p de la forme (2), on en déduit

$$N_p(2) = p^2 - \frac{p(p-1)}{2} - p = \frac{p(p-1)}{2} \geq 1.$$

– Pour $n \geq 3$, on utilise le théorème 5.15 (page 65).
Le polynôme Π_n étant de degré p^n, il résulte du théorème 5.15 que

$$\sum_{d/n} d\, N_p(d) = p^n, \tag{1}$$

d'où en particulier

$$n\, N_p(n) \leq p^n. \tag{2}$$

Appliquant l'inégalité (2) à tous les diviseurs d de n et en reportant dans (1), on obtient

$$p^n - n\, N_p(n) \leq \sum_{d/n,\ d<n} p^d \leq \sum_{d=1}^{[\frac{n}{2}]} p^d = \frac{p^{[\frac{n}{2}]+1} - 1}{p-1} < p^{[\frac{n}{2}]+1}.$$

Ce qui donne la minoration

$$N_p(n) \geq \frac{p^n - p^{[\frac{n}{2}]+1}}{n} > 0.$$

$N_p(n)$ étant entier, on en déduit $N_p(n) \geq 1$. □

Il en résulte le théorème d'existence des corps finis.

Théorème 5.17 (Existence des corps finis) *Pour tout nombre premier p et tout entier positif n, il existe un corps à $q = p^n$ éléments.*

Preuve : Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n, le corps $\mathbb{F}_p[X]/\langle P\rangle$ possède p^n éléments. □

Enfin, l'énoncé suivant est une autre importante conséquence du théorème 5.15 (page 65).

Théorème 5.18 (Isomorphisme) *Deux corps qui ont même nombre d'éléments sont isomorphes, ce qui permet de parler **du** corps $\mathbb{F}_q$ à q éléments.*

Preuve : Soit $\mathbb{K}$ et $\mathbb{K}'$ deux corps à p^n éléments. Soit α un élément primitif de $\mathbb{K}$, et soit $P \in \mathbb{F}_p[X]$ le polynôme minimal de α. On sait d'après le théorème 5.13 (page 64) que $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/\langle P\rangle$.

Il résulte du théorème 5.15 que le polynôme P, irréductible de degré n, divise le polynôme $X^{p^n} - X$, lequel admet pour racines les éléments de $\mathbb{K}'$, (théorème 5.10 page 63). Le polynôme P admet donc n racines distinctes dans le corps $\mathbb{K}'$. Soit β l'une d'elles.

Le polynôme P étant irréductible dans $\mathbb{F}_p[X]$, β est de degré n sur $\mathbb{F}_p$ et P est son polynôme minimal, donc $\mathbb{K}' = \mathbb{F}_p(\beta)$ est isomorphe à $\mathbb{F}_p[X]/\langle P\rangle$ d'après le théorème 5.12 (page 63). Plus précisément, il existe un seul isomorphisme u de $\mathbb{K}$ sur $\mathbb{K}'$ tel que $u(\alpha) = \beta$, mais attention, le choix de β n'est pas unique dès que $n \geq 2$. □

Chapitre 6

Codes correcteurs d'erreurs

6.1 Généralités

Coder, ou encoder une information consiste à lui donner *temporairement* une certaine forme, l'information étant ultérieurement restituée par l'opération de décodage, c'est-à-dire l'opération inverse de l'encodage. Encoder une information peut avoir plusieurs buts.

- La confidentialité.
- Le stockage, la compression de données en est un exemple.
- La possibilité de détecter et/ou de corriger les erreurs qui surviennent lors de la transmission de cette information, c'est-à-dire lorsque l'information devient message. C'est l'objet des codes correcteurs d'erreurs, appelés plus simplement codes correcteurs. C'est ce cadre qui nous intéresse ici.

Le principe de base des codes correcteurs d'erreurs est de rajouter à un message à transmettre une information supplémentaire, appelée information **redondante** ou **de contrôle**, de manière à pouvoir détecter et éventuellement corriger de possibles erreurs de transmission. Cette opération s'appelle **encodage** du message et son résultat est un **mot de code**. A chaque message est donc associé un mot de code de longueur supérieure à celle du message. Le **code** est l'ensemble des mots de code ainsi obtenus.

6.1.1 Exemples élémentaires

Supposons qu'on veuille guider un avion en lui faisant parvenir par radio l'un ou l'autre des quatre messages suivants : virer à tribord, a bâbord, vers le haut ou vers le bas.
L'idée la plus simple et la plus économique consiste à représenter les messages *tribord*, *bâbord*, *haut* et *bas* respectivement par les **mots binaires** 01, 10, 11 et 00 qui seront *les messages à transmettre*.
Le problème est que si le canal de transmission radio est bruité, des erreurs peuvent se produire. Si par exemple le mot 10 est envoyé et qu'une erreur de transmission affecte le premier bit, le pilote de l'avion recevra le mot 00 et n'aura aucun moyen de savoir qu'une erreur est intervenue. D'où danger. Voici trois exemples d'encodage de ces quatre messages.

1. La première idée venant à l'esprit consiste à dédoubler chaque message, c'est-à-dire à encoder les messages 01, 10, 11 et 00 respectivement par les mots de code de longueur 4

   $$0101, \quad 1010, \quad 1111 \text{ et } 0000.$$

   Une erreur est alors détectable par le pilote puisque l'effet d'une erreur sur un mot de code le transforme en un mot qui n'est pas un mot de code. Une erreur intervenant par exemple lors de la transmission du mot de code 0101 donnera l'un des mots 1101, 0001,

0111 ou 0100 qui n'appartiennent pas au code. Recevant l'un de ces quatre mots, le pilote *saura qu'il y a eu erreur lors de la transmission*, ce qui est important, mais il ne pourra pas retrouver le mot de code d'origine puisque par exemple, si le message reçu est 1101, le mot de code d'origine, **sous l'hypothèse d'une seule erreur**, peut aussi bien être 0101 que 1111. Le pilote n'aura d'autre choix que de demander que le message lui soit réexpédié.
Mais attention, ce qui précède ne vaut que sous l'hypothèse de l'occurrence d'une seule erreur. Si en effet deux erreurs interviennent lors de la transmission du mot de code 0101, le pilote pourra recevoir par exemple le mot 0000, qui est un mot de code, et n'aura pas de raison de se méfier.
Le **code** est l'ensemble des mots de code. On a ici $C_1 = \{0101, 1010, 1111, 0000\}$.

2. Utiliser des mots de code plus courts pour le même résultat est plus économique. Par exemple, si on encode nos messages 01, 10, 11 et 00 en leur ajoutant un *bit de parité*, de sorte que la somme des bits d'un mot de code soit paire, on obtient le code de longueur 3

$$C_2 = \{011, 101, 110, 000\}.$$

Comme l'effet d'une erreur modifie la parité d'un mot, le code C_2 détecte une erreur, il a donc la même efficacité que C_1 tout en étant plus court.

3. Si maintenant on triple chaque message, obtenant le code de longueur 6

$$C_3 = \{011100, 100011, 111111, 000000\},$$

et que le pilote reçoive le mot 110101, il sait qu'il y a erreur puisque ce mot n'est pas un mot de code, et de plus, *sous l'hypothèse d'une seule erreur*, il sait que le seul mot de code qui a pu être envoyé est le mot 010101, ce qui lui permet de **corriger l'erreur**.

6.1.2 Définitions

On généralise facilement les exemples ci-dessus.

1. On commence par supposer que tous les messages à transmettre sont des "mots" de même longueur $k > 0$, écrits à l'aide d'un **alphabet** F à q éléments. Chaque message, noté $x = x_0\, x_1 \dots x_{k-1}$, est assimilé à un élément $(x_0, x_1, \dots, x_{k-1})$ de l'ensemble F^k, qui devient ainsi **l'espace des messages**. On a alors q^k messages possibles.
Un code construit sur un alphabet F à q éléments est appelé code **q-aire**, il est dit **binaire** si $q = 2$ et **ternaire** si $q = 3$. Dans les exemples ci-dessus, on avait $q = k = 2$.
2. On suppose que tous les mots de code sont de même longueur $n > k$.
3. Si on veut **encoder** M messages de longueur k, avec $M \leq q^k$, **l'encodage** consiste à choisir un entier $n > k$, puis à associer à chaque message à encoder un **mot de code** de longueur n, c'est-à-dire un élément de l'ensemble F^n, et cela de façon bien évidemment injective.
4. Le **code** obtenu, c'est-à-dire l'ensemble des mots de code, apparaît donc comme un ensemble C à M éléments, avec $M \leq q^k$, contenu dans F^n. La longueur n des mots de code est appelée **longueur** du code. On parle alors de code q-aire de longueur n à M mots.
5. Le rapport k/n est appelé **taux d'information** du code C.
6. Lors de la transmission d'un mot de code $m = m_0\, m_1 \dots m_{n-1}$ par un canal bruité, on dira que m est entaché de r erreurs, avec $1 \leq r \leq n$, ou d'une **erreur de poids** r, si r des composantes m_i de du mot m sont modifiées.

7. L'encodage introduit une **redondance** égale à $n-k$. C'est cette redondance qui doit permettre d'obtenir des mots plus "distants" les uns des autres de façon à pouvoir détecter ou corriger des erreurs intervenant lors de la transmission.
8. Le **décodage** consiste, lors de la réception d'un mot $x \in F^n$, à déterminer si x est un mot de code, puis, si ce n'en est pas un, à le **corriger** grâce à la redondance, c'est-à-dire à déterminer me mot de code m émis qui a été transformé en x lors de la transmission. Le décodage suppose un certain nombre d'hypothèses portant sur les propriétés du canal de transmission et sur le nombre maximum d'erreurs affectant le mot m.

Dans les exemples 6.1.1 (page 67), les codes C_1, C_2 et C_3 sont des codes binaires à 4 mots, de longueur respectivement 4, 3 et 6.

6.1.3 Distance entre les mots, la distance de Hamming

Richard Hamming (1915-1998), mathématicien nord-américain, a joué un rôle important dans l'élaboration de la théorie du codage algébrique.

Définition 6.1 *Soit $x = x_0\,x_1 \ldots x_{n-1}$ et $y = y_0\,y_1 \ldots y_{n-1} \in F^n$ deux mots de longueur n, on appelle **distance de Hamming** entre les mots x et y, et on note $d_H(x,y)$ le nombre d'indices $i \in \{0,1,2,\ldots,n-1\}$ tels que $x_i \neq y_i$.*

Proposition 6.1 *La distance de Hamming définit une distance sur l'ensemble F^n.*

Preuve : Soit x et $y \in F^n$, il résulte directement de la définition de la distance de Hamming que l'on a $d_H(x,y) = d_H(y,x) \geq 0$ et que $(d_H(x,y) = 0)$ si et seulement si $(x = y)$.
Reste à démontrer l'inégalité triangulaire.
Soit x, y et $z \in F^n$ et soit i un indice tel que $x_i \neq y_i$, alors on ne peut pas avoir $(x_i = z_i)$ et $(z_i = y_i)$, c'est-à-dire qu'on a soit $(x_i \neq z_i)$, soit $(z_i \neq y_i)$, soit les deux, ce qui signifie que

$$d_H(x,y) \leq d_H(x,z) + d_H(z,y). \qquad \square$$

Étant donné un code C, on appelle **distance minimum** de C l'entier d défini par

$$d = \min\{d_H(m,m') \,|\, m \in C,\, m' \in C,\, m \neq m'\}.$$

Dans les exemples 6.1.1 (page 67), les codes C_1 et C_2 ont pour distance minimum $d = 2$, et le code C_3 a pour distance minimum $d = 3$.

Les paramètres qui caractérisent un code sont
– sa longueur n,
– le nombre M de ses mots,
– sa distance minimum d,
– le nombre d'éléments q de l'alphabet F.
On parlera donc de $(n, M, d)_q$-codes ou de codes q-aires de paramètres (n, M, d).

6.1.4 Stratégie du maximum de vraisemblance

On fait l'hypothèse que le canal de transmission a un comportement symétrique, c'est-à-dire que lors de la transmission, chaque composante m_i d'un mot m transmis a, indépendamment des autres composantes, la probabilité $1-p$ d'être transmise sans erreur, et la probabilité $p/(q-1)$ d'être remplacée par chacun des $q-1$ autre symboles de F. Dans ce cas, la probabilité qu'un mot de code m soit transformé en un mot x à la suite de r erreurs est égale à

$$P(x/m) = (1-p)^{n-r}\left(\frac{p}{q-1}\right)^r = (1-p)^n\left(\frac{p}{(q-1)(1-p)}\right)^r.$$

Or on a $0 < \dfrac{p}{(q-1)(1-p)} < 1$ dès que $0 < p < \dfrac{q-1}{q}$, condition qu'on supposera satisfaite.

Dès lors, **la probabilité $P(x/m)$ est une fonction décroissante de r.**

La stratégie **du maximum de vraisemblance** consiste à rechercher le mot code m qui rend l'observation x la plus vraisemblable, c'est-à-dire la probabilité $P(x/m)$ maximum. Cela est réalisé dans notre cas lorsque le nombre d'erreurs r est minimum.

Comme $r = d_H(m, x)$, cela revient à **corriger x en lui faisant correspondre le mot de code m le plus proche de x au sens de la distance de Hamming**, et cela n'est possible que lorsque ce mot de code est unique.

6.1.5 Capacité de correction

Proposition 6.2 *Soit C un code de distance minimum d, et soit $x \in F^n$ un message reçu affecté de r erreurs, avec $r \geq 1$.*

1. *Si $2r < d$, c'est-à-dire si $r \leq \lfloor (d-1)/2 \rfloor$, le code C corrige les r erreurs.*
2. *Si $\lfloor (d-1)/2 \rfloor < r = \lfloor d/2 \rfloor$, (ce qui suppose d pair) le code C détecte l'existence de r erreurs mais ne peut pas toujours les corriger.*
3. *Si $\lfloor d/2 \rfloor < r \leq d-1$, le code C détecte l'existence d'erreurs mais risque d'effectuer une correction erronée.*

Preuve : Soit $m \in C$ le mot de code émis, on a par hypothèse $d_H(m, x) = r$.

1. Le mot de code m est alors le seul mot de code tel que $d_H(m, x) \leq r$, supposons en effet $m' \in C$ vérifiant $d_H(m', x) \leq r$, on en déduit $m' = m$ puisque

$$d_H(m', m) \leq d_H(m', x) + d_H(m, x) \leq 2r \leq d - 1 < d.$$

2. Il n'existe pas de mot de code $m' \in C$ tel que $d_H(m', x) < d_H(m, x) = r$, mais le mot de code m n'est plus nécessairement le seul à vérifier $d_H(m, x) = r$.
3. On sait qu'il y a erreur car $x \notin C$, mais il peut exister un mot de code $m' \in C$ tel que $d_H(m', x) < d_H(m, x) = r$. □

L'entier $t = \lfloor (d-1)/2 \rfloor$ est appelé **capacité de correction** du code C, on dit alors que C est un code **t-correcteur**.

Les codes correcteurs jouent un rôle capital dans tous les domaines où une information numérique est transmise par le biais d'un canal plus ou moins bruité. Cela va de la transmission de données informatiques à l'intérieur d'une même machine ou sur un réseau informatique, à la transmission de données satellitaires, en passant par la lecture d'un CD ou d'un DVD.
Augmenter la capacité de correction d'un code implique une plus grande redondance, donc un coût de transmission accru et une perte de vitesse de transmission de l'information.
Aussi, lorsque la rapidité est prioritaire et les erreurs peu fréquentes, comme c'est le cas en ce qui concerne par exemple les échanges de données à l'intérieur d'un même ordinateur, il suffit qu'on puisse détecter l'existence d'erreurs, l'opération de transmission est alors répétée.
A l'inverse, lorsque la répétition de la transmission est impossible, comme dans le cas de satellites envoyant des observations en direct, et que l'on veut une information de haute qualité, une grande capacité de correction est nécessaire.

6.1.6 Codes parfaits

Soit $x \in F^n$ et soit r un entier positif. La boule $B_H(x,r)$ de centre x et de rayon r pour la distance de Hamming est définie par

$$B_H(x,r) = \{\, y \in F^n \,|\, d_H(x,y) \leq r \}\,.$$

Proposition 6.3 *Si $\#F = q$, on a*

$$\#B_H(x,r) = \sum_{i=0}^{r} \mathcal{C}_i^n (q-1)^i.$$

Preuve : Pour chaque $i \in \{0,1,\ldots,r\}$, il existe $\mathcal{C}_i^n(q-1)^i$ mots $y \in F^n$ tels que $d_H(x,y) = i$.□

Soit C un code de paramètres $(n,M,d)_q$. Dire que $t = \lfloor (d-1)/2 \rfloor$ est la capacité de correction de C signifie que les M boules $B_H(m,t)$ centrées en les mots de code $m \in C$ sont deux à deux disjointes dans F^n. Ceci implique l'inégalité

$$M \sum_{i=0}^{t} \mathcal{C}_i^n (q-1)^i \leq q^n.$$

Cette égalité est appelée **borne d'empilement des sphères**.

Définition 6.2 *Un code de paramètres $(n,M,d)_q$ est **parfait** si $d = 2t+1$ est impair et si*

$$\bigcup_{m \in C} B_H(m,t) = F^n.$$

Proposition 6.4 *Un code de de paramètres $(n,M,d=2t+1)_q$ est parfait si et seulement si*

$$M \sum_{i=0}^{t} \mathcal{C}_i^n (q-1)^i = q^n.$$

Quand un code est parfait, tout élément $x \in F^n$ est dans une boule de Hamming de rayon t centrée en un mot de code, et une seule. C'est une situation idéale pour le décodage. Aucune place n'est perdue. Malheureusement, les codes parfaits sont rares.

6.2 Codes linéaires

Dans tout ce qui suit, on choisit pour alphabet F le corps $\mathbb{F}_q$ à q éléments. Dans la pratique, q est la plupart du temps de la forme 2^r où $r \in \mathbb{N}^*$, ou éventuellement $q = 3$.
L'ensemble $\mathbb{F}_q^n$ des mots de longueur n est muni d'une structure naturelle d'espace vectoriel de dimension n sur le corps $\mathbb{F}_q$, **chaque mot est assimilé à un vecteur de** $\mathbb{F}_q^n$. Cela permet de parler du mot nul, dont toutes les composantes sont égales à 0, qu'on notera lui-même 0, d'additionner deux mots, de retrancher un mot d'un autre, etc.

Proposition 6.5 *Sur $\mathbb{F}_q^n$, la distance de Hamming d_H vérifie*

$$\forall x \in \mathbb{F}_q^n,\ \forall y \in \mathbb{F}_q^n,\ \forall z \in \mathbb{F}_q^n, \quad d_H(x,y) = d_H(x+z,y+z) = d_H(x-y,0).$$

Preuve : Pour chaque indice $i \in \{0, 1, 2, \ldots, n-1\}$, on a les équivalences

$$(x_i \neq y_i) \Longleftrightarrow (x_i + z_i \neq y_i + z_i) \Longleftrightarrow (x_i - y_i \neq 0). \qquad \square$$

On définit le **poids** $w(x)$ d'un mot $x \in \mathbb{F}_q^n$ comme étant le nombre des composantes non nulles de x. On voit que $w(x) = d_H(x, 0)$ et il résulte de la proposition précédente que si x et $y \in \mathbb{F}_q^n$,

$$d_H(x, y) = w(x - y).$$

Si, lors de la transmission, un mot de code m est affecté de r erreurs, c'est le mot $x = m + e$ qui sera reçu, où $e \in \mathbb{F}_q^n$ est un mot de poids r qui représente les r erreurs.

Définition 6.3 *Un* ***code linéaire*** q***-aire de longueur*** n ***et de dimension*** k *est un sous-espace vectoriel de dimension* k *de* $\mathbb{F}_q^n$*. On supposera toujours* $k \geq 1$*.*

On dira aussi **code linéaire de longueur** n **et de dimension** k **sur** $\mathbb{F}_q$.

Exemple Les code C_1, C_2 et C_3 définis en 6.1.1 (page 67) sont des codes linéaires binaires.

Proposition 6.6 *Soit* C *un code linéaire, la distance minimum* d *de* C *est donnée par*

$$d = \min\{w(m) \,|\, m \in C,\ m \neq 0\}$$

Preuve : Posons $d' = \min\{w(m) \,|\, m \in C,\ m \neq 0\} = \min\{d_H(m, 0) \,|\, m \in C,\ m \neq 0\}$. Comme le mot nul 0 appartient à C, il résulte de la définition de la distance minimum d que $d' \geq d$. Réciproquement, C étant un ensemble fini, il existe m_1 et $m_2 \in C$ tels que $m_1 \neq m_2$ et $d = d_H(m_1, m_2)$, or $d_H(m_1, m_2) = w(m_1 - m_2)$, et $(m_1 - m_2) \in C$, $(m_1 - m_2) \neq 0$, d'où $d \leq d'$. $\square$

Un code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$ possède $M = q^k$ mots.

Les **paramètres d'un code linéaire** s'écriront $(n, k, d)_q$ au lieu de $(n, q^k, d)_q$, où n est la longueur, k la dimension et d la distance minimum du code.

L'inégalité suivante fournit une majoration de la distance minimum d en fonction des deux autres paramètres n et k, elle est appelée **borne de Singleton**.

Proposition 6.7 *Soit* C *un code linéaire de longueur* n *et de dimension* k*, alors on a*

$$(S) \qquad d + k \leq n + 1.$$

Preuve : Soit F_k le sous-espace vectoriel de $\mathbb{F}_q^n$ constitué des mots dont les $k-1$ dernières composantes sont nulles, alors $\dim(F_k) = n - (k-1) = n - k + 1$, donc $\dim(C) + \dim(F_k) = n + 1 > n$, on en déduit $C \cap F_k \neq \{0\}$. Il existe un mot non nul $m \in C \cap F_k$, ce qui implique $w(m) \leq n - k + 1$, donc $d \leq n - k + 1$ d'après la proposition 6.6 ci-dessus. $\square$

On appelle **distance relative** du code C le rapport $\delta = \dfrac{d}{n}$. L'inégalité (S) signifie que la distance relative δ et le taux de transmission $R = \dfrac{k}{n}$ ne peuvent être simultanément arbitrairement proches de 1 puisque reliés par l'inégalité

$$\delta + R \leq 1 + \frac{1}{n}.$$

Définition 6.4 *Un code linéaire pour lequel on a* $d = n - k + 1$ *est appelé code* ***MDS****, de l'anglais "Maximum Distance Separable".*

> **Exercice 38** — Soit n un entier positif. Montrer qu'une condition nécessaire pour qu'il existe un code linéaire binaire parfait 1-correcteur de longueur n est que l'entier n soit de la forme $n = 2^r - 1$, où r est un entier positif.

6.2.1 Encodage des codes linéaires - Matrices génératrices

Conventions de notations Soit k et n deux entiers positifs, A une application linéaire de $\mathbb{F}_q^k$ dans $\mathbb{F}_q^n$, et M la matrice de A par rapport aux bases canoniques respectives de $\mathbb{F}_q^k$ et $\mathbb{F}_q^n$. Soit $x = x_0\, x_1 \ldots x_{k-1}$ un mot q-aire de longueur k, identifié au vecteur

$$x = (x_0, x_1, \ldots, x_{k-1}) \in \mathbb{F}_q^k,$$

on conviendra pour alléger le texte d'écrire $A(x) = M(x)$ au lieu de $A(x) = M \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$.

On écrira aussi $\mathrm{Im}(M)$ pour $\mathrm{Im}(A)$ et $\ker(M)$ pour $\ker(A)$.

Soit C un $(n,k,d)_q$-code linéaire C. L'espace des messages est identifié à $\mathbb{F}_q^k$, **on encode les messages à l'aide d'une application linéaire** injective $\mathcal{E}$ de $\mathbb{F}_q^k$ dans $\mathbb{F}_q^n$ dont l'image $\mathrm{Im}(\mathcal{E})$ est égale à C.

Pour les codeurs, les vecteurs de $\mathbb{F}_q^k$ ou $\mathbb{F}_q^n$ sont des mots, **ils les notent donc traditionnellement comme des vecteurs lignes**, ce qui signifie que si $x = x_0\, x_1 \ldots x_{k-1}$ est un message à encoder, l'encodage $x \mapsto \mathcal{E}(x)$ sera représenté matriciellement par

$$\mathcal{E} : \quad x = x_0\, x_1 \ldots x_{k-1} \longrightarrow (x_0, x_1, \ldots, x_{k-1})\, G = x\, G, \tag{1}$$

où G est la **transposée** de la matrice de $\mathcal{E}$ par rapport aux bases canoniques respectives de $\mathbb{F}_q^k$ et $\mathbb{F}_q^n$, c'est-à-dire une matrice à k lignes et n colonnes à coefficients dans $\mathbb{F}_q$.

Remarque Si on désigne par $\ell_0, \ell_1, \ldots, \ell_{k-1} \in \mathbb{F}_q^n$ les lignes de la matrice G, alors

$$(x_0\, x_1 \ldots x_{k-1})\, G = x_0\, \ell_0 + x_1\, \ell_1 + \cdots + x_{k-1}\, \ell_{k-1}. \tag{2}$$

Définition 6.5 *Une matrice G à k lignes et n colonnes à coefficients dans $\mathbb{F}_q$ est appelée **matrice génératrice** du $(n,k,d)_q$-code C si les lignes de G constituent une base de l'espace vectoriel C.*

Proposition 6.8 *Soit G une matrice à k lignes et n colonnes à coefficients dans $\mathbb{F}_q$, pour que l'application linéaire $\mathcal{E}$ définie par (1) soit un encodage de C, il faut et il suffit que G soit une matrice génératrice de C.*

Preuve : Résulte de la relation (2) ci-dessus et de la définition d'une matrice génératrice. □

Proposition 6.9 *Soit G une matrice génératrice d'un $(n,k,d)_q$-code C.*

1. *Les k lignes de G étant linéairement indépendantes, G est de rang maximum égal à k.*
2. *Toute matrice déduite de G par une ou plusieurs des transformations suivantes, appelées **opérations élémentaires** sur les lignes, est encore une matrice génératrice de C :*
   - *permutation de deux lignes,*
   - *multiplication de tous les éléments d'une ligne par un scalaire non nul de $\mathbb{F}_q$,*
   - *addition à une ligne d'une combinaison linéaire des autres lignes.*

Preuve :

1. Résulte des propositions 0.25 et 0.26 (page 18).
2. Une opération élémentaire appliquée à une base de l'espace vectoriel C la transforment en une autre base de C. □

Proposition 6.10 *Réciproquement, soit G une matrice à k lignes et n colonnes à coefficients dans $\mathbb{F}_q$, de rang maximum k. Il existe un seul $(n,k,d)_q$-code admettant G pour matrice génératrice, c'est le code $C = Im(\mathcal{E})$, où $\mathcal{E}$ est l'application linéaire définie en (1) ci-dessus à partir de G. On l'appelle code **défini** par G, ou code de matrice génératrice G.*

Preuve : La matrice G étant de rang k, ses k lignes constituent une base de $\mathrm{Im}(\mathcal{E})$. □

6.2.2 Exemple : le code binaire de Hamming de longueur 7

C'est un code linéaire de longueur 7 et de dimension 4. On considère le mot $1101000 \in \mathbb{F}_2^7$, ainsi que les trois mots qui s'en déduisent par décalage, 0110100, 0011010 et 0001101. En tant que vecteurs de $\mathbb{F}_2^7$, on voit facilement que ces quatre mots sont linéairement indépendants. Le code binaire de Hamming de longueur 7 est le code linéaire engendré par ces 4 mots, désignons-le par C_H. Une matrice génératrice de C_H est donnée par

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Les $2^4 = 16$ mots de code sont

$$\begin{array}{ll} (0000)\,G = 0000000, & (0001)\,G = 0001101, \\ (0010)\,G = 0011010, & (0011)\,G = 0010111, \\ (0100)\,G = 0110100, & (0101)\,G = 0111001, \\ (0110)\,G = 0101110, & (0111)\,G = 0100011, \\ (1000)\,G = 1101000, & (1001)\,G = 1100101, \\ (1010)\,G = 1110010, & (1011)\,G = 1111111, \\ (1100)\,G = 1011100, & (1101)\,G = 1010001, \\ (1110)\,G = 1000110, & (1111)\,G = 1001011. \end{array}$$

Tous les mots non nuls de C_H sont de poids ≥ 3, on a donc $d = 3$, ce qui signifie que C est un code 1-correcteur.

De plus, une boule de Hamming de rayon 1 dans $\mathbb{F}_2^7$ possède $1 + 7 = 2^3$ éléments. Comme il existe 2^4 mots de code et que $2^4 \times 2^3 = 2^7$, le code de Hamming de longueur 7 est parfait, (cf. exercice 38 ci-dessus). En revanche, $d = 3 < n - k + 1 = 7 - 4 + 1 = 4$, le code de Hamming C_H n'est pas MDS.

6.2.3 Codes systématiques

Un $(n, k, d)_q$-code est dit **systématique** s'il possède une matrice génératrice G qu'on peut écrire par blocs sous la forme

$$G = (I_k \,|\, B)$$

où I_k désigne la matrice unité à k lignes et k colonnes, et B une matrice à k lignes et $(n - k)$ colonnes.

Une telle matrice est dite **normalisée**, ou **de forme standard**. L'intérêt d'un code systématique tient au fait que si un message $x = x_0\, x_1 \ldots x_{k-1} \in \mathbb{F}_q^k$ est encodé par une la matrice normalisée G, on le retrouve sous forme des k premières composantes du mot de code xG associé à x, puisque

$$x\,G = \underbrace{x_0\, x_1 \ldots x_{k-1}}_{x}\; c_1 \;\ldots c_{n-k}.$$

Théorème 6.11 *Soit $G = (a_{i\,j})_{0 \leq i \leq k-1,\, 0 \leq j \leq n-1}$ une matrice à k lignes et n colonnes, de rang maximum k. On peut transformer G en une matrice normalisée, par une suite d'opérations élémentaires **sur les lignes** de G, si et seulement si G possède la propriété suivante :*

(N) *La sous-matrice carrée $A = (a_{i\,j})_{0 \leq i \leq k-1,\, 0 \leq j \leq k-1}$ de G est de rang k.*

Preuve : Dire que la matrice A est de rang k signifie qu'elle est inversible, c'est-à-dire qu'on peut, à l'aide de **la méthode du pivot de Gauss**, par une suite d'opérations élémentaires **sur les lignes** de G, transformer A en la matrice unité I_k, ce qui transforme G en une matrice normalisée. □

Un code linéaire possédant une matrice génératrice normalisée est appelé **code systématique**.

Théorème 6.12 *1. Un $(n,k,d)_q$-code est systématique si et seulement s'il admet une matrice génératrice possédant la propriété (N).*

2. Toutes ses matrices génératrices possèdent alors la propriété (N).

Preuve :

1. Résulte de la proposition 6.9 (page 73) et du théorème 6.11 (page 74).
2. Soit $G = (a_{ij})$ et $G' = (a'_{ij})$ deux matrices génératrices du même code C, posons

$$A = (a_{ij})_{0\leq i\leq k-1,\, 0\leq j\leq n-1} \quad \text{et} \quad A' = (a'_{ij})_{0\leq i\leq k-1,\, 0\leq j\leq n-1}.$$

Les k lignes de G, ainsi que les k lignes de G', constituent une bases de C, il existe donc une matrice carrée M à k lignes et k colonnes, inversible, (matrice de changement de base) telle que $G' = MG$, ce qui implique $A' = MA$, c'est-à-dire que les matrices A et A' on même rang. □

Codes équivalents

Soit C un $(n,k,d)_q$-code non systématique et G une matrice génératrice de C. Comme G est de rang k, il existe k colonnes de G linéairement indépendantes, une permutation des colonnes de G peut placer ces colonnes en les k premières positions.
En d'autres termes, il existe une permutation π de $\{0,1,\ldots,n-1\}$ qui, appliquée aux colonnes de G, transforme G en une matrice G' possédant la propriété (N).
Le code C' défini par G' est donc systématique.
Il est facile de voir que
– si $m = m_0\, m_1 \ldots m_{n-1} \in C$, le mot $\pi(m) = m_{\pi(0)}\, m_{\pi(1)} \ldots m_{\pi(n-1)}$ appartient à C',
– tout mot de C' et de cette forme.
On écrit dans ce cas que $\pi(C) = C'$.

Définition 6.6 *Deux codes linéaires C et C' de longueur n sont dits **équivalents** s'il existe une permutation π de $\{0,1,\ldots,n-1\}$ telle que $\pi(C) = C'$.*

On a ainsi démontré le théorème suivant.

Théorème 6.13 *Tout code linéaire est équivalent à un code systématique.*

Exercice 39 — Montrer que le code binaire de Hamming de longueur 7 est systématique. En déterminer une matrice génératrice normalisée à l'aide de la méthode du pivot de Gauss.

6.2.4 Décodage des codes linéaires - Matrices de contrôle

Soit C un $(n,k,d)_q$-code. On **contrôle** qu'un mot reçu $x \in \mathbb{F}_q^n$ est un mot de code à l'aide d'une application linéaire S de $\mathbb{F}_q^n$ sur $\mathbb{F}_q^{n-k}$ dont le noyau $\ker(S)$ est égal à C. Cette application linéaire est donc de rang maximum $n-k$, et on a l'équivalence

$$\forall x \in \mathbb{F}_q^n, \quad (x \in C) \Longleftrightarrow (S(x) = 0)$$

Le vecteur $S(x) \in \mathbb{F}_q^{n-k}$ est appelé **syndrome** de x, il est nul si et seulement si $x \in C$.
La matrice H de S par rapport aux bases canoniques respectives de $\mathbb{F}_q^n$ et $\mathbb{F}_q^{n-k}$ possède $(n-k)$ lignes et n colonnes. H est de rang maximum $n-k$ et $\ker(H) = C$. On l'appelle **matrice de contrôle** du code C. Plus généralement :

Définition 6.7 *On appelle* ***matrice de contrôle*** *d'un $(n,k,d)_q$-code C toute matrice H à $(n-k)$ lignes et n colonnes, de rang maximum $n-k$, à coefficients dans $\mathbb{F}_q$, telle que* $\ker(H) = C$. *Le* ***syndrome*** *du mot x est alors le vecteur $H(x) \in \mathbb{F}_q^{n-k}$.*

Proposition 6.14 *Soit G une matrice génératrice du $(n,k,d)_q$-code C. Une matrice H à $(n-k)$ lignes et n colonnes, de rang $n-k$, à coefficients dans $\mathbb{F}_q$, est une matrice de contrôle de C si et seulement si on a la relation*

$$H\,{}^tG = 0. \tag{1}$$

Preuve : Dire que $H\,{}^tG = 0$ équivaut à dire que pour tout vecteur colonne c de ${}^tG$, on a $H(c) = 0$. Or les vecteurs colonnes de ${}^tG$ sont les vecteurs lignes de G et on sait qu'ils constituent une base de l'espace vectoriel C. La condition (1) équivaut donc à l'inclusion $C \subseteq \ker(H)$, mais la matrice H étant de rang $(n-k)$, $\ker(H)$ est de dimension $n-(n-k) = k = \dim(C)$, d'où l'égalité $C = \ker(H)$. □

Nous allons voir comment déterminer une matrice de contrôle d'un code défini par une matrice génératrice.

Cas d'un code systématique

Corollaire 6.15 *Soit C un $(n,k,d)_q$-code systématique et $G = (I_k|B)$ une matrice génératrice normalisée de C, alors la matrice*

$$H = \left(-{}^tB \,|\, I_{n-k}\right)$$

est une matrice de contrôle de C.

Preuve : La matrice ${}^tG$ s'écrit par blocs sous la forme ${}^tG = \begin{pmatrix} I_k \\ {}^tB \end{pmatrix}$ et il est clair que

$$\left(-{}^tB \,|\, I_{n-k}\right)\begin{pmatrix} I_k \\ {}^tB \end{pmatrix} = -{}^tB + {}^tB = 0.$$ □

Exercice 40 — Déterminer une matrice de contrôle du code de Hamming C_H de longueur 7 défini en 6.2.2 (page 74).

Cas d'un code non systématique

Soit C un $(n,k,d)_q$-code non systématique, on procède comme suit.

1. On sait d'après le théorème 6.13 (page 75) qu'il existe une permutation π de l'ensemble $\{0,1,\ldots,n-1\}$ telle que le code $\pi(C) = C'$ soit systématique. On détermine une matrice génératrice normalisée G' de C'.
2. Le corollaire 6.15 (page 76) permet alors de déterminer une matrice de contrôle H' de C'.
3. Il est clair que la matrice H déduite de H' en appliquant la permutation π^{-1} aux colonnes de H' est une une matrice de contrôle de C.

Exercice 41 — Déterminer une matrice de contrôle du code binaire C de matrice génératrice

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Un code peut enfin être défini par une de ses matrices de contrôle. On démontrera le résultat suivant à titre d'exercice.

Proposition 6.16 *Étant donnée une matrice H à $(n-k)$ lignes et n colonnes, de rang maximum $n-k$, à coefficients dans $\mathbb{F}_q$, il existe un seul $(n,k,d)_q$-code admettant H pour matrice de contrôle, c'est le code $C = \{x \in \mathbb{F}_q^n \mid H(x) = 0\} = \ker(H)$.*
Si H est de la forme $H = (A|I_{n-k})$, le code $C = \ker(H)$ est systématique et une matrice génératrice normalisée G de C est donnée par

$$G = \left(I_k \mid -{}^tA\right).$$

6.2.5 Propriétés des matrices de contrôle

Outre sa fonction à strictement parler de contrôle, une matrice de contrôle est utile à deux autres titres, elle permet d'une part de calculer la distance minimum d du code et fournit un algorithme de décodage.

1. Détermination de la distance minimum

L'énoncé suivant montre comment on peut déduire la distance minimum d'un code de sa matrice de contrôle.

Théorème 6.17 *Soit C un $(n,k,d)_q$-code, H une matrice de contrôle de C, et soit r un entier vérifiant $1 \leq r \leq n$.*

1. *S'il existe dans C un mot de poids r, il existe r colonnes de la matrice H linéairement dépendantes.*
2. *S'il existe r colonnes de la matrice H linéairement dépendantes, il existe un mot de code de poids r', avec $1 \leq r' \leq r$.*
3. *On en déduit que la distance minimum d est égale au nombre minimum de colonnes de la matrice H qui sont linéairement dépendantes. Tout système constitué de $(d-1)$ des n colonnes de H est alors libre.*
4. *Il en résulte que pour tout $x \in \mathbb{F}_q^n$, on a*

$$\left.\begin{array}{l} w(x) \leq d-1 \\ h(x) = 0 \end{array}\right\} \implies (x = 0).$$

Preuve : Désignons par $c_0, c_1, \ldots, c_{n-1}$ les n colonnes de H.

1. Soit $m = m_0\, m_1 \ldots m_{n-1} \in \mathbb{F}_q^n$ un mot de code de poids r, et soit $m_{i_1}, m_{i_2}, \ldots, m_{i_r}$ les r composantes non nulles de m. De l'égalité

$$H(m) = \sum_{p=1}^{r} m_{i_p} c_{i_p} = 0, \tag{1}$$

il résulte que les r colonnes $c_{i_1}, c_{i_2}, \ldots, c_{i_r}$ sont linéairement dépendantes.

2. Soit $c_{i_1}, c_{i_2}, \ldots, c_{i_r}$ r colonnes de H linéairement dépendantes, il existe r scalaires *non tous nuls* $m_{i_1}, m_{i_2}, \ldots, m_{i_r}$ de $\mathbb{F}_q$ tels que $\sum_{p=1}^{r} m_{i_p} c_{i_p} = 0$. Le mot $m \in \mathbb{F}_q^n$, dont les composantes de rang $i_1, i_2, \ldots, i_r$ sont respectivement $m_{i_1}, m_{i_2}, \ldots, m_{i_r}$, et dont les autres composantes sont nulles, vérifie la relation (1), c'est donc un mot de code de poids $r' \leq r$, où $r' \geq 1$ désigne le nombre des scalaires m_{i_j} non nuls.
3. Conséquence directe de 1. et 2.
4. Si x n'était pas nul, il existerait $(d-1)$ colonnes de H linéairement dépendantes. □

2. Table de décodage

Soit C un $(n,k,d)_q$-code, $t = \lfloor (d-1)/2 \rfloor$ sa capacité de correction, et H une matrice de contrôle. Une fois transmis, si un mot m est entaché de r erreurs, le mot reçu x est de la forme $x = m+e$, où $e \in \mathbb{F}_q^n$ est de poids $w(e) = r$ et représente les r erreurs de transmission. On parle aussi d'une **erreur** e **de poids** r. Le syndrome de x est

$$H(x) = H(m+e) = H(m) + H(e) = H(e).$$

Il résulte du théorème 6.17 ci-dessus que

si l'erreur e ***est de poids*** $w(e) \leq t$***, la connaissance de*** $H(e)$ ***détermine*** e.

Supposons en effet $e' \in \mathbb{F}_q^n$, de poids $w(e') \leq t$, vérifiant $H(e) = H(e')$, c'est-à-dire $H(e-e') = 0$. Comme $w(e-e') \leq w(e) + w(e') \leq 2t \leq d-1$, il résulte du théorème 6.17 que $e = e'$.

Sous l'hypothèse d'au plus t erreurs, il ne reste plus qu'à dresser **une table de décodage** contenant tous les éléments $e \in \mathbb{F}_q^n$ de poids $w(e) \leq t$, chacun suivi de son syndrome.

Si le mot x est reçu, on calcule le syndrome $H(x)$.
– Si $H(x) = 0$, pas de correction.
– Si $H(x)$ figure dans la table, on décode x par $m = x - e$, où $H(e) = H(x)$.
– Si $H(x)$ ne figure pas dans la table, c'est que x est affecté de plus de t erreurs.

Cas d'une erreur de poids 1. Lorsque seule la i-ième composante m_i du mot m est affecté d'une erreur, qui le transforme en $m_i + a$, avec $a \in \mathbb{F}_q^*$, le syndrome du mot reçu x est égal au vecteur obtenu en multipliant le i-ième vecteur colonne de la matrice H par a.
Dans le cas d'un code binaire, le décodage est particulièrement simple puisque $a = 1$, *le syndrome d'une erreur en* i*-ième position est alors le* i*-ième vecteur colonne de la matrice* H.

6.3 Codes cycliques

Soit $m = m_0\, m_1 \ldots m_{n-1} \in \mathbb{F}_q^n$ un mot de longueur n, on note

$$\sigma(m) = m_{n-1}\, m_0\, m_1 \ldots m_{n-2}$$

le mot obtenu par décalage circulaire *à droite* des composantes de m.

Définition 6.8 *Un* ***code cyclique*** C *est un code linéaire tel que*

$$\forall m \in C, \quad \sigma(m) \in C.$$

Il en résulte que si m est un mot de code, le mot $\sigma^2(m) = m_{n-2}\, m_{n-1}\, m_0 \dots m_{n-3}$ est encore un mot de code, ainsi que tous les mots $\sigma^k(m)$ pour tout $k \geq 3$. En particulier, le mot $\sigma^{n-1}(m) = m_1\, m_2 \dots m_{n-1}\, m_0$, qui est le mot obtenu par décalage *à gauche* des composantes de m. Les mots $\sigma^k(m)$ sont appelés mots décalés de m. Notons que $\sigma^n(m) = m$.

Les codes cycliques sont les codes linéaires les plus importants, cela tient au fait qu'on peut les décrire facilement en termes de polynômes.

Étant donné un mot $m = m_0\, m_1 \dots m_{n-1} \in \mathbb{F}_q^n$, le polynôme

$$m(X) = m_0 + m_1 X + \cdots + m_{n-1} X^{n-1} \in \mathbb{F}_q[X]$$

est appelé **polynôme associé** au mot m. Cette représentation d'un mot par un polynôme permet, comme on va le voir, de décrire entièrement les codes cycliques.

On démontrera la proposition suivante à titre d'exercice.

Proposition 6.18 *L'application $m \mapsto m(X)$ est un isomorphisme de l'espace vectoriel $\mathbb{F}_q^n$ sur le sous-espace vectoriel $\mathbb{F}_q[X]^{(n)}$ de $\mathbb{F}_q[X]$ constitué des polynômes de degré au plus égal à $n-1$.*

Étant donné un polynôme $P = a_0 + a_1 X + \cdots + a_r X^r \in \mathbb{F}_q[X]^{(n)}$, l'unique mot $m \in \mathbb{F}_q^n$ tel que $m(X) = P$ est le mot

$$m = a_0\, a_1 \dots a_r \underbrace{0 \dots 0}_{n-r-1}$$

qu'on appellera donc le **mot de longueur n associé au polynôme P.**

Étudions l'effet du décalage à droite sur cette représentation polynômiale des mots.

Soit $m = m_0\, m_1 \dots m_{n-1} \in \mathbb{F}_q^n$, on a

$$\begin{aligned} \sigma(m)(X) &= m_{n-1} + m_0 X + \cdots + m_{n-2} X^{n-1} \\ &= m_0 X + \cdots + m_{n-2} X^{n-1} + (m_{n-1}\, X^n - m_{n-1}\, X^n) + m_{n-1} \\ &= X\, m(X) + m_{n-1}\, (1 - X^n), \end{aligned}$$

ce qui implique $$\sigma(m)(X) = X m(X) \pmod{X^n - 1}.$$

Cela signifie que, modulo le polynôme $X^n - 1$, le décalage à droite effectué sur le mot m se traduit par la multiplication par X du polynôme $m(X)$.

Les deux propositions suivantes résument les propriétés essentielles de la représentation polynômiale des mots de $\mathbb{F}_q^n$. La première découle directement de ce qui précède.

Proposition 6.19 *Pour tout $m = m_0\, m_1 \dots m_{n-1} \in \mathbb{F}_q^n$, on a*

a) $$\sigma(m)(X) = X m(X) + m_{n-1}(1 - X^n),$$

ce qui implique, pour tout entier positif k,

b) $$\sigma^k(m)(X) \equiv X^k m(X) \pmod{X^n - 1}.$$

En d'autres termes, ***le polynôme $\sigma^k(m)(X)$ est le reste de la division euclidienne dans l'anneau $\mathbb{F}_q[X]$ du polynôme $X^k m(X)$ par le polynôme $X^n - 1$.***

On a vu plus haut que le mot de longueur n associé à un polynôme $P \in \mathbb{F}_q[X]^{(n)}$ de degré $r \leq n-1$ se termine à droite par $(n - r - 1)$ zéros. Les mots se terminant à droite par un certain nombre de zéros jouent par conséquent un rôle particulier dans la théorie des codes cycliques, la proposition suivante détaille les calculs qui les concernent.

Proposition 6.20 *Soit k un entier tel que $1 \leq k \leq n$, et soit $m = m_o m_1 \dots m_{n-1} \in \mathbb{F}_q^n$ un mot* ***non nul*** *dont les $k-1$ dernières composantes sont nulles. Alors*

a) *Les k mots*

$$\begin{cases} m &= m_0\, m_1 \dots m_{n-k}\, 0 \dots 0\, 0, \\ \sigma(m) &= 0\, m_0\, m_1 \dots m_{n-k}\, 0 \dots 0, \\ \dots &= \dots \\ \sigma^{k-1}(m) &= 0\, 0 \dots 0\, m_0\, m_1 \dots m_{n-k} \end{cases}$$

sont linéairement indépendants dans $\mathbb{F}_q^n$.

b) *On a dans $\mathbb{F}_q[X]$ les égalités suivantes*

$$\begin{cases} \sigma(m)(X) &= Xm(X) \\ \cdots\cdots\cdots &= \cdots\cdots \\ \sigma^{k-1}(m)(X) &= X^{k-1}m(X) \\ \sigma^{k}(m)(X) &= X^{k}m(X) - m_{n-k}(X^n - 1) \end{cases}$$

Preuve :

a) Il est clair que la matrice dont les lignes sont les k mots m, $\sigma(m), \dots,$ $\sigma^{k-1}(m)$ est de rang k, ces mots sont donc linéairement indépendants.

b) Résulte de la proposition 6.19 ci-dessus, compte tenu du fait que les $k-1$ dernières composantes du mot m sont nulles, c'est-à-dire $\deg(m(X)) \leq n-k$. □

6.3.1 Polynôme générateur d'un code cyclique

Théorème 6.21 *Soit C un code linéaire de longueur n sur $\mathbb{F}_q$, il existe dans C un mot non nul* ***unique*** *$\widetilde{m}$ possédant* ***un nombre maximum de zéros à droite****, et tel que la dernière lettre non nulle de $\widetilde{m}$ soit égale à 1.*

$$\widetilde{m} = a_0\, a_1 \dots a_{r-1}\, 1\, 0 \dots 0.$$

On désignera $\widetilde{m}$ comme étant le ***mot minimal*** *du code C.*

Preuve : La propriété fondamentale de $\mathbb{N}$ assure l'existence d'un mot non nul $m \in C$ possédant un nombre maximum de zéros à droite. On écrit $m = a_0\, a_1 \dots a_r\, 0 \dots 0$, avec $a_r \neq 0$. Multipliant m par ${a_r}^{-1}$, on obtient un mot de C répondant aux conditions ci-dessus.
Ce mot est unique dans C car si $m' \in C$ est un autre tel mot, le mot $m' - \widetilde{m}$ possède au moins un zéro de plus à droite que $\widetilde{m}$, donc $m' - \widetilde{m} = 0$.

> **Exercice 42** — Montrer que si un code est cyclique, son mot minimal $\widetilde{m} = a_0\, a_1 \dots a_{r-1}\, 1\, 0 \dots 0$ vérifie $a_0 \neq 0$.

Théorème 6.22 *Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$, et soit $\widetilde{m} = a_0\, a_1 \dots a_{r-1} 1\, 0 \dots 0 \in C$ le mot minimal de C. Alors*

1. *Les $n-r$ mots*

$$\begin{cases} \widetilde{m} &= a_0\, a_1 \dots a_{r-1}\, 1\, 0 \dots 0\, 0, \\ \sigma(\widetilde{m}) &= 0\, a_0\, a_1 \dots a_{r-1}\, 1\, 0 \dots 0, \\ \dots &= \dots \\ \sigma^{n-r-1}(\widetilde{m}) &= 0\, 0 \dots 0\, a_0\, a_1 \dots a_{r-1}\, 1 \end{cases}$$

constituent une base de C.

2. *On en déduit $r = n - k$.*

3. *Pour tout* $m \in \mathbb{F}_q^n$, *on a l'équivalence*

$$(m \in C) \Longleftrightarrow (\widetilde{m}(X) \text{ divise } m(X)).$$

4. *Le polynôme* $\widetilde{m}(X)$ *divise le polynôme* $X^n - 1$.

Preuve : Posons $l = n - r$, et soit $m \in \mathbb{F}_q^n$.
La division euclidienne dans $\mathbb{F}_q[X]$ de $m(X)$ par $\widetilde{m}(X)$ s'écrit

$$m(X) = (b_0 + b_1 X + \cdots + b_{l-1}X^{l-1})\widetilde{m}(X) + R(X), \quad \deg(R) \leq r - 1. \tag{1}$$

Il en résulte, d'après la proposition 6.20 b) (page 80),

$$m(X) = b_0\widetilde{m}(X) + b_1\sigma(\widetilde{m})(X) + \cdots + b_{l-1}\sigma^{l-1}(\widetilde{m})(X) + R(X)$$

ce qui donne dans $\mathbb{F}_q^n$

$$m = b_0\widetilde{m} + b_1\sigma(\widetilde{m}) + \cdots + b_{l-1}\sigma^{l-1}(\widetilde{m}) + m_R, \tag{2}$$

où m_R est le mot de $\mathbb{F}_q^n$ associé au polynôme R.

1. Le code C est un sous-espace vectoriel de $\mathbb{F}_q^n$ qui contient tous les mots $\sigma^i(\widetilde{m})$, il résulte donc de (2) que si $m \in C$, alors $m_R \in C$. Or $\deg(R) < \deg(\widetilde{m}) = r$, c'est-à-dire que m_R possède plus de zéros à droite que $\widetilde{m}$, on en déduit $m_R = 0$. La relation (2) devient

   $$m = b_0\widetilde{m} + b_1\sigma(\widetilde{m}) + \cdots + b_{l-1}\sigma^{l-1}(\widetilde{m}), \tag{3}$$

   ce qui signifie que la famille $\{\widetilde{m},\ \sigma(\widetilde{m}), \ldots,\ \sigma^{l-1}(\widetilde{m})\}$ engendre C. Mais on sait d'après la proposition 6.20 a) que cette famille est libre, c'est donc une base de C.
2. Il en résulte $k = l = n - r$.
3. On a vu que si $m \in C$, on a $m_R = 0$, mais comme $\deg(R) < r \leq n - 1$, c'est-à-dire $R \in \mathbb{F}_q[X]^{(n)}$, cela implique $R = 0$ d'après la proposition 6.18 (page 79). La relation (1) devient

   $$m(X) = (b_0 + b_1 X + \cdots + b_{k-1}X^{k-1})\widetilde{m}(X), \tag{4}$$

   ce qui signifie que $\widetilde{m}(X)$ divise $m(X)$.
   Réciproquement, soit $m \in \mathbb{F}_q^n$, dire que $\widetilde{m}(X)$ divise $m(X)$ équivaut à la relation (4) qui elle-même implique (3), c'est-à-dire $m \in C$.
4. Comme $a_r = 1$ et $k = n - r$, la dernière égalité de la proposition 6.20 b) s'écrit

   $$\sigma^k(\widetilde{m})(X) = X^k\widetilde{m}(X) - (X^n - 1).$$

   Comme $\sigma^k(\widetilde{m}) \in C$, on peut remplacer $m(X)$ par $\sigma^k(\widetilde{m})(X)$ dans la relation (4), d'où

   $$\sigma^k(\widetilde{m})(X) = X^k\widetilde{m}(X) - (X^n - 1) = (b_0 + b_1 X + \cdots + b_{k-1}X^{k-1})\widetilde{m}(X). \tag{5}$$

   Il en résulte que $\widetilde{m}(X)$ divise $X^n - 1$ puisque (5) s'écrit

   $$X^n - 1 = (-b_0 - b_1 X - \cdots - b_{k-1}X^{k-1} + X^k)\widetilde{m}(X). \qquad \square$$

Le point 2. du théorème ci-dessus décrit le code cyclique C comme étant l'ensemble des mots $m \in \mathbb{F}_q^n$ tels que le polynôme $\widetilde{m}(X)$ divise le polynôme $m(X)$. Cela justifie la définition suivante.

Définition 6.9 *Le polynôme $g = \widetilde{m}(X)$ associé au mot minimal $\widetilde{m}$ d'un code cyclique C est appelé* ***polynôme générateur de*** *C.*

Remarquons que le polynôme $g = \widetilde{m}(X)$ est **unitaire et de degré minimum** parmi tous les polynômes $m(X)$ associés aux mots non nuls m de C.
Le théorème suivant montre que chacune des trois premières propriétés énoncées dans le théorème 6.22 ci-dessus est en fait une propriété caractéristique du polynôme générateur d'un code cyclique, souvent plus pratique à utiliser que la définition 6.9 ci-dessus.

Théorème 6.23 *Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$, et soit*

$$g = g_0 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r \in \mathbb{F}_q[X]$$

un polynôme unitaire de degré $r \leq n-1$ tel que le mot $\widetilde{m} = g_0\, g_1 \ldots g_{r-1}\, 1\, 0 \ldots 0$ de longueur n associé au polynôme g soit un mot de code, les conditions suivantes sont équivalentes.

1. *Le mot $\widetilde{m}$ est le mot minimal de C.*
2. *Le polynôme g est le polynôme générateur de C.*
3. *Pour chaque mot $m \in \mathbb{F}_q^n$, on a l'équivalence*
$$(m \in C) \Longleftrightarrow (g \text{ divise } m(X))\,.$$
4. *Pour chaque mot $m \in C$, g divise $m(X)$.*
5. *La famille des $n-r$ mots $\{\widetilde{m},\ \sigma(\widetilde{m}),\ \ldots, \sigma^{n-r-1}(\widetilde{m})\}$ est une base de C.*
6. *$r = n - k$.*
7. *$r \leq n - k$.*

Si ces conditions équivalentes sont vérifiées, le polynôme g divise le polynôme $X^n - 1$, (ce qui implique en particulier que $g_0 \neq 0$, cf. exercice 42.)

Preuve : Les conditions 1. et 2. sont équivalentes d'après la proposition 6.18 (page 79).
Soit g' le polynôme générateur de C.

- 2. $\Longrightarrow$ 3. d'après le théorème 6.22, et il est clair que 3. $\Longrightarrow$ 4.
  On sait d'après le théorème 6.22 que $\deg(g') = n - k$ et que g' divise $\widetilde{m}(X) = g$. La condition 4. implique que g divise g', les deux polynômes étant unitaires, on en déduit que $g = g'$. On a donc montré l'équivalence de 2., 3. et 4.
- De même, 2. $\Longrightarrow$ 5. d'après le théorème 6.22, et 5. $\Longrightarrow (k = n - r)$, c'est-à-dire 6., enfin il est clair que 6. $\Longrightarrow$ 7.
- La condition 7. signifie que $\deg(g) \leq \deg(g')$, et comme g' divise g et que les deux polynômes sont unitaires, on en déduit $g = g'$, c'est-à-dire 2.
  D'où l'équivalence entre 2., 5., 6. et 7.

Le polynôme générateur g divise le polynôme $X^n - 1$ d'après le théorème 6.22. □
Réciproquement, à tout diviseur unitaire $g \in \mathbb{F}_q[X]$ du polynôme $X^n - 1$ correspond un code cyclique de longueur n dont g est le polynôme générateur. C'est l'objet du théorème suivant.

Théorème 6.24 *Soit $g = g_0 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r$ un diviseur unitaire de degré r du polynôme $X^n - 1$ dans $\mathbb{F}_q[X]$, avec $0 \leq r \leq n-1$. Soit $\widetilde{m} = g_0\, g_1 \ldots g_{r-1}\, 1\, 0 \ldots 0 \in \mathbb{F}_q^n$ le mot de longueur n associé au polynôme g, et soit $k = n - r$.*
Alors le code $C \subseteq \mathbb{F}_q^n$ de longueur n engendré par les k mots

$$\{\widetilde{m},\ \sigma(\widetilde{m}),\ \ldots, \sigma^{k-1}(\widetilde{m})\}$$

est cyclique, de dimension k, et son polynôme générateur est le polynôme g.
On dit que le code C est le code cyclique engendré par g.

Preuve : Le code C est de dimension k car les mots $\widetilde{m}$, $\sigma(\widetilde{m})$, $\ldots$, $\sigma^{k-1}(\widetilde{m})$ sont linéairement indépendants dans $\mathbb{F}_q^n$ d'après la proposition 6.20 a) (page 80).
Soit $m' = \lambda_0\widetilde{m} + \lambda_1\sigma(\widetilde{m}) + \cdots + \lambda_{k-1}\sigma^{k-1}(\widetilde{m})$ un élément de C, on a

$$\sigma(m') = \lambda_0\sigma(\widetilde{m}) + \lambda_1\sigma^2(\widetilde{m}) + \cdots + \lambda_{k-1}\sigma^k(\widetilde{m}).$$

Pour montrer que C est cyclique, on voit qu'il suffit de montrer que $\sigma^k(\widetilde{m}) \in C$.
Comme $g_r = 1$, on sait par la proposition 6.20 b) que

$$\sigma^k(\widetilde{m})(X) = X^k\widetilde{m}(X) - (X^n - 1). \tag{1}$$

Le polynôme $\widetilde{m}(X) = g$, unitaire de degré r, divise le polynôme unitaire $X^n - 1$, le quotient est un polynôme de $\mathbb{F}_q[X]$ unitaire de degré $k = n - r$. On peut donc écrire

$$X^n - 1 = (h_0 + h_1X + \cdots + X^k)\widetilde{m}(X),$$

ce qui, rapporté dans (1), donne

$$\begin{aligned}\sigma^k(\widetilde{m})(X) &= X^k\widetilde{m}(X) - (h_0 + h_1X + \cdots + h_{k-1}X^{k-1} + X^k)\widetilde{m}(X)\\ &= (h_0 + h_1X + \cdots + h_{k-1}X^{k-1})\widetilde{m}(X)\\ &= h_0\,\widetilde{m}(X) + h_1X\widetilde{m}(X) + \cdots + h_{k-1}X^{k-1}\widetilde{m}(X).\end{aligned}$$

On en déduit, compte tenu des propositions 6.18 et 6.20 a) (page 80), l'égalité dans $\mathbb{F}_q^n$

$$\sigma^k(\widetilde{m}) = h_0\widetilde{m} + h_1\sigma(\widetilde{m}) + \cdots + h_{k-1}\sigma^{k-1}(\widetilde{m})$$

qui montre que $\sigma^k(\widetilde{m}) \in C$ et que C est cyclique.
Enfin, le polynôme g est associé à un mot de C, il est unitaire de degré $(n-k)$, c'est donc le polynôme générateur de C d'après le théorème 6.23. □

Le théorème 6.23 signifie que tout code cyclique est engendré, au sens du théorème 6.24, par son polynôme générateur.

Ainsi, puisqu'on a vu que deux codes cycliques de même longueur possédant le même polynôme générateur sont identiques, et si on excepte le code trivial $C = \mathbb{F}_q^n$ pour lequel $g = 1$, *il existe autant de codes cycliques de longueur n sur $\mathbb{F}_q$ que de diviseurs unitaires propres du polynôme $X^n - 1$ dans l'anneau $\mathbb{F}_q[X]$*. Savoir décomposer le polynôme $X^n - 1$ dans l'anneau $\mathbb{F}_q[X]$ est donc essentiel pour définir des codes cycliques de longueur n.

> **Exercice 43** — Soit m un mot non nul de $\mathbb{F}_q^n$ et soit C_m le sous-espace vectoriel de $\mathbb{F}_q^n$ engendré par la famille $\{\sigma^i(m) \mid i = 0, 1, \ldots, n-1\}$. Montrer que
>
> 1. C_m est un code cyclique et que c'est le plus petit code cyclique contenant le mot m.
> 2. Le polynôme générateur du code C_m est le pgcd des polynômes $X^n - 1$ et $m(X)$.
> 3. Déterminer le code C_m et son polynôme générateur lorsque $q = 3$, $n = 9$ et $m = 022011000$.

Retour sur le code binaire de Hamming de longueur 7

Le code binaire de Hamming C_H de longueur 7 défini en 6.2.2 (page 74) est engendré par les mots $l_1 = 1101000$ et les trois mots qui s'en déduisent par décalage à droite $l_2 = 0110100$, $l_3 = 0011010$ et $l_4 = 0001101$.
Pour qu'il soit cyclique, il suffit que $\sigma(l_4) \in C_H$, or $\sigma(l_4) = 1000110 = l_1 + l_2 + l_3$.
L'examen de la liste des mots de code page 74 montre que le mot minimal est $l_1 = 1101000$, le polynôme générateur de C_H est donc le polynôme

$$g = l_1(X) = 1 + X + X^3,$$

polynôme qui divise $X^7 - 1$ puisque $X^7 - 1 = (1 + X + X^3)(1 + X + X^2 + X^4)$.

6.3.2 Matrice génératrice d'un code cyclique

Il résulte du point 1. du théorème 6.22 (page 80) qu'on peut construire une matrice génératrice d'un code cyclique à partir du mot minimal de ce code, ou, ce qui revient au même, de son polynôme générateur.

Théorème 6.25 *Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$ et soit*

$$g = g_0 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r$$

son polynôme générateur, de degré $r = n - k$. La matrice à k lignes et n colonnes

$$G = \begin{pmatrix} g_0 & \dots & g_{r-1} & 1 & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & \dots & g_{r-1} & 1 & 0 \\ 0 & 0 & \dots & 0 & g_0 & \dots & g_{r-1} & 1 \end{pmatrix}$$

est une matrice génératrice de C.

Preuve : Résulte du théorème 6.22 et de la définition d'une matrice génératrice : la première ligne de G est le mot minimal de $\widetilde{m} \in C$, les lignes suivantes sont les décalés à droite de $\widetilde{m}$. □

Corollaire 6.26 *Tout code cyclique est systématique.*

Preuve : Cela résulte de la forme de la matrice G ci-dessus et du fait que $g_0 \neq 0$. □

Exemple De l'égalité $X^8 - 1 = (X^3 + X^2 + X + 1)(X^5 + X^4 + X + 1)$ dans $\mathbb{F}_2[X]$, on déduit que le code cyclique binaire de longueur 8 engendré par le polynôme $g = 1 + X + X^4 + X^5$ est de dimension 3 et admet pour matrice génératrice la matrice

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

6.3.3 Polynôme de contrôle et matrice de contrôle d'un code cyclique

Définition 6.10 *Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$, de polynôme générateur g. On appelle* ***polynôme de contrôle*** *de C le polynôme h, quotient de la division euclidienne dans $\mathbb{F}_q[X]$ du polynôme $X^n - 1$ par le polynôme g.*

Comme g est unitaire de degré $n - k$, le polynôme de contrôle h est unitaire de degré k.

Théorème 6.27 *Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, et soit*

$$h = h_0 + h_1 X + \cdots + h_{k-1} X^{k-1} + X^k$$

son polynôme de contrôle. La matrice à $(n - k)$ lignes et n colonnes

$$H = \begin{pmatrix} 1 & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & 1 & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & h_{k-1} & \dots & h_0 & 0 \\ 0 & 0 & \dots & 0 & 1 & h_{k-1} & \dots & h_0 \end{pmatrix}$$

est une matrice de contrôle de C.

Preuve : Soit $g = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$ le polynôme générateur de C. L'égalité

$$g(X)h(X) = X^n - 1$$

signifie qu'on a $(h_0 g_0 = -1)$ et que pour chaque entier $l = 1, \ldots, n-1$, on a

$$\sum_{i+j=l} h_i g_j = 0, \text{ avec } (h_j = 0 \text{ si } j > k) \text{ et } (g_i = 0 \text{ si } i > r). \tag{1}$$

La matrice H ci-dessus est de rang maximum $n-k$ et les relations (1) expriment que $H\,{}^tG = 0$, où G est la matrice génératrice de C définie par le théorème 6.25. La matrice H est donc une matrice de contrôle de C d'après la proposition 6.14 (page 76). □

Exercice 44 — Soit C un code cyclique de longueur n sur $\mathbb{F}_q$, et soit h son polynôme de contrôle. Montrer que pour tout mot $m \in \mathbb{F}_q^n$, on a $(m \in C)$ si et seulement si le polynôme $m(X)h(X)$ est divisible par le polynôme $X^n - 1$.

Exemples

1. Dans l'exemple précédent du code cyclique binaire de longueur 8 engendré par le polynôme $g = 1 + X + X^4 + X^5$, le polynôme de contrôle est $h = X^3 + X^2 + X + 1$.

   La matrice à 5 lignes et 8 colonnes

   $$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   est donc une matrice de contrôle de ce code.

2. On a vu que le code binaire de Hamming de longueur 7 est engendré par le polynôme $g = 1 + X + X^3$, et que $X^7 - 1 = (1 + X + X^3)(1 + X + X^2 + X^4)$.

   Son polynôme de contrôle est donc $h = X^4 + X^2 + X + 1$ et la matrice à 3 lignes et 7 colonnes

   $$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

   en est une matrice de contrôle.

6.3.4 Code binaire de Hamming de longueur $2^s - 1$

Autre approche du code binaire de Hamming de longueur 7 Le polynôme générateur $g = 1 + X + X^3$ de ce code est irréductible dans $\mathbb{F}_2[X]$. Désignons par $\mathbb{F}_8$ le corps $\mathbb{F}_2[X]/\langle g \rangle$, et par α la classe de X dans $\mathbb{F}_8$. Comme $\mathbb{F}_8^*$ est d'ordre premier 7, et $\alpha \neq 1$, α est un élément primitif de $\mathbb{F}_8$.
Comme $g \in \mathbb{F}_2[X]$, on a $g(\alpha^2) = (g(\alpha))^2 = 0$ et $g(\alpha^4) = (g(\alpha))^4 = 0$, on en déduit

$$g = (X - \alpha)(X - \alpha^2)(X - \alpha^4).$$

De même, pour tout $P \in \mathbb{F}_2[X]$, si $P(\alpha) = 0$, alors $P(\alpha^2) = P(\alpha^4) = 0$ et il en résulte que P est divisible par g, c'est-à-dire que $P(\alpha) = 0$ si et seulement si P est divisible par g dans $\mathbb{F}_2[X]$.
Soit $m = c_0\, c_1 \ldots c_6 \in \mathbb{F}_2^7$, il résulte du théorème 6.22 (page 80) que $m \in C_H$ si et seulement si le polynôme

$$m(X) = c_0 + c_1X + \cdots + c_6X^6$$

est divisible par g, ce qui équivaut d'après ce qui précède à $m(\alpha) = c_0 + c_1\alpha + \cdots + c_6\alpha^6 = 0$. Le code C_H apparaît donc comme le noyau de l'application linéaire u de $\mathbb{F}_2^7$ dans $\mathbb{F}_8$ définie par

$$\forall\, x_0\, x_1 \ldots x_6 \in \mathbb{F}_2^7, \quad u(x_0\, x_1 \ldots x_6) = \sum_{k=0}^{6} x_k \alpha^k.$$

Généralisation Rappelons (théorème 5.8 page 58) l'égalité suivante dans $\mathbb{F}_q[X]$

$$X^{q-1} - 1 = \prod_{a \in \mathbb{F}_q^*} (X - a).$$

Soit α un élément primitif de $\mathbb{F}_q$, le groupe $\mathbb{F}_q^*$ est décrit par l'ensemble des puissances α^i, qui sont toutes distinctes pour $i = 1, 2 \ldots, q-1$. On en déduit l'égalité

$$X^{q-1} - 1 = \prod_{i=1}^{q-1} (X - \alpha^i). \tag{1}$$

Soit $q = 2^s$, avec $s \geq 2$, soit $n = q - 1$ et soit u l'application linéaire de $\mathbb{F}_2^n$ dans $\mathbb{F}_q$ définie par

$$\forall\, x_0\, x_1 \ldots x_{n-1} \in \mathbb{F}_2^n, \quad u(x_0\, x_1 \ldots x_{n-1}) = \sum_{k=0}^{n-1} x_k\, \alpha^k.$$

Le code défini par $C_H = \ker(u)$ est appelé code binaire de Hamming de longueur $n = 2^s - 1$.
On montrera à titre d'exercice que C_H est un code cyclique parfait de dimension $k = 2^s - 1 - s$, de distance minimum $d = 3$ et de polynôme générateur

$$g = \prod_{i=0}^{s-1} (X - \alpha^{2^i}) \in \mathbb{F}_2[X],$$

lequel est un diviseur de $X^n - 1$ d'après l'égalité (1) ci-dessus.

6.3.5 Codes de Reed-Solomon

Ce sont des codes de Reed-Solomon qui sont utilisés pour la lecture des disques compacts, des DVD, et pour la télémétrie par satellite. Ces codes sont des codes cycliques de longueur $n = q - 1$, sur un corps $\mathbb{F}_q$ avec $q > 2$. Le plus souvent on prend $q = 2^s$ avec $s \geq 2$.
L'égalité (1) ci-dessus permet, en choisissant un entier k tel que $1 \leq k < n = q - 1$, de définir un polynôme g de degré $n - k$ qui divise le polynôme $X^n - 1$ dans $\mathbb{F}_q[X]$ en posant

$$g = \prod_{i=1}^{n-k} (X - \alpha^i) \in \mathbb{F}_q[X]. \tag{2}$$

Un code de Reed-Solomon de longueur n et de dimension k est un code cyclique engendré par un polynôme g de la forme (2) ci-dessus. Un code de Reed-Solomon est MDS, c'est-à-dire que sa distance minimum vérifie $d = n - k + 1$. (Cf exercice 46 page 87).
Lorsque $q = 2^s$, avec $s \geq 2$, $\mathbb{F}_q$ est un $\mathbb{F}_2$-espace vectoriel de dimension s, on représente chaque élément de $\mathbb{F}_q$ par une séquence de s bits 0 ou 1. Un mot de code s'écrit donc comme une suite de $2^s - 1$ séquences de s bits.
On en déduit donc un code binaire C' de longueur $sn = s(2^s - 1)$ et de dimension sk, dont la distance minimum est au moins égale à la distance minimum $d = q - k = 2^s - k$ du code C, et souvent strictement supérieure.

Les codes de Reed-Solomon ont un bon comportement vis à vis des "bouffées" d'erreurs causées, par exemple, par une rayure sur un disque. En effet, si $t = \lfloor (d-1)/2 \rfloor$ est la capacité de correction de C, le code est capable de corriger un nombre d'erreurs de transmission de bits qui ne modifient pas plus de t s-uples représentant les éléments de $\mathbb{F}_q$, autrement dit qui se répartissent dans au plus t des n tranches de s bits. Si ces erreurs sont groupées, ce nombre peut être nettement plus grand que t et peut atteindre le nombre st.
Un code de Reed-Solomon sur le corps $\mathbb{F}_{256}$, avec $n = 255$, $k = 251$ et $d = 5$ est utilisé pour la lecture des disques compacts. Comme $256 = 2^8$, chaque élément de $\mathbb{F}_{256}$ est représentable par un *octet*, un mot de code est donc constitué d'une suite de 255 octets. Le nombre des messages qu'il est possible d'encoder est quasi-illimité : $q^k = 256^{251} = 2^{2008} \approx 3.10^{604}$, bien supérieur au nombre, estimé à 10^{80}, des particules de l'univers. Sa matrice de contrôle ne possède que 4 lignes. Le code de Reed-Solomon $(255, 251, 5)$ corrige 2 octets entachés d'erreurs, c'est-à-dire jusqu'à 16 erreurs de bits si ces erreurs sont groupées.

Exercice 45 — Exemple d'un code de Reed-Solomon.
Soit $\mathbb{F}_8 = \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$ et soit $\alpha = \overline{X}$.

1. Montrer que α est un élément primitif de $\mathbb{F}_8$.
2. Écrire la table des logarithmes de base α.
3. Soient $g \in \mathbb{F}_8[X]$ le diviseur unitaire de $(X^7 - 1)$ défini par
$$g = (X - \alpha)(X - \alpha^2).$$
Montrer que $g = X^2 + \alpha^4 X + \alpha^3$.
4. Écrire une matrice génératrice du code (de Reed-Solomon) C de longueur 7 engendré par g.
5. Déterminer le polynôme de contrôle et une matrice de contrôle de C.
6. En déduire que C est MDS.
7. Corriger le mot reçu $\alpha^3\alpha^2\alpha\alpha^4\alpha\alpha^4 1$.

Exercice 46 — Soit α un élément primitif du corps $\mathbb{F}_q$. On pose $n = q - 1$ et on considère un entier k vérifiant $1 \leq k \leq n - 1$. Soit $P \in \mathbb{F}_q[X]$ un polynôme de degré $\leq n - 1$ possédant au plus $(n - k)$ coefficients non nuls.

1. Montrer que P peut s'écrire sous la forme $P = \sum_{i=1}^{n-k} c_i X^{d_i}$, où les d_i sont $n-k$ entiers vérifiant
$$0 \leq d_1 < \cdots < d_{n-k} \leq n - 1.$$
2. On pose $a_i = \alpha^{d_i}$ pour chaque $i = 1, 2, \ldots, n - k$. Montrer que le déterminant de Vandermonde
$$D = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-k-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{n-k} & a_{n-k}^2 & \cdots & a_{n-k}^{n-k-1} \end{vmatrix}$$
associée au $(n - k)$-uple $(a_1, a_2, \ldots, a_{n-k})$ est non nul.
3. En déduire que si $P(\alpha^i) = 0$ pour tout entier $i = 1, 2, \ldots, n - k$, alors $P = 0$.
4. En déduire que la distance minimum d du code de Reed-Solomon de dimension k défini en section 6.3.5 vérifie $d \geq n - k + 1$, donc que ce code est MDS.