Université Paris-Saclay
M1 Agrégation – Formation à l'Enseignement Supérieur

Année 2021–2022

M1 – Mathématiques générales 2

Anne Moreau

anne.moreau@universite-paris-saclay.fr
https://www.imo.universite-paris-saclay.fr/~moreau/

Ferdinand Georg Frobenius, *connu aussi sous le nom de Georg Frobenius, est un mathématicien allemand, né le 26 octobre 1849 à Charlottenbourg (Prusse, aujourd'hui sous-municipalité de Berlin) et mort le 3 août 1917 à Berlin. Durant la deuxième moitié de sa carrière, la théorie des groupes a constitué l'un des principaux intérêts de Frobenius. L'une de ses premières contributions a été la redémonstration des théorèmes de Sylow pour un groupe abstrait (la preuve originelle de Sylow était formulée pour un groupe de permutations). La démonstration du premier théorème de Sylow (sur l'existence des sous-groupes de Sylow) élaborée par Frobenius est encore la plus enseignée de nos jours.*

Évariste Galois, *est un mathématicien français, né le 25 octobre 1811 à Bourg-Égalité (aujourd'hui Bourg-la-Reine) et mort le 31 mai 1832 à Paris. Son nom a été donné à une branche des mathématiques dont il a posé les prémices, la théorie de Galois. Il est un précurseur dans la mise en évidence de la notion de groupe et un des premiers à expliciter la correspondance entre symétries et invariants. Sa « théorie de l'ambiguïté » est toujours féconde au XXIième siècle.*

Table des matières

1

Représentations linéaires des groupes finis

Prérequis : théorie des groupes (notions de groupe, groupe abélien, sous-groupe, morphisme de groupe, action de groupes, produits direct et semi-direct), algèbre linéaire et bilinéaire.

Dans ce chapitre, nous allons nous intéresser aux *représentations linéaires* des groupes finis, c'est-à-dire aux morphismes de groupes $G \to \mathrm{GL}(V)$, où V est un espace vectoriel (de dimension finie le plus souvent) et G est un groupe fini ; voir la section 2 pour une définition plus précise.

Ce chapitre suit pour une large part les chapitres 1, 2, 3 et 5 de [2].

1. Exemples importants de groupes finis

Comme il est bon d'avoir à l'esprit des exemples, nous commençons le cours par des exemples variés et concrets de groupes finis, importants en géométrie notamment, qui illustreront les principaux résultats du chapitre.

On note $\mathfrak{S}_n$ le ***groupe symétrique de degré*** n, c'est-à-dire le groupe des permutations de l'ensemble $\{1, \dots, n\}$. On rappelle que ce groupe est muni d'un morphisme surjectif

$$\varepsilon \colon \mathfrak{S}_n \to \{\pm 1\},$$

appelé la ***signature***. Son noyau est formé des permutations ***paires*** σ, i.e., $\varepsilon(\sigma) = 1$. C'est un sous-groupe de $\mathfrak{S}_n$ de cardinal $n!/2$, appelé le ***groupe alterné de degré*** n, et noté $\mathfrak{A}_n$.

1.1. Le groupe cyclique Γ_n. Rappelons que le ***groupe cyclique*** Γ_n est le groupe d'ordre n formé des puissances $1, r, \dots, r^{n-1}$ d'un élément r tel que $r^n = 1$. C'est un groupe abélien, isomorphe à $\mathbb{Z}/n\mathbb{Z}$, qui peut être réalisé comme le groupe des rotations d'un plan euclidien orienté d'angle $2k\pi/n$, $k = 0, \dots, n-1$.

1.2. Le groupe diédral D_n. Il s'agit du groupe des isométries du plan affine qui préservent un polygone régulier à n côtés centré à l'origine O. Il contient les n rotations $r_{O,2k\pi/n}$, $k = 0, \dots, n-1$ qui forment un sous-groupe cyclique Γ_n isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et les n réflexions (ou symétries) par rapport aux droites passant par O et les sommets ou milieux des côtés opposés du polygone (selon la parité de n). L'ordre du ***groupe diédral*** D_n est donc $2n$. On note r la rotation $r_{O,2\pi/n}$ et s l'une des réflexions de D_n. On a

$$r^n = 1, \qquad s^2 = 1, \qquad srs = srs^{-1} = r^{-1}.$$

Les éléments de D_n sont ou bien de la forme r^k, $k = 0, \dots, n-1$ (s'ils appartiennent au groupe cyclique Γ_n), ou bien de la forme sr^k, $k = 0, \dots, n-1$ (s'ils n'appartiennent pas à Γ_n). On remarque que pour tout $k = 0, \dots, n-1$, $sr^k s = sr^k s^{-1} = r^{-k}$, d'où $(sr^k)^2 = 1$.

Exercice de cours 1.

1. Montrer que le groupe Γ_n est distingué dans D_n et que l'on a un isomorphisme
$$D_n \cong \Gamma_n \rtimes \mathbb{Z}/2\mathbb{Z}.$$
2. Vérifier que l'on a $D_3 \cong \mathfrak{S}_3$.

Exercice de cours 2.

1. On suppose que n est pair. Montrer que les réflexions forment deux classes de conjugaison et les rotations forment $\frac{n}{2}+1$ classes de conjugaisons.
2. On suppose que n est impair. Montrer que les réflexions forment une seule classe de conjugaison et les rotations forment $\frac{n+1}{2}$ classes de conjugaisons.

1.3. Le groupe alterné $\mathfrak{A}_4$. Rappelons que $\mathfrak{A}_4$ est le groupe des permutations paires de $\{1,2,3,4\}$. Il est isomorphe au groupe des rotations dans l'espace affine orienté $\mathbb{R}^3$ qui préservent un tétraèdre régulier dont l'isobarycentre est l'origine O.

Il possède 12 éléments :
- l'identité,
- 3 éléments d'ordre 2, $x=(1\,2)(3\,4)$, $y=(1\,3)(2\,4)$, $z=(1\,4)(2\,3)$, qui correspondent aux *retournements* (ou rotations d'angle π par rapport à un axe) du tétraèdre relatives aux droites joignant les milieux de deux arrêtes opposées,
- 8 éléments d'ordre 3, $(1\,2\,3),(1\,3\,2),(2\,3\,4),(2\,4\,3),(1\,2\,4),(1\,4\,2),(1\,3\,4),(1\,4\,3)$, qui correspondent aux rotations d'angle $\pm\frac{2\pi}{3}$ et d'axe les droites joignant un sommet au barycentre de la face opposée.

Comme d'habitude, on a noté $(a_1 \dots a_k)$ le **k-cycle** *de $\mathfrak{S}_n$ qui envoie a_1 sur a_2, a_2 sur a_3, …, a_{k-1} sur a_k, a_k sur a_1 et fixe tous les éléments de $\{1,\dots,n\}\setminus\{a_1,\dots,a_k\}$.*

Exercice de cours 3. Faire un dessin et vérifier toutes les assertions précédentes.

On pose $c=(123)$, $H=\{1,c,c^2\}$ et $K=\{1,x,y,z\}$. On a

$$cxt^{-1}=z, \qquad czc^{-1}=y, \qquad cyc^{-1}=x.$$

Exercice de cours 4.

1. Vérifier que H et K sont des sous-groupes de $\mathfrak{A}_4$ et que K est distingué dans $\mathfrak{A}_4$. Montrer que
$$\mathfrak{A}_4 \cong K \rtimes H,$$
et que le produit n'est pas direct.
2. Montrer qu'il y a quatre classes de conjugaison dans $\mathfrak{A}_4$ que l'on explicitera.

1.4. Le groupe symétrique $\mathfrak{S}_4$. Il s'agit du groupe des permutations de $\{1,2,3,4\}$. Il est isomorphe au groupe de toutes les isométries de $\mathbb{R}^3$ qui préservent un tétraèdre régulier dont l'isobarycentre est l'origine O.

Il possède 24 éléments :
- l'identité,
- 6 transpositions, $(1\,2),(1\,3),(1\,4),(2\,3),(2\,4),(3\,4)$,
- les 3 éléments d'ordre 2 de $\mathfrak{A}_4$, x,y,z,
- les 8 éléments d'ordre 3 de $\mathfrak{A}_4$,
- 6 éléments d'ordre 4, $(1\,2\,3\,4),(1\,2\,4\,3),(1\,3\,2\,4),(1\,3\,4\,2),(1\,4\,2\,3),(1\,4\,3\,2)$.

⚠ Les permutations d'ordre 4 sont les plus difficiles à visualiser sous forme d'isométries !

Exercice de cours 5.

1. Faire un dessin, vérifier les assertions précédentes et interpréter géométriquement les « nouveaux » éléments, c'est-à-dire ceux de $\mathfrak{S}_4\setminus\mathfrak{A}_4$.
2. Combien y a-t-il de classes de conjugaison dans $\mathfrak{S}_4$?
3. Soient $K=\{1,x,y,z\}$ et $L\cong\mathfrak{S}_3$ le groupe des permutations de $\mathfrak{S}_4$ qui fixe 4. Montrer que
$$\mathfrak{S}_4 \cong K \rtimes L.$$

1.5. Le groupe du cube. Considérons dans $\mathbb{R}^3$ le cube $\mathcal{C}$ dont les sommets ont pour coordonnées (x,y,z) avec $x=\pm1$, $y=\pm1$, $z=\pm1$. Soit $\mathrm{Iso}(\mathcal{C})$ le groupe des isométries de $\mathbb{R}^3$ qui préservent $\mathcal{C}$, i.e., qui permutent ces 8 sommets.

Ce groupe peut être décrit de différentes façons.

a) En faisant opérer $\mathrm{Iso}(\mathcal{C})$ *sur l'ensemble des diagonales du cube.* Soit $\mathscr{D}$ l'ensemble des grandes diagonales du cube $\mathcal{C}$. En notant A_i les quatre sommets de coordonnées $(\pm 1, \pm 1, 1)$ et B_i les quatre sommets de coordonnées $(\mp 1, \mp 1, -1)$, ces diagonales sont les quatre droites (A_iB_i), $i = 1, 2, 3, 4$.

Exercice de cours 6.

1. Déterminer le cardinal de $\mathrm{Iso}(\mathcal{C})$. (*Indication : on pourra faire opérer* $\mathrm{Iso}(\mathcal{C})$ *sur l'ensemble des sommets de* $\mathcal{C}$ *et déterminer le cardinal du stabilisateur d'un sommet. Il y a d'autres façons de faire !*)
2. Montrer que $\mathrm{Iso}(\mathcal{C})$ opère sur l'ensemble $\mathscr{D}$, et que le morphisme de groupes induit par cette opération,
$$\mathrm{Iso}(\mathcal{C}) \longrightarrow \mathfrak{S}(\mathscr{D}) \cong \mathfrak{S}_4,$$
est surjectif. Quel est son noyau ?
3. Montrer que l'on a
$$\mathrm{Iso}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}.$$
Combien y a-t-il de classes de conjugaison dans G ?
4. Montrer que le sous-groupe de $\mathrm{Iso}(\mathcal{C})$ formé par les rotations de $\mathbb{R}^3$ qui préservent le cube $\mathcal{C}$ est isomorphe à $\mathfrak{S}_4$.

b) À l'aide d'un tétraèdre. On note $\mathcal{T}$ le tétraèdre dont les sommets sont les points de coordonnées $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, $(-1, -1, 1)$.

⚠ $\mathcal{T}$ n'est pas un tétraèdre régulier !

On pose $\mathcal{T}' = (-I)\mathcal{T} = -\mathcal{T}$, où I désigne l'identité de $\mathbb{R}^3$. Chaque sommet de $\mathcal{C}$ est ou bien un sommet de $\mathcal{T}$ ou bien un sommet de $\mathcal{T}'$. Soit $\mathrm{Iso}(\mathcal{T})$ le groupe des automorphismes de $\mathbb{R}^3$ qui préservent $\mathcal{T}$.

Pour tout $s \in \mathrm{Iso}(\mathcal{T})$, on a
$$s\mathcal{T}' = s(-I)\mathcal{T} = (-I)\mathrm{Iso}(\mathcal{T}) = (-I)\mathcal{T} = \mathcal{T}',$$
et donc s préserve tous les sommets de $\mathcal{C}$, donc préserve $\mathcal{C}$. On en déduit que $\mathrm{Iso}(\mathcal{T}) \subset \mathrm{Iso}(\mathcal{C})$.

Exercice de cours 7. En utilisant, par exemple, le cardinal de $\mathrm{Iso}(\mathcal{C})$, montrer que l'on a
$$\mathrm{Iso}(\mathcal{C}) = \mathrm{Iso}(\mathcal{T}) \times \{I, -I\}.$$

Comme $\mathrm{Iso}(\mathcal{T}) \cong \mathfrak{S}_4$, on retrouve que $\mathrm{Iso}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$. En effet, bien que $\mathcal{T}$ ne soit pas régulier, on peut montrer comme dans au paragraphe précédent que $\mathrm{Iso}(\mathcal{T}) \cong \mathfrak{S}_4$ en considérant les automorphismes de $\mathbb{R}^3$ qui préservent $\mathcal{T}$.

c) À l'aide du groupe $\mathfrak{S}_3$. Observons que le groupe $\mathrm{Iso}(\mathcal{C})$ contient le groupe $\mathfrak{S}_3$ des permutations de $\{x, y, z\}$ (on permute les coordonnées), ainsi que le groupe M d'ordre 8 formé de toutes les transformations
$$(x, y, z) \longmapsto (\pm x, \pm y, \pm z).$$

Exercice de cours 8.

1. Vérifier que l'on a $\mathrm{Iso}(\mathcal{C}) = M \rtimes \mathfrak{S}_3$ (on retrouve ainsi que $\mathrm{Iso}(\mathcal{C})$ est d'ordre $8 \times 6 = 48$).
2. Retrouver la décomposition $\mathrm{Iso}(\mathcal{C}) = M \rtimes \mathfrak{S}_3$ à partir de la décomposition $\mathrm{Iso}(\mathcal{C}) = \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et de la décomposition $\mathfrak{S}_4 = K \rtimes \mathfrak{S}_3$ (voir l'exercice 5).

2. Définition, sous-représentations, morphismes et sommes directes

Soient V un espace vectoriel défini sur le corps $\mathbb{C}$ des nombres complexes, et $\mathrm{GL}(V)$ le groupe des automorphismes de V. Soit maintenant G un groupe fini. On notera, comme d'habitude, 1 son élément neutre et $(s, t) \mapsto st$ la multiplication dans G.

Définition 1 – représentation linéaire d'un groupe fini

Une ***représentation linéaire*** (ou, simplement, ***représentation***) de G est un morphisme de groupes $\rho\colon G \to \mathrm{GL}(V)$ de G dans $\mathrm{GL}(V)$. Autrement dit, à tout élément s de G, on associe un élément $\rho(s)$ de $\mathrm{GL}(V)$ de sorte que, pour tous $s, t \in G$,

$$\rho(st) = \rho(s) \circ \rho(t).$$

En particulier, $\rho(1) = I$ et $\rho(s^{-1}) = \rho(s)^{-1}$ pour tout $s \in G$, où I désigne l'identité de V.

(On notera souvent ρ_s au lieu de $\rho(s)$ pour éviter l'écriture peu élégante $\rho(s)(x)$, $s \in G$, $x \in V$.)

Lorsque ρ est donné, on dit que V est ***l'espace d'une représentation***. Parfois, par abus et lorsqu'il n'y a pas d'ambiguïté sur ρ, on dit que V est une représentation de G.

Dans toute la suite, on se restreint au cas où V est de dimension finie, que l'on notera n. On dit que n est le ***degré*** de la représentation (ρ, V).

Exemple 1.

1. Une représentation de degré 1 de G est un morphisme de groupes $\rho\colon G \to \mathbb{C}^*$, où $\mathbb{C}^*$ est le groupe multiplicatif. Comme tout élément de G est d'ordre fini, les éléments $\rho(s)$ sont des racines de l'unité. En particulier $|\rho(s)| = 1$.

Si $\rho(s) = 1$ pour tout $s \in G$, on obtient la représentation dite ***triviale*** de G.

2. Soient g l'ordre de G, V un espace vectoriel de dimension $n = g$ et $(e_t)_{t\in G}$ une base de V indexée par les éléments de G. Pour $s \in G$, on note ρ_s l'endomorphisme de V qui envoie e_t sur e_{st}. Ceci définit une représentation linéaire de G, appelée la ***représentation régulière*** de G. Son degré est l'ordre du groupe.

Exercice de cours 9 (représentations de degré 1 du groupe cyclique). Quelles sont les représentations de degré 1 groupe cyclique Γ_n (voir le paragraphe 1.1) ?

Exemple 2.

1. Le groupe diédral opère naturellement dans $\mathbb{R}^2$ et donc dans $\mathbb{C}^2$ (on étend par linéarité). Cette opération induit une représentation de degré 2 de D_n.

2. Les groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$ et le groupe du cube $\mathrm{Iso}(\mathcal{C})$ opèrent naturellement dans $\mathbb{R}^3$ et donc dans $\mathbb{C}^3$. Ces opérations induisent des représentations de degré 3 de $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathrm{Iso}(\mathcal{C})$.

Définition 2 – représentations isomorphes

Soient ρ et ρ' deux représentations du même groupe G d'espaces respectifs V et V'. On dit que les représentations ρ et ρ' sont ***isomorphes*** (ou ***équivalentes***) s'il existe un isomorphisme d'espaces vectoriels $\tau\colon V \to V'$ tel que pour tout $s \in G$,

$$\tau \circ \rho_s = \rho'_s \circ \tau.$$

En particulier, V et V' ont même dimension si ρ et ρ' sont isomorphes.

Exercice de cours 10 (interprétation matricielle d'un isomorphisme de représentations). Soient $(e_1, \ldots, e_n)$ une base de V, et $(e'_1, \ldots, e'_n)$ une base de V'. On note, pour tout $s \in G$, R_s et R'_s les matrices de ρ_s et ρ'_s dans cette base. Interpréter matriciellement le fait que ρ et ρ' soient isomorphes.

Exercice de cours 11.

1. Soit (ρ, V) la représentation régulière de G. Vérifier que les images $\rho_s(e_1)$ forment une base de V, si s parcours G.

2. Réciproquement, soit $\rho\colon G \to \mathrm{GL}(W)$ une représentation de G telle qu'il existe $w \in W$ tel que les éléments $\rho_s(w)$, $s \in G$, forment une base de W. Montrer que W est isomorphe à la représentation régulière.

On généralise l'exemple précédent de la représentation régulière.

Exemple 3. On suppose que G opère dans un ensemble fini X. Autrement dit, pour tout $s \in G$, il existe une permutation, $\tau_s \colon X \to X, x \to s.x$, de X telle que

$$1.x = x, \quad s.(t.x) = (st).x, \qquad \forall\, s,t \in G,\ x \in X.$$

Soient V un espace vectoriel possédant une base $(e_x)_{x\in X}$ indexée par les éléments de X. Pour $s \in G$, soit ρ_s l'endomorphisme de V qui envoie e_x sur $e_{s.x}$. La représentation linéaire de G ainsi obtenue est appelée la ***représentation par permutations associée à l'action de*** G ***sur*** X.

Soient $\rho \colon G \to \mathrm{GL}(V)$ une représentation de G, et W un sous-espace vectoriel de V. Supposons que W soit ***stable*** (ou ***invariant***) sous l'action de G, c'est-à-dire que $\rho_s(W) \subset W$ pour tout $s \in G$.

L'endomorphisme induit $\rho_s^W : W \to W$ est alors un automorphisme de W et on a

$$\rho_{st}^W = \rho_s^W \rho_t^W, \qquad \forall\, s,t \in G.$$

Par conséquent, l'application $\rho^W : G \to \mathrm{GL}(W)$, $s \mapsto \rho_s^W$ définit une représentation linéaire de W.

Définition 3 – sous-représentation

Dans les notations précédentes, si W est un sous-espace de V stable par l'action de G, la représentation ρ^W est appelée une ***sous-représentation*** de V.

Exemple 4. Supposons que V soit la représentation régulière de G. Soit W la droite de V engendrée par $x = \sum_{s\in G} e_s$. On a $\rho_s x = x$ pour tout x donc W est une sous-représentation de V, isomorphe à la représentation triviale.

Théorème 4 – tout sous-espace stable admet un supplémentaire stable

Soient $\rho \colon V \to \mathrm{GL}(V)$ une représentation linéaire de G, et W un sous-espace de V stable par G. Alors il existe un supplémentaire W^0 de W dans V qui est stable par G.

Exercice de cours 12 (démonstration du théorème 4). L'objectif de cet exercice est de démontrer le théorème.

1. Soient W' n'importe quel supplémentaire W dans V (il en existe !) et p la projection vectorielle de V sur W de direction W'. On pose

$$p^0 = \frac{1}{g} \sum_{t\in G} \rho_t \circ p \circ \rho_t^{-1}, \quad \text{où } g \text{ est l'odre de } G.$$

(p^0 *est une « moyenne » des conjugués de* p *par les éléments de* G.)
Montrer que p^0 est une projection vectorielle de V sur W ; on note W^0 sa direction.

2. Montrer que pour tout $s \in G$,

$$\rho_s \circ p^0 = p^0 \circ \rho_s.$$

3. En déduire que W^0 est stable par G. Conclure.

Remarque 1 (une autre démonstration). Supposons que V soit muni d'un produit scalaire hermitien $(x|y)$ (i.e., $(\ |\ )$ est linéaire à gauche, semi-linéaire à droite et défini positif) ; c'est toujours le cas ! Supposons de plus que $(\ |\ )$ soit ***invariant*** par G, c'est-à-dire que pour tout $s \in G$ et tous $x, y \in V$,

$$(\rho_s(x)|\rho_s(y)) = (x|y).$$

On peut toujours se ramener à ce cas en remplaçant $(x|y)$ par $\sum_{t\in G} (\rho_t(x)|\rho_t(y))$. Sous ces hypothèses, l'orthogonal $W^0 = W^\perp$ fournit un supplémentaire stable par G. On a ainsi obtenu une autre démonstration du théorème 4.

L'invariance du produit scalaire signifie que tous les éléments ρ_s, $s \in G$, sont des endomorphismes unitaires (i.e., dont la matrice R_s dans une base orthonormée vérifie $R_s R_s^* = I_n$, où $R_s^* = \overline{R_s}^T$ est la matrice adjointe de R_s). Il est bien connu que tout sous-espace stable par un endomorphisme unitaire admet un supplémentaire stable par cet endomorphisme. Nous obtenons ici une version « simultanée » de ce résultat.

Soient $x \in V$, que l'on écrit $x = w + w^0$ selon la décomposition $V = W \oplus W^0$ donnée par le théorème 4. Comme W et W^0 sont stables par G, on a pour tout $s \in G$,

$$\rho_s(x) = \underbrace{\rho_s(w)}_{\in W} + \underbrace{\rho_s(w^0)}_{\in W^0}.$$

de sorte que $\rho_s(w)$ est $\rho_s(w^0)$ sont les composantes de $\rho_s(x)$ selon W et W^0 respectivement. Il en résulte que les sous-représentations W et W^0 déterminent entièrement la représentation V.

Définition 5 – somme directe de sous-représentations

Dans ces conditions, on dit que V est la ***somme directe*** de W et W^0 (en tant que représentation de G) et on note $V = W \oplus W^0$. On définit de même la somme directe d'un nombre fini de sous-représentations.

Exercice de cours 13. Interpréter matriciellement le théorème 4 et cette définition.

Définition 6 – représentation irréductible

Soit $\rho\colon G \to \mathrm{GL}(V)$ une représentation de G. On dit qu'elle est ***irréductible*** ou ***simple*** si $V \neq \{0\}$ et si les seuls sous-espaces stables par G sont $\{0\}$ et V.

D'après le théorème 4, une représentation est donc irréductible si et seulement si elle n'est pas somme directe de deux sous-représentations non triviales.

Une représentation de degré 1 est toujours irréductible. Nous verrons plus loin que tout groupe non abélien possède au moins une représentation irréductible de degré $\geqslant 2$ (voir la proposition 16).

Théorème 7 – complète réductibilité des représentations

Toute représentation d'un groupe fini est la somme directe de représentations irréductibles.

Exercice de cours 14. Démontrer ce théorème par récurrence et à l'aide du théorème 4.

Remarque 2. En général, une décomposition $V = W_1 \oplus \cdots \oplus W_k$ en somme directe de représentations irréductibles n'est pas unique. Par exemple, si tous les ρ_s sont égaux à 1, les sous-espaces W_i sont tous des droites, et la décomposition n'est certainement pas unique puisqu'il y a pléthore de décompositions de V en somme de droites vectorielles. Nous verrons que, toutefois, le nombre de W_i isomorphes à une représentation irréductible donnée ne dépend pas de la décomposition choisie (voir le théorème 12).

Exercice de cours 15. Le groupe symétrique $\mathfrak{S}_3$ opère dans $\mathbb{C}^3$ par $s.(x_1, x_2, x_3) = (x_{s(1)}, x_{s(2)}, x_{s(3)})$ (permutations des coordonnées) et cela définit une représentation de $\mathfrak{S}_3$ de degré 3. Cette représentation est-elle irréductible ? Si non, trouver une décomposition de $\mathbb{C}^3$ en une somme directe de sous-représentations de $\mathfrak{S}_3$.

Exercice de cours 16 (représentations irréductibles de degré 1 et 2 du groupe diédral). On considère le groupe diédral D_n (voir le paragraphe 1.2).

1. Trouver toutes les représentations de degré 1 de D_n. (*On distinguera les cas selon la parité de n.*)
2. On construit dans cette question des représentations irréductibles de degré 2. Posons $w = e^{2i\pi/n}$. On rappelle que D_n opère naturellement dans $\mathbb{C}^2$ (voir l'exemple 2). Montrer qu'il existe une base $\mathscr{B}$ de $\mathbb{C}^2$ telle que la matrice de r^k dans cette base soit $\begin{pmatrix} w^k & 0 \\ 0 & w^{-k} \end{pmatrix}$ et celle de sr soit $\begin{pmatrix} 0 & w^{-k} \\ w^k & 0 \end{pmatrix}$.

3. Montrer que les formules suivantes définissent une représentation ρ^h de D_n d'espace $\mathbb{C}^2$ pour tout $h \in \mathbb{N}$:

$$\rho^h(r^k) = \begin{pmatrix} w^{hk} & 0 \\ 0 & w^{-hk} \end{pmatrix}, \qquad \rho^h(sr^k) = \begin{pmatrix} 0 & w^{-hk} \\ w^{hk} & 0 \end{pmatrix}, \qquad k = 0, \dots, n-1,$$

où l'on identifie, pour $t \in D_n$, $\rho^h(t)$ à sa matrice dans la base $\mathscr{B}$.

Ces représentations ne dépendent que de $h \bmod n$. De plus, ρ^h et ρ^{n-h} sont isomorphes. On peut donc supposer que $h = 0, \dots, n/2$.

4. Montrer que ρ^0 et $\rho^{n/2}$ (si n est paire) sont réductibles, et que les autres ρ^h, $0 < h < n/2$, sont irréductibles et deux à deux non isomorphes.

Nous verrons plus loin que les représentation irréductibles obtenues dans cet exercice sont les seules représentations irréductibles du groupe diédral D_n (voir l'exercice 38).

3. Lemme de Schur et applications

La proposition suivante est très célèbre. Elle est connue sous le nom de *Lemme de Schur*.

Proposition 8 – lemme de Schur

Soient $\rho^1 : G \to \mathrm{GL}(V_1)$ et $\rho^2 : G \to \mathrm{GL}(V_2)$ deux représentations irréductibles de G, et soit f une application linéaire de V_1 dans V_2 telle que $\rho^2_s \circ f = f \circ \rho^1_s$ pour tout $s \in G$.

1. Si ρ^1 et ρ^2 ne sont pas isomorphes, alors $f = 0$,

2. Si $V_1 = V_2$ et si $\rho^1 = \rho^2$, alors f est une homothétie.

***Issaï Schur**, né à Moguilev le 10 janvier 1875 et mort à Tel-Aviv le 10 janvier 1941, est un mathématicien d'origine russe qui a surtout travaillé en Allemagne. Son nom est aussi transcrit Issaï Chour (transcription du russe en français).*

Exercice de cours 17 (démonstration du lemme de Schur).

1. Comme le cas $f = 0$ est trivial, on suppose que $f \neq 0$.

1.1 Montrer que le noyau W_1 de f est stable par G ; en déduire que $W_1 = 0$.

1.2 Montrer que l'image W_2 de f est stable par G ; en déduire que $W_2 = V_2$.

1.3 Conclure pour la partie (1).

2. On suppose que $V_1 = V_2$ et $\rho^1 = \rho^2$ de sorte que f est un endomorphisme de V_1. Soit λ une valeur propre de f (il en existe !) et posons $f' = f - \lambda I$. À l'aide de la partie (1), montrer que $f' = 0$ et conclure.

Corollaire 9 – une application technique du lemme de Schur

Soit $h \in \mathscr{L}(V_1, V_2)$ une application linéaire de V_1 dans V_2, où V_1, V_2 sont des représentations irréductibles de G. On pose

$$h^0 = \frac{1}{g} \sum_{t \in G} (\rho_t^2)^{-1} h \rho_t^1.$$

1. Si ρ^1 et ρ^2 ne sont pas isomorphes, alors $h^0 = 0$,
2. Si $V_1 = V_2$ et si $\rho^1 = \rho^2$, alors h^0 est une homothétie de rapport $\frac{1}{n}\operatorname{Tr}(h)$, où $n = \dim V_1$.

Exercice de cours 18. Démontrer le corollaire.

Voici pour terminer cette section une jolie application du lemme de Schur.

Exercice de cours 19 (les représentations irréductibles d'un groupe abélien sont de dégré 1). Soit G une groupe abélien fini. Montrer à l'aide du lemme de Schur que toute représentation de G est de degré 1. (*Remarque : on peut aussi penser à la diagonalisation simultanée, sans le lemme de Schur, mais c'est la même idée sous-jacente.*)

4. Théorie des caractères

4.1. Caractère d'une représentation. Soit $\rho\colon G \to \mathrm{GL}(V)$ une représentation de G. Pour tout $s \in G$, on pose

$$\boxed{\chi_\rho(s) = \operatorname{Tr}(\rho_s)}$$

où $\operatorname{Tr}(\rho_s)$ est la trace de l'endomorphisme ρ_s (c'est-à-dire la trace de sa matrice dans n'importe quelle base de V).

Définition 10 – caractère d'une représentation

La fonction $\chi_\rho\colon G \to \mathbb{C}$ est appelée le ***caractère*** de la représentation ρ.

La terminologie vient de ce que le caractère χ_ρ *caractérise* la représentation, comme nous le verrons plus loin (voir le corollaire 13).

Exercice de cours 20. Soit χ le caractère d'une représentation ρ de degré n. Montrer :
(i) $\chi(1) = n$,
(ii) $\chi(s^{-1}) = \overline{\chi(s)}$ pour tout $s \in G$,
(iii) $\chi(tst^{-1}) = \chi(s)$ pour tous $s, t \in G$.

On appelle ***fonction centrale*** une fonction $f\colon G \to \mathbb{C}$ qui est constante sur les classes de conjugaison, i.e.,

$$f(tst^{-1}) = f(s), \qquad \forall\, s, t \in G.$$

Le caractère d'une représentation de G est donc une fonction centrale d'après la propriété (iii) de l'exercice 20.

Exercice de cours 21. Soient $\rho^1\colon G \to \mathrm{GL}(V_1)$ et $\rho^2\colon G \to \mathrm{GL}(V_2)$ deux représentations de G, et χ_1, χ_2 les caractères associés. Que vaut le caractère de la représentation $\rho\colon G \to V = V_1 \oplus V_2$ définie par

$$\rho_s(x_1 + x_2) = \rho_s^1(x_1) + \rho_s^2(x_2), \qquad \forall\, s \in G,\ (x_1, x_2) \in V_1 \times V_2,$$

en fonction de χ_1 et χ_2 ?

Il serait plus correct d'écrire $V = V_1 \times V_2$. Comme $V_1 \times V_2 = (V_1 \times \{0\}) \oplus (\{0\} \times V_2)$, on s'autorise l'écriture $V = V_1 \oplus V_2$ et $V_1 \cong V_1 \times \{0\}$ et $V_2 \cong \{0\} \times V_2$ sont des sous-représentations de $V_1 \times V_2$.

Exercice de cours 22 (caractère de la représentation par permutations). Soit X un ensemble sur lequel agit le groupe G. On note $\rho\colon G \to \mathrm{GL}(V)$ la représentation par permutations associée à l'action de G (voir l'exemple 3), et χ son caractère. Montrer que pour tout $s \in G$, $\chi(s)$ est égal au nombre d'éléments de X fixés par G, i.e.,

$$\chi(s) = \#\{x \in X : s.x = x\}.$$

Exercice de cours 23 (représentation contragrédiante). Soient $\rho\colon G \to \mathrm{GL}(V)$ une représentation de G de caractère χ, et V' le dual de V (i.e., $V' = \mathscr{L}(V, \mathbb{C})$ est l'ensemble des formes linéaires de V). On écrit $\langle x', x\rangle$ pour $x'(x)$ si $x \in V$ et $x' \in V'$. Montrer qu'il existe une unique représentation $\rho'\colon G \to \mathrm{GL}(V')$ telle que

$$\langle \rho'_s(x'), \rho_s(x)\rangle = \langle x', x\rangle, \qquad \forall\, s \in G,\ x \in V,\ x' \in V'.$$

On l'appelle la représentation ***contragrédiente*** ou ***duale*** de V. Quel est son caractère ?

4.2. Relations d'orthogonalité pour les caractères. On note $\mathscr{F}(G, \mathbb{C})$ l'ensemble des fonctions de G dans $\mathbb{C}$.

Exercice de cours 24. Vérifier que $\mathscr{F}(G, \mathbb{C})$ est un espace vectoriel complexe et montrer que $\mathscr{F}(G, \mathbb{C})$ est de dimension finie g égale au cardinal de G.

Soient $\psi\colon G \to \mathbb{C}$ et $\phi\colon G \to \mathbb{C}$ deux fonctions définies sur G. On pose

$$(\phi|\psi) = \frac{1}{g}\sum_{t\in G} \phi(t)\overline{\psi(t)}.$$

C'est un produit scalaire hermitien sur $\mathscr{F}(G, \mathbb{C})$, comme on le vérifie aisément.

Théorème 11 – les caractères des représentations irréductibles forment un système orthogonal

1. Si χ est le caractère d'une représentation irréductible, alors $(\chi|\chi) = 1$. Autrement dit, χ est de norme 1.
2. Si χ et χ' sont les caractères de deux représentations irréductibles non isomorphes, alors $(\chi|\chi') = 0$. Autrement dit, χ et χ' sont orthogonaux.

Le théorème implique que les caractères des représentations irréductibles forment un système orthogonal dans $\mathscr{F}(G, \mathbb{C})$. En particulier, ils forment une famille libre. Par conséquent,

l'ensemble des représentations irréductibles de G, à isomorphisme près, est fini. Son cardinal est majorée par g, le cardinal de G.

Exercice de cours 25 (démonstration du théorème 11). L'objectif de cet exercice est de démontrer le théorème. On commence par établir des relations matricielles qui découle du corollaire 9.

1. Dans les notations de ce corollaire, on note $\left(r^1_{i_1,j_1}(t)\right)_{1\leqslant i_1,j_1\leqslant n_1}$ et $\left(r^2_{i_2,j_2}(t)\right)_{1\leqslant i_2,j_2\leqslant n_2}$ les matrices de ρ^1 et ρ^2 dans des bases de V_1 et V_2 ; la première est d'ordre $n_1 = \dim V_1$, la deuxième d'ordre $n_2 = \dim V_2$.

   1.1 Dans le cas (1) du corollaire 9, montrer que l'on a

   $$\frac{1}{g}\sum_{t\in G} r^2_{i_2,j_2}(t^{-1})r^1_{i_1,j_1}(t) = 0, \qquad \forall\, i_1, i_2, j_1, j_2.$$

   1.2 Dans le cas (2) du corollaire 9, montrer que l'on a

   $$\frac{1}{g}\sum_{t\in G} r^2_{i_2,j_2}(t^{-1})r^1_{i_1,j_1}(t) = \frac{1}{n}\delta_{i_2,j_1}\delta_{j_2,i_1} = \begin{cases} \frac{1}{n} & \text{si } j_1 = i_2 \text{ et } i_1 = j_2, \\ 0 & \text{sinon.} \end{cases}$$

   où $\delta_{i,j}$ est le symbol de Kronecker.

2. On démontre dans cette question le théorème.

2.1 À l'aide de l'exercice 20 (ii), observer que si χ est le caractère d'une représentation, alors pour toute fonction $\phi\colon G \to \mathbb{C}$,

$$(1) \qquad (\phi|\chi) = \frac{1}{g}\sum_{t\in G}\phi(t)\chi(t^{-1}) = \frac{1}{g}\sum_{t\in G}\phi(t^{-1})\chi(t).$$

2.2 Déduire de la question 1.2 que l'on a $(\chi|\chi) = 1$ si χ est le caractère d'une représentation irréductible.

2.3 Déduire de la question 1.1 que l'on a $(\chi|\chi') = 0$ si χ et χ' sont les caractères de deux représentations irréductibles non isomorphes.

Théorème 12 – « unicité » de la décomposition en somme de représentations irréductibles

Soit V une représentation de G, de caractère ϕ. Supposons que V se décompose en une somme directe de représentations irréductibles

$$V = W_1 \oplus \cdots \oplus W_k.$$

Alors, si W est une représentation irréductible de G de caractère χ, le nombre de $i \in \{1, \dots, k\}$ tels que W soit isomorphe à W_i est égal au produit scalaire $(\phi|\chi)$.

En particulier, le nombre de W_i isomorphes à W ne dépend pas de la décomposition. Ce nombre est appelé la ***multiplicité de*** W ***dans*** V.

⚠ Comme nous l'avons déjà mentionné, la décomposition de V en une somme directe de représentations irréductibles n'est pas unique. L'unicité est seulement au sens précédent.

Exercice de cours 26. Démontrer le théorème à l'aide de l'exercice 21.

Clairement, si deux représentations sont isomorphes, elles ont le même caractère. De façon plus surprenante, la réciproque est vraie aussi.

Corollaire 13 – deux représentations ayant le même caractère sont isomorphes

Deux représentations de G ayant le même caractère sont isomorphes.

Exercice de cours 27. Démontrer le corollaire.

► *Le résultat précédent permet de réduire l'étude des représentations à celle des caractères des représentations irréductibles.*

Soient $\chi_1, \dots, \chi_h$ les caractères distincts des représentations irréductibles $W_1, \dots, W_h$ de G (les W_i sont donc deux à deux non isomorphes). Rappelons que G à un nombre fini de représentations irréductibles, à isomorphisme près.

Toute représentation V de G est donc isomorphe à une somme directe

$$V = m_1W_1 \oplus \cdots\cdots m_hW_h, \qquad m_i \in \mathbb{N}.$$

Le caractère ϕ de V est égale à $m_1\chi_1 + \cdots + m_h\chi_h$ d'après l'exercice 21 et, d'après le théorème 12,

$$m_i = (\phi|\chi_i).$$

De plus, les relations d'orthogonalité (voir le théorème 11) donnent :

$$(\phi|\phi) = \sum_{i=1}^{h} m_i^2.$$

Théorème 14 – une représentation est irréductible si et seulement si son caractère est de norme 1

Si ϕ est le caractère d'une représentation V, alors $(\phi|\phi)$ est un entier positif, et on a $(\phi|\phi) = 1$ si et seulement si V est irréductible.

Exercice de cours 28. Démontrer le théorème.

On obtient ainsi un critère très simple pour tester l'irréductibilité d'une représentation.

Exercice de cours 29 (multiplicité de la représentation triviale). Soit ρ une représentation de G de caractère χ. Quelle est la multiplicité de la représentation triviale en fonction de χ ?

Exercice de cours 30 (cas de la représentation par permutations). Soient X un ensemble fini dans lequel opère le groupe G, et ρ la représentation par permutations associée. On note χ son caractère. Pour $x \in X$, on note $G.x = \{s.x \colon s \in G\}$ son ***orbite*** et c le nombre d'orbites distinctes de X.

1. Montrer que c est égal à la multiplicité de la représentation triviale dans ρ. En déduire que $(\chi|1) = c$. Que peut-on dire de plus si l'action est ***transitive***, c'est-à-dire si $c = 1$?
2. Le groupe G opère dans $X \times X$ par $s.(x, y) = (s.x, s.y)$, où $s \in G$, $(x, y) \in X \times X$. Quel est, en fonction de χ, le caractère de la représentation par permutations associée à cette nouvelle action ?

Exercice de cours 31 (décomposition de la représentation régulière). Soit ρ_G la représentation régulière de G ; voir l'exemple 1 (2). Son degré est g, l'ordre du groupe G. On note χ_G son caractère.

1. Montrer que l'on a

$$\begin{cases} \chi_G(1) = g, \\ \chi_G(s) = 0 \text{ if } s \neq 1. \end{cases} \tag{2}$$

2. Montrer que toute représentation irréductible W de G apparaît dans la décomposition de la représentation régulière avec multiplicité $m = \dim W$. (*Indication : calculer* $(\chi_G|\chi)$*, où* χ *est le caractère de* W *et utiliser la relation* (1).)
3. On note $W_1, \dots, W_h$ les représentations irréductibles distinctes (à isomorphisme près) de G, de caractères $\chi_1, \dots, \chi_h$ et de degré $n_1, \dots, n_h$ respectivement. Montrer que

$$n_1^2 + \cdots + n_h^2 = g, \tag{3}$$

et que si $s \neq 1$,

$$\sum_{i=1}^{h} n_i \chi_i(s) = 0.$$

Remarque 3. L'exercice précédent peut être utilisé pour trouver toutes les représentations irréductibles d'un groupe G. Supposons que l'on ait construit des représentations irréductibles non isomorphes deux à deux de degrés $n_1, \dots, n_k$. On cherche à savoir si elles donnent toutes les représentations irréductibles de G. Il suffit pour cela de vérifier que

$$n_1^2 + \cdots + n_k^2 = g.$$

Exercice de cours 32 (obtention de toutes représentations irréductibles du groupe diédral). Montrer que les représentations irréductibles de degré 1 et 2 construites lors de l'exercice 16 donnent toutes les représentations de D_n (à isomorphisme près). Déterminer les caractères de ces représentations.

4.3. Fonctions centrales et nombres de représentations irréductibles. Rappelons qu'une ***fonction centrale*** est une fonction $f \colon G \to \mathbb{C}$ telle que f est constante sur les classes de conjugaison de G, c'est-à-dire que $f(tst^{-1}) = f(s)$ pour tous $s, t \in G$.

Exercice de cours 33 (encore une application du lemme de Schur). Soient $f\colon G \to \mathbb{C}$ une fonction centrale et $\rho\colon G \to \mathrm{GL}(V)$ une représentation de G. Soit ρ_f l'endomorphisme de V défini par :

$$\rho_f = \sum_{t\in G} f(t)\rho_t.$$

Montrer que si V est irréductible de degré n et de caractère χ, alors ρ_f est une homothétie de rapport

$$\lambda = \frac{1}{n}\sum_{t\in G} f(t)\chi_t = \frac{g}{n}(f|\overline{\chi}).$$

(*Indication : utiliser le lemme de Schur.*)

Soit $\mathbf{H}$ l'espace vectoriel des fonctions centrales. C'est un sous-espace de l'espace $\mathscr{F}(G,\mathbb{C})$ des fonctions de G dans $\mathbb{C}$. On note comme avant $\chi_1,\dots,\chi_h$ les caractères des représentations irréductibles de G.

Exercice de cours 34 (dimension de l'espace des fonctions centrales). Montrer que la dimension de l'espace $\mathbf{H}$ est égale au nombre de classes de conjugaison de G.

Théorème 15 – le nombre de représentations irréductibles est le nombre de classes de conjugaison

Les caractères $\chi_1,\dots,\chi_h$ forment une base orthonormale de $\mathbf{H}$.
En particulier, le nombre de représentations irréductibles de G est égale au nombre de classes de conjugaison de G.

Exercice de cours 35 (démonstration du théorème 15). Le but de cet exercice est de démontrer le théorème. Nous savons déjà que les caractères $\chi_1,\dots,\chi_h$ forment une famille libre de $\mathbf{H}$. Il reste donc à montrer que cette famille est génératrice. Soit $f \in \mathbf{H}$ tel que $(f|\overline{\chi_i}) = 0$.

1. Dans les notations de l'exercice 33, montrer que $\rho_f = 0$ pour toute représentation ρ de G
2. Avec $\rho = \rho_G$ la représentation régulière de G, en déduire que $f(t) = 0$ pour tout $t \in G$. Conclure.

5. Exemples et tables de caractères

Commençons par résumer les principaux résultats qui donnent une trame d'étude dans les exemples.

— Le nombre de représentations irréductibles est égale au nombre de classes de conjugaisons (théorème 15).
  ▶ *On commence donc par calculer le nombre de ces classes.*
— Le caractère d'une représentation irréductible détermine entièrement celle-ci (corollaire 13), et le caractère est une fonction centrale.
  ▶ *Dès qu'on a construit une représentation irréductible, on calcule son caractère sur un représentant de chaque classe de conjugaison.*
— Pour vérifier qu'on a obtenu toutes les représentations irréductibles, on vérifie que l'on a

$$g = n_1^2 + \cdots + n_k^2,$$

où $k \leqslant h$ est le nombre de représentations irréductibles qu'on a construit, et $n_1,\dots,n_k$ leur degré ; voir la formule (3).
— Pour vérifier qu'une représentation donnée de caractère χ est irréductible, on peut s'assurer que l'on a $(\chi|\chi) = 1$ (théorème 14). Le théorème 15 peut servir à vérifier que la table est correcte : on vérifie que les caractères sont de norme 1 et deux à deux orthogonaux.

⚠ Le plus dur est donc en général de construire des représentations irréductibles, mais il n'est pas toujours nécessaire de les construire explicitement pour connaître leur caractère comme nous le verrons sur des exemples (voir l'exemple 6 entre autres).

Il n'y a pas de recette pour cela, mais nous avons déjà vu quelques exemples.

5.1. Cas des groupes abéliens. Pour les groupes abéliens, voici un raffinement de l'exercice 19 qui donne une réponse complète.

Proposition 16 – une caractérisation des groupes abéliens

Le groupe fini G est abélien si et seulement si toutes ses représentations irréductibles sont de degré 1.

Exercice de cours 36. Démontrer la proposition à l'aide du théorème 15 et de la formule (3). *Cela donne une autre démonstration de la partie « seulement si » vue lors de l'exercice 19.*

Exercice de cours 37 (dual d'un groupe abélien). On suppose que G est un groupe abélien g. Soit $\widehat{G}$ l'ensemble des caractères de représentations irréductibles de G. D'après la proposition 16, $\widehat{G}$ est l'ensemble des morphismes de groupes $\chi\colon G \to \mathbb{C}^*$.

1. Montrer que $\widehat{G}$ est un groupe abélien d'ordre g, où la multiplication est donné par $\chi_1 \times \chi_2$ si $\chi_1, \chi_2 \in \widehat{G}$. Le groupe $\widehat{G}$ est appelé le ***dual*** du groupe G.
2. Pour tout $s \in G$, l'application $\widehat{G} \to \mathbb{C}^*$, $\chi \mapsto \chi(s)$ définit un élément du dual $\widehat{\widehat{G}}$ de $\widehat{G}$. On obtient ainsi une application $G \to \widehat{\widehat{G}}$. Montrer que cette application est un morphisme de groupes injectif.
3. Conclure que G et $\widehat{\widehat{G}}$ sont isomorphes.

5.2. Table des caractères. Les caractères irréductibles d'un groupe sont parfois donnés sous forme de table, appelée la ***table des caractères***. Comme ces caractères sont constants sur chaque classe de conjugaison, la table est donnée sur les classes de conjugaison ; c'est donc un tableau à h lignes et h colonnes (avec h le nombre de représentations irréductibles qui est le nombre de classes de conjugaison).

Exemple 5. La table des caractères du groupe cyclique Γ_3 est la suivante :

	1	r	r^2
χ_0	1	1	1
χ_1	1	w	w^2
χ_2	1	w^2	w

où $w = e^{2i\pi/3}$; voir l'exercice 9.

Exercice de cours 38. À l'aide de l'exercice 16, dresser la table des caractères du groupe diédral D_6. Plus généralement, lister toutes les représentations irréductibles de D_n, à isomorphisme près, en précisant le caractère.

Exemple 6 (table des caractères du groupe symétrique $\mathfrak{S}_3$). Le groupe symétrique $\mathfrak{S}_3$ a 3 classes de conjugaisons : 1, les trois transpositions et les deux 3-cycles. Soit $t = (1\,2)$ et $c = (1\,2\,3)$. On a

$$t^2 = 1, \qquad c^3 = 1, \qquad tc = c^2 t.$$

On en déduit qu'il y a seulement deux caractères de degré 1 (dont la représentation sous-jacente est de degré 1) : le caractère trivial χ_1 et la signature $\chi_2 = \varepsilon$. Le théorème 15 montre qu'il existe un autre caractère irréductible (associé à une représentation irréductible) ; on le note θ. Si n est le degré de θ, alors la formule (3) donne

$$1 + 1 + n^2 = 6,$$

d'où $n = 2$. Les valeurs de θ sur t et c peuvent se déduire de la relation

$$\chi_1 + \chi_2 + 2\theta = \chi_{\mathfrak{S}_3},$$

où $\chi_{\mathfrak{S}_3}$ est le caractère de la représentation régulière de $\mathfrak{S}_3$, et des relations (2).

On en déduit la table des caractères de $\mathfrak{S}_3$:

	1	t	c
χ_1	1	1	1
χ_2	1	-1	1
θ	2	0	-1

Vérifions la cohérence de cette table avec le théorème 14. La classe de 1 a un 1 élément, celle de t a trois éléments, $(12), (23), (13)$, et celle de c a deux éléments, $(123), (132)$. Or,

$$\begin{aligned}
(\chi_1|\chi_1) &= \frac{1}{6}(1^2 \times 1 + 1^2 \times 3 + 1^2 \times 2) = 1,\\
(\chi_2|\chi_2) &= \frac{1}{6}(1^2 \times 1 + (-1)^2 \times 3 + 1^2 \times 2) = 1,\\
(\theta|\theta) &= \frac{1}{6}(2^2 \times 1 + 0 \times 3 + (-1)^2 \times 2) = 1,\\
(\chi_1|\chi_2) &= \frac{1}{6}(1 \times 1 + (-1) \times 3 + 1 \times 2) = 0,\\
(\chi_2|\theta) &= \frac{1}{6}(2 \times 1 + 0 \times 3 + (-1) \times 2) = 0,\\
(\theta|\chi_1) &= \frac{1}{6}(2 \times 1 + 0 \times 3 + (-1) \times 2) = 0,
\end{aligned}$$

ce qui est cohérent !

Remarque 4. Nous avons construit une représentation irréductible de $\mathfrak{S}_3$ de degré 2 lors de l'exercice 15. Son caractère est donc θ, ce que l'on peut vérifier par ailleurs.

Exercice de cours 39 (table des caractères du groupe alterné $\mathfrak{A}_4$). On reprend les notations du paragraphe 1.3.

1. Montrer que $\mathfrak{A}_4$ possède trois représentations irréductibles de degré 1 et expliciter ces représentations.
2. En déduire la table des caractères de $\mathfrak{A}_4$. Donner une réalisation de la « quatrième » représentation irréductible de $\mathfrak{A}_4$, et vérifier la cohérence de la table avec le théorème 14.

Exercice de cours 40 (table des caractères du groupe symétrique $\mathfrak{S}_4$). On reprend les notations du paragraphe 1.4.

1. Déduire de la table des caractères de $\mathfrak{S}_3$ (voir l'exemple 6) que $\mathfrak{S}_4$ possède deux représentations de degré 1 et une représentation irréductible de degré 2.
2. Montrer que la représentation naturelle de $\mathfrak{S}_4$ dans $\mathbb{C}^3$ est irréductible.
3. En déduire la table de caractères de $\mathfrak{S}_4$.

On remarque que les caractères de $\mathfrak{S}_4$ sont à valeurs entières (ce n'est pas le cas des groupes Γ_3 ou $\mathfrak{A}_4$ par exemple). Ceci est un fait général pour le groupe symétrique $\mathfrak{S}_n$ qui dépasse le programme.

Exercice de cours 41 (table des caractères du groupe du cube). Dresser la table de caractères du groupe du cube $\mathrm{Iso}(\mathcal{C})$ (voir le paragraphe 1.5) à l'aide de celle de $\mathfrak{S}_4$.

6. Quelques remarques culturelles sur le groupe « Monstre »

La classification des groupes finis simples est connue ; il existe 18 familles infinies dénombrables de groupes finis simples, plus 26 groupes dits *sporadiques* qui ne suivent aucune règles apparentes. Le ***groupe Monstre*** ou ***groupe de Fischer-Griess*** est le plus grand de ces groupes sporadiques.

Son ordre est

$$\begin{aligned}
&246 \times 320 \times 59 \times 76 \times 112 \times 133 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71\\
&= 808017424794512875886459904961710757005754368000000000\\
&\approx 8 \times 10^{53}.
\end{aligned}$$

***Bernd Fischer**, né le 18 décembre 1936 à Bad Endbach dans le Land de Hesse, et mort le 13 août 2020, était un mathématicien allemand. Il est principalement connu pour son théorème de caractérisation des groupes de transpositions, qu'il démontra en 1970.*

***Robert Louis Griess**, né le 10 octobre 1945 à Savannah en Géorgie, est un mathématicien américain spécialiste des groupes finis, connu pour sa construction du groupe Monstre, le plus grand groupe sporadique.*

Le Monstre a 194 classes de conjugaisons. Sa table des caractères fut calculée en 1979, avant que l'existence ou l'unicité du Monstre fût prouvée. C'est Bernd Fischer et Robert Griess qui conjecturèrent son existence sur la base de sa table de caractères. Le calcul est fondé sur la supposition que le degré minimal d'une représentation fidèle complexe est 196 883. Le Monstre a ensuite été construit en 1982 par Robert Griess comme groupe de rotations d'un espace à 196 883 dimensions. John Conway a simplifié plus tard cette construction.

***John Horton Conway**, né le 26 décembre 1937 à Liverpool et mort le 11 avril 2020 à New Brunswick (New Jersey), est un mathématicien britannique. Il s'est intéressé aux théories des groupes finis, des nœuds, des nombres, des jeux et du codage. Le 11 avril 2020, il meurt de la Covid-19 à New Brunswick, N.J.*

Le groupe Monstre agit par automorphismes sur une certaine *algèbre vertex* (une structure algébrique de dimension infinie assez compliquée) dont la construction fut donnée par Igor Frenkel, James Lepowsky et Arne Meurman. Le groupe Monstre apparaît dans la conjecture *monstrous moonshine* qui relie des mathématiques discrètes et non discrètes, et qui fut prouvée par Richard Borcherds en 1992 grâce à la théorie des algèbres vertex.

***Richard Ewen Borcherds**, né le 29 novembre 1959 au Cap en Afrique du Sud, est un mathématicien anglais connu pour ses travaux en théorie des réseaux, des groupes et des algèbres de Lie. Borcherds est particulièrement connu pour son travail reliant la théorie des groupes finis à d'autres secteurs des mathématiques. En particulier, il inventa la notion d'algèbre vertex, qui est utilisée dans la preuve de la conjecture Conway-Norton à propos du* monstrous moonshine*. Ce résultat est lié à la théorie des représentations du groupe Monstre, un groupe fini dont la structure n'avait jusque-là pas été bien comprise.*

En 1998, au 23ème congrès international des mathématiciens à Berlin, il reçoit la médaille Fields.

2

Théorie des corps

Prérequis : notions d'anneaux et de corps.

Sauf dans l'énoncé du théorème de Wedderburn (théorème 55), les corps seront toujours supposés commutatifs. Nous suivons pour une large part le chapitre III de [1] et les chapitres 15 et 18 de [3].

1. Caractéristique d'un corps

Soient K un corps (quelconque pour le moment). Soit

$$\begin{array}{rccc} \sigma\colon & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n.1 = \underbrace{1+1+\cdots+1}_{n \text{ fois}}. \end{array}$$

C'est un morphisme d'anneaux dont le noyau est un idéal de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. On a donc une inclusion $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im}\sigma \hookrightarrow K$. Or un corps est un anneau intègre, donc $n\mathbb{Z}$ est un idéal premier. Autrement dit, ou bien $n = 0$ ou bien $n = p$ est un nombre premier. En effet, si tel n'était pas le cas, la factorisation précédente fournirait des diviseurs non nuls de 0 dans K.

Définition 17 – caractéristique d'un corps

Si $n = 0$, on dit que le corps K est de ***caractéristique nulle***.
Sinon, $n = p > 0$ est un nombre premier que l'on appelle la ***caractéristique du corps*** K.

Remarque 5.

1. Si le corps K est de caractéristique $p > 0$, on a alors par définition $p.1 = 0$, mais aussi, pour tout $x \in K$, $p.x = p.(1.x) = (p.1).x = 0$.

2. Si le corps K est de caractéristique nulle, alors $\sigma(\mathbb{Z}) \cong \mathbb{Z} \hookrightarrow K$, donc K est infini. De plus, K contient un corps isomorphe au corps des fractions de $\mathbb{Z}$, à savoir $\mathbb{Q}$.

On appelle ***sous-corps premier*** de K le plus petit sous-corps de K (contenant 1). C'est l'intersection de tous les sous-corps de K.

— Si K est fini de caractéristique $p > 0$, le plus petit sous-corps de K est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On le note aussi $\mathbf{F}_p$.
— Si K est de caractéristique nulle, alors le plus petit sous-corps de K est isomorphe à $\mathbb{Q}$.

⚠ Attention, il se peut qu'un corps soit de caractéristique $p > 0$ sans être de cardinal fini ! Penser, par exemple, au corps $\mathbf{F}_p(X)$.

2. Extension de corps, éléments algébriques

Définition 18 – extension de corps

Soient K, L des corps, avec $K \subset L$. Autrement dit, l'inclusion $i\colon K \hookrightarrow L$ est un morphisme d'anneaux. On dit que L est une ***extension (de corps)*** de K.

Remarque 6. Comme tout morphisme de corps est injectif, se donner une extension revient à se donner deux corps K, L et un morphisme de corps $i\colon K \hookrightarrow L$; on identifie alors $i(K)$ à un sous-corps de L.

Exercice de cours 42 (exemples d'extensions de corps). Citer des exemples variés d'extensions de corps.

Exercice de cours 43.

1. Vérifier que si L est une extension de K, alors L est un K-espace vectoriel.
2. On suppose que K et L sont des corps finis. Montrer que $|L| = |K|^n$, où $n = \dim_K L$.

Si K est de cardinal fini q, sa caractéristique est nécessairement égale à un nombre premier $p > 0$. D'après l'exercice précédent, on a donc $q = |K| = p^n$. Par exemple, il n'existe pas de corps de cardinal 6. On retient que

> le cardinal d'un corps fini est une puissance d'un nombre premier, sa caractéristique.

Si $K \subset L$ sont des corps tels que la dimension du K-espace vectoriel L soit finie, on pose

$$[L : K] = \dim_K L.$$

L'entier $[L : K]$ s'appelle la ***degré*** de l'extension L sur K.

Le théorème suivant est très simple, mais sera bien utile dans la théorie des corps comme nous le verrons plus loin, par exemple lors de la démonstration du théorème 24.

Théorème 19 – théorème de la base télescopique

Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$, une base de L sur K, et $(f_j)_{j\in J}$, une base de M sur L. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.
En particulier, si les degrés sont finis, on a

$$[M : K] = [M : L][L : K].$$

Remarque 7. Si $[M : K]$ est un nombre premier, il n'existe aucun corps L tel que $K \subset L \subset M$ et $K \neq L$, $L \neq M$.

Exercice de cours 44. Démontrer ce théorème.

Dans tout ce qui suit, $K \subset L$ désigne une extension de corps.

Définition 20 – partie génératrice

Soit A une partie de L. On dit que A ***engendre*** L sur K, et on écrit $L = K(A)$, si L est le plus petit sous-corps de L contenant K et A.
Si $A = \{x_1, \ldots, x_n\}$ est fini, on note $L = K(x_1, \ldots, x_n)$.
L'extension est dite ***monogène*** s'il existe $x \in A$ tel que $L = K(x)$.

Soit $x \in L$. On note $K[x]$ le sous-anneau engendré par K et x. On a

$$K[x] \subset K(x).$$

On peut décrire $K[x]$ et $K(x)$ ainsi :

— Si $y \in K[x]$, alors y s'écrit $y = P(x)$ avec $P \in K[X]$, i.e., $y = a_n x^n + \cdots + a_1 x + a_0$, avec $a_0, a_1, \ldots, a_n \in K$.

— Si $y \in K(x)$, alors $y = \dfrac{P(x)}{Q(x)}$ avec $P, Q \in K[X]$ et $Q(x) \neq 0$.

Autrement dit,

$$K[x] = \{P(x) \colon P \in K[X]\}, \qquad K(x) = \left\{ \frac{P(x)}{Q(x)} \colon P, Q \in K[X],\, Q(x) \neq 0 \right\},$$

Exercice de cours 45. Vérifier ces assertions.

⚠ Attention, $K[x]$ n'est pas en général isomorphe à l'anneau des polynômes $K[X]$, et $K(x)$ n'est pas en général isomorphe au corps des fractions rationnelles $K(X)$. En effet, on peut avoir $Q(x) = 0$ avec $Q \in K[X]$ et $Q \neq 0$.

De façon précise, l'application suivante

$$\varphi \colon K[X] \longrightarrow L, \quad P \longmapsto P(x)$$

définit un morphisme d'algèbres. On note I_x sont noyau.

Il y a deux cas possibles.

Définition 21 – élément algébrique et élément transcendant

1. Si $I_x = \{0\}$, on dit que x est ***transcendant sur*** K. Le morphisme φ induit alors un isomorphisme de $K[X]$ sur $K[x]$ qui se prolonge en un isomorphisme de $K(X)$ sur $K(x)$.
2. Si $I_x \neq \{0\}$, on dit que x est ***algébrique sur*** K.

   L'anneau $K[X]$ étant principal, il existe un un unique polynôme irréductible unitaire P_x tel que $I_x = (P_x)$.

   Le polynôme P_x est appelé le ***polynôme minimal de*** x ***sur*** K. Son degré est le ***degré de*** x ***sur*** K.

Exercice de cours 46. Vérifier que les nombres $\sqrt{2}$, i, $\sqrt[3]{2}$ de $\mathbb{C}$ sont algébriques sur $\mathbb{Q}$. Quels sont leurs polynômes minimaux ?

Remarque 8.
1. On peut montrer que les nombres réels $e = \exp(1)$ et π sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$ évidemment).
2. Dans $K(X)$, l'élément X est transcendant sur K.

Théorème 22 – différentes caractérisations des éléments algébriques

Soit $x \in L$. Les propriétés suivantes sont équivalentes :

1. x est algébrique sur K,
2. on a $K[x] = K(x)$,
3. on a $\dim_K K[x] < \infty$.

Lorsque ces propriétés sont satisfaites, que vaut $\dim_K K[x]$?

Exercice de cours 47. Démontrer le théorème.

Définition 23 – extension finie et extension algébrique

1. Une extension de corps $K \subset L$ est dite ***finie*** si $\dim_K L = [L : K] < \infty$.
2. Une extension de corps $K \subset L$ est dite ***algébrique*** si pour tout $x \in L$, x est algébrique sur K.

Exercice de cours 48. Déduire du théorème 22 que toute extension finie est algébrique.

⚠ Nous verrons plus loin que la réciproque est fausse : voir l'exemple 7 !

Théorème 24 – l'ensemble des éléments algébriques sur un corps est un sous-corps

Soit $K \subset L$ une extension de corps. Posons

$$M = \{x \in L : x \text{ est algébrique sur } K\}.$$

Alors M est un sous-corps de L qui contient K.

Exercice de cours 49. Démontrer ce théorème à l'aide du théorème 22 et du théorème de la base télescopique (théorème 19).

Exemple 7. Soit

$$\mathbf{A} = \{x \in \mathbb{C} : x \text{ algébrique sur } \mathbb{Q}\}.$$

Alors $\mathbf{A}$ est un sous-corps de $\mathbb{C}$, algébrique sur $\mathbb{Q}$, mais l'extension $\mathbb{Q} \subset \mathbf{A}$ n'est pas finie. En effet, il existe des éléments de $\mathbf{A}$ de degré arbitrairement grand, par exemple $\sqrt[n]{2}$, qui est de degré n, car le polynôme $X^n - 2$ est irréductible sur $\mathbb{Q}$ (en vertu du critère d'Eisenstein : voir le théorème 48 plus loin).

Définition 25 – corps algébriquement fermé dans un autre

Si $K \subset L$ est une extension, on dit que K est ***algébriquement fermé*** (ou ***algébriquement clos***) dans L si tout élément de L, algébrique sur K, appartient à K.

Autrement dit, dans les notations du théorème 24, $M = K$.

Exercice de cours 50. Dans les notations du théorème 24, montrer que M est une extension algébrique de K, algébriquement fermée dans L.

Définition 26 – clôture algébrique d'un corps dans une extension

On dit que M est la ***fermeture algébrique*** (ou la ***clôture algébrique***) de K dans L.

Exercice de cours 51. Vérifier que les propriétés suivantes sont équivalentes :

1. tout polynôme $P \in K[X]$ de degré $\geqslant 1$ admet une racine dans K,
2. tout polynôme $P \in K[X]$ de degré $\geqslant 1$ est produit de polynômes de $K[X]$ de degré 1,
3. les éléments irréductibles de $K[X]$ sont les $X - x$, avec $x \in K$,
4. si une extension $K \subset L$ est algébrique, alors on a $L = K$.

Définition 27 – corps algébriquement clos

Un corps K est dit ***algébriquement clos*** s'il vérifie l'une quelconque des propriétés équivalentes de l'exercice 51.
En particulier, K est algébriquement clos s'il est algébriquement clos dans toute extension de K.

EXEMPLE 8. **1.** Le corps $\mathbb{C}$ est algébriquement clos d'après le théorème de d'Alembert-Gauss.

***Jean le Rond D'Alembert**, né le 16 novembre 1717 à Paris où il est mort le 29 octobre 1783, est un mathématicien, physicien, philosophe et encyclopédiste français. Il est célèbre pour avoir dirigé l'Encyclopédie avec Denis Diderot jusqu'en 1757 et pour ses recherches en mathématiques sur les équations différentielles et les dérivées partielles.*

***Johann Carl Friedrich Gauss**, né le 30 avril 1777 à Brunswick et mort le 23 février 1855 à Göttingen, est un mathématicien, astronome et physicien allemand. Il a apporté de très importantes contributions à ces trois domaines. Surnommé «le prince des mathématiciens», il est considéré comme l'un des plus grands mathématiciens de tous les temps.*

2. le corps **A** défini dans l'exemple 7 est lui aussi algébriquement clos. On montre aisément que **A** est dénombrable (exercice !) ce qui, puisque $\mathbb{R}$ ne l'est pas, prouve l'existence dans $\mathbb{R}$ de nombres transcendants sur $\mathbb{Q}$.

3. Corps de rupture et corps de décomposition

Soit K un corps. Compte tenu des notions précédentes, voici deux problèmes bien naturels que nous allons résoudre dans cette section :

— étant donné un polynôme $P \in K[X]$, irréductible de degré $d > 1$, construire une extension dans laquelle P admet une racine a, donc est divisible par $X - a$ et, en particulier, n'est plus irréductible,

— étant donné un polynôme $P \in K[X]$, construire une extension dans laquelle P se décompose en produit de polynômes de degré 1.

3.1. Corps de rupture.

Définition 28 – corps de rupture d'un polynôme irréductible

Soient K un corps et $P \in K[X]$ un polynôme irréductible. Une extension L de K est appelée un ***corps de rupture de P sur K*** si L est une extension monogène $L = K(x)$ avec $P(x) = 0$.

Théorème 29 – existence et unicité du corps de rupture

Soit $P \in K[X]$ un polynôme irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Exercice de cours 52. Montrer que le corps $L = K[X]/(P)$ est un corps de rupture de P sur K.

L'exercice démontre la partie « existence » du théorème. L'unicité découle quant à elle du lemme suivant.

Lemme 30

Soient $K, \tilde{K}$ deux corps, $i\colon K \to \tilde{K}$ un isomorphisme que l'on étend de manière unique en un isomorphisme, encore noté i, de $K[X]$ sur $\tilde{K}[X]$ en envoyant X sur X. Soit $P \in K[X]$ un polynôme irréductible. Posons

$$\tilde{P} = i(P).$$

Soit $L = K(x)$ (resp. $\tilde{L} = \tilde{K}(\tilde{x})$) un corps de rupture de P sur K (resp. de $\tilde{P}$ sur $\tilde{K}$) engendré par une racine x de P (resp. une racine $\tilde{x}$ de $\tilde{P}$). Alors il existe un unique isomorphisme φ de L sur $\tilde{L}$ prolongeant i, et vérifiant $\varphi(x) = \tilde{x}$.

Exercice de cours 53 (démonstration du lemme 30). L'objectif de cet exercice est de démontrer le lemme ci-dessus.

1. Vérifier que les morphismes suivants,
$$u\colon K[X]/(P) \longrightarrow L, \qquad \tilde{u}\colon \tilde{K}[X]/(\tilde{P}) \longrightarrow \tilde{L},$$
définis par $u(\overline{X}) = x$ et $\tilde{u}(\overline{X}) = \tilde{x}$ où $\overline{X}$ désigne l'image de X dans le quotient, sont des isomorphismes.
2. En déduire que $\varphi = \tilde{u} \circ \bar{i} \circ u^{-1}$ est l'isomorphisme recherché, où
$$\bar{i}\colon K[X]/(P) \longrightarrow \tilde{K}[X]/(\tilde{P})$$
est l'isomorphisme induit par i.

Exercice de cours 54. Supposons que $K = \mathbb{Q}$ et $P = X^3 - 2$. Trouver un corps de rupture L contenu dans $\mathbb{R}$. Les racines de P sont-elles toutes dans L ?

3.2. Corps de décomposition. L'exercice précédent nous conduit à la définition suivante.

Définition 31 – corps de décomposition d'un polynôme

Soient K un corps et $P \in K[X]$ un polynôme (non nécessairement irréductible). On appelle ***corps de décomposition de P sur K*** toute extension L de K telle que :

1. dans $L[X]$, P est un produit de polynômes de degré 1, ou encore P a toutes ses racines dans L,
2. le corps L est minimal pour ces propriétés, ou encore L est engendré par les racines de P.

Théorème 32 – existence et unicité du corps de décomposition

Pour tout polynôme $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près.

Exercice de cours 55. Montrer par récurrence sur le degré de P l'existence d'un corps de décomposition de P sur K.

Comme précédemment, l'unicité découle d'un lemme un peu plus précis.

Lemme 33

Soient $K, \tilde{K}$ et $i\colon K \to \tilde{K}$ comme dans le lemme 30, $P \in K[X]$ un polynôme quelconque et $\tilde{P} = i(P)$. Soit L (resp. $\tilde{L}$) un corps de décomposition de P sur K (resp. de $\tilde{P}$ sur $\tilde{K}$). Alors il existe un isomorphisme φ de L sur $\tilde{L}$ prolongeant i.

Exercice de cours 56 (démonstration du lemme 33). Démontrer le lemme par récurrence sur $[L : K]$. (*Indication : considérer, si $K \neq L$, une racine $x \in L \setminus K$ de P et Q le polynôme minimal de x puis utiliser le lemme 30.*)

Exercice de cours 57. Quel est le corps de décomposition du polynôme $P = X^3 - 2$ de $\mathbb{Q}[X]$? Et du polynôme $P = X^4 - 2$ de $\mathbb{Q}[X]$?

3.3. Clôture algébrique.

Exercice de cours 58. Soient $K \subset L$ une extension, et M la fermeture algébrique de K dans L (voir la définition 26). Montrer que si L est algébriquement clos, M l'est aussi.

Théorème 34

Soient $K \subset L$ une extension algébrique, et $\sigma\colon K \to M$ un morphisme de corps où M est algébriquement clos.

1. Il existe un morphisme $\theta\colon L \to M$ prolongeant σ.
2. Si L est algébriquement clos et si l'extension $\sigma(K) \subset M$ est algébrique, tout morphisme de L dans M prolongeant σ est un isomorphisme.

Définition 35 – clôture algébrique d'un corps

Une extension $\overline{K}$ de K est appelée une ***clôture algébrique de*** K si $\overline{K}$ est algébriquement clos et si $\overline{K}$ est algébrique sur K.

Théorème 36 – Steinitz

Soit K un corps.

1. K possède une clôture algébrique.
2. Si L et L' sont des clôtures algébriques de K, il existe un isomorphisme ϕ de L sur L' tel que $\phi(x) = x$ pour tout $x \in K$.

La partie (2) du théorème 36 résulte du théorème 34. Les démonstrations du théorème 34 et de la partie (1) du théorème 36 sont assez délicates. Nous les présenterons si le temps le permet.

Par abus de langage, comme tenu du théorème 36 (2), on parle souvent de *la* clôture algébrique d'un corps.

***Ernst Steinitz**, (13 juin 1871 – 29 septembre 1928) est un mathématicien allemand. Steinitz est né à Laurahütte, province de Silésie, Royaume de Prusse. Il fit ses études à l'université de Breslau, où il passa sa thèse en 1894, et à l'université de Berlin. Il occupa ensuite des postes à Charlottenberg (devenu l'université technique de Berlin), à Breslau, et à l'université de Kiel, où il mourut en 1928. En 1910, Steinitz publie dans le journal de Crelle un article qui aura beaucoup d'impact :* Algebraische Theorie der Körper *(Théorie algébrique des corps). Dans cet article, il étudie la théorie axiomatique des corps commutatifs et définit des concepts importants comme ceux de corps premier, corps parfait et degré de transcendance d'une extension de corps. Il démontre que tout corps possède une clôture algébrique.*

EXEMPLE 9. **1.** Le corps $\mathbb{C}$ est algébriquement clos et de dimension 2 sur $\mathbb{R}$. C'est donc la clôture algébrique de $\mathbb{R}$.

2. Le corps $\mathbf{A}$ (voir l'exemple 7) est la clôture algébrique de $\mathbb{Q}$. Comme $\mathbf{A}$ est dénombrable, il n'est pas isomorphe à $\mathbb{C}$.

4. Théorie des corps finis

4.1. Morphisme de Frobenius. Soit K un corps de caractéristique $p > 0$.

EXERCICE DE COURS 59.

1. Montrer, à l'aide de la formule du binôme de Newton, que l'application $F\colon K \to K$ définie par

$$F(x) = x^p$$

est un morphisme de corps. (*On rappelle que p divise $\binom{p}{i}$ pour tout $i \in \{1, \dots, p-1\}$.*)

2. Montrer que si K est fini, alors F est un automorphisme.

3. Montrer que si $K = \mathbf{F}_p$, alors F est l'identité.

Définition 37 – morphisme de Frobenius

Le morphisme de corps F de l'exercice 59 précédent est appelé le ***morphisme de Frobenius***.

***Ferdinand Georg Frobenius**, connu aussi sous le nom de Georg Frobenius, est un mathématicien allemand, né le 26 octobre 1849 à Charlottenbourg (Prusse, aujourd'hui sous-municipalité de Berlin) et mort le 3 août 1917 à Berlin. Durant la deuxième moitié de sa carrière, la théorie des groupes a constitué l'un des principaux intérêts de Frobenius. L'une de ses premières contributions a été la redémonstration des théorèmes de Sylow pour un groupe abstrait (la preuve originelle de Sylow était formulée pour un groupe de permutations). La preuve du premier théorème de Sylow (sur l'existence des sous-groupes de Sylow) élaborée par Frobenius est encore celle la plus enseignée de nos jours.*

Ce morphisme joue un rôle très important dans l'étude des corps finis.

Théorème 38 – existence et unicité d'un corps fini de cardinal fixé

Soient p un nombre premier, et $n \in \mathbb{N}^*$. On pose $q = p^n$. Il existe un unique corps K, à isomorphisme près, de cardinal q ; c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$.
On le note $\mathbf{F}_q$.

Exercice de cours 60. L'objectif de cet exercice est de démontrer le théorème 38.

1. Dans cette question on s'intéresse à la partie « existence ». Soient K le corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$, et $k \subset K$ l'ensemble des racines de $X^q - X$.
   - **1.1** Montrer à l'aide du morphisme de Frobenius que k est un corps.
   - **1.2** Montrer que les racines de $P = X^q - X$ sont simples. En déduire que $|k| = q$, et conclure.
2. Soit K un corps à q éléments. En remarquant que tout élément de K est une racine du polynôme $X^q - X$, montrer que K est isomorphe au corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$.

4.2. Étude du groupe multiplicatif $\mathbf{F}_q^*$. On rappelle que la ***fonction d'Euler*** $\varphi\colon \mathbb{N}^* \to \mathbb{N}^*$ associe à tout nombre entier non nul n le nombre $\varphi(n)$ de nombres entiers x tels que $1 \leqslant x \leqslant n$ et x est premier à n. Autrement dit, $\varphi(n)$ est le cardinal du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, ou encore le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exercice de cours 61. Démontrer la relation pour tout $n \in \mathbb{N}^*$:

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

Théorème 39 – le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique

Le groupe multiplicatif $\mathbf{F}_q^*$ est cyclique, et donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Exercice de cours 62 (démonstration du théorème 39). Posons $\ell = q - 1$. Pour tout diviseur d de ℓ, on note $N(d)$ le nombre d'éléments de $\mathbf{F}_q^*$ d'ordre d.

1. Montrer : $\ell = \sum_{d|\ell} N(d)$.
2. Soient d un diviseur de ℓ et x un élément de $\mathbf{F}_q^*$ d'ordre d. En considérant le sous-groupe cyclique $H = \langle x \rangle$ engendré par x, montrer que $N(d)$ vaut 0 ou $\varphi(d)$.
3. Démontrer le théorème à l'aide de l'exercice 61.

Remarque 9.
1. On ne sait pas, en général, trouver explicitement des générateurs de $\mathbf{F}_q^*$, sauf des cas particuliers (voir l'exercice 63).
2. Le même raisonnement que dans l'exercice 62 permet de démontrer que tout sous-groupe fini d'un corps commutatif est cyclique.

Exercice de cours 63. Déterminer les générateurs de $\mathbf{F}_p^*$ pour $p = 2, 3, 5, 7, 11, 31, 43, 71$.
Indication : commencer par essayer les petits entiers $\pm 2, \pm 3, \ldots$ *et se rappeler que si* x *et* y *sont d'ordre premiers entre eux, alors*

$$\mathrm{ord}(xy) = \mathrm{ord}(x) \times \mathrm{ord}(y).$$

4.3. Les carrés de $\mathbf{F}_q$. Comme toujours, $q = p^n$ est une puissance d'un nombre premier $p > 0$. On pose

$$\mathbf{F}_q^2 = \{x^2 \colon x \in \mathbf{F}_q\}, \qquad (\mathbf{F}_q^*)^2 = \mathbf{F}_q^2 \cap \mathbf{F}_q^*.$$

Exercice de cours 64 (les carrés de $\mathbf{F}_q$).

1. On suppose $p = 2$. Montrer que $\mathbf{F}_q^2 = \mathbf{F}_q$.

2. On suppose $p > 2$. Quel est le cardinal du noyau du morphisme de groupes

$$\begin{array}{ccc} \mathbf{F}_q^* & \longrightarrow & (\mathbf{F}_q^*)^2 \quad ? \\ x & \longmapsto & x^2 \end{array}$$

En déduire que $\left|\mathbf{F}_q^2\right| = \dfrac{q+1}{2}$ et $\left|(\mathbf{F}_q^*)^2\right| = \dfrac{q-1}{2}$.

Proposition 40 – caractérisation des carrés

On suppose $p > 2$. Alors on a :

$$x \in (\mathbf{F}_q^*)^2 \iff x^{\frac{q-1}{2}} = 1.$$

Exercice de cours 65. Le but de l'exercice est de démontrer la proposition. Posons

$$X = \{x \in \mathbf{F}_q : x^{\frac{q-1}{2}} = 1\}.$$

Montrer que X est de cardinal $\dfrac{q-1}{2}$ et conclure à l'aide de l'exercice 64.

Exercice de cours 66. Supposons que $q = 7$. Le nombre 2 est-il un carré de $\mathbf{F}_q$? Et 3 ?

Corollaire 41

On suppose $p > 2$. Alors on a :

$$-1 \in (\mathbf{F}_q^*)^2 \iff q \equiv 1 \bmod 4.$$

Exercice de cours 67. Démontrer le corollaire :

— comme application directe de la proposition 40,

— comme application du théorème de Sylow.

Théorème 42 – un « petit » théorème de Dirichlet

Il existe une infinité de nombres premiers de la forme $4m + 1$.

***Johann Peter Gustav Lejeune Dirichlet**, (13 février 1805, Düren – 5 mai 1859, Göttingen) est un mathématicien prussien qui apporta de profondes contributions à la théorie des nombres, en créant le domaine de la théorie analytique des nombres et à la théorie des séries de Fourier. On lui doit d'autres avancées en analyse mathématique. On lui attribue la définition formelle moderne d'une fonction.*

Exercice de cours 68. Démontrer le théorème.
Indication : considérer un facteur premier de $(n!)^2 + 1$ et utiliser le corollaire 41.

5. Irréductibilité des polynômes de $K[X]$

Rappelons que si A est un anneau factoriel de corps de fractions $K = \mathrm{Frac}(A)$, alors la connaissance des irréductibles de $A[X]$ passe par celle de ceux de $K[X]$.

5.1. Quelques rappels d'arithmétique dans un anneau A, et propriétés de $A[X]$. Soit A un anneau commutatif unitaire. On rappelle qu'un élément p de A est dit ***irréductible*** si $p \notin A^\times$ et si

$$p = ab \quad \Longrightarrow \quad \left(a \in A^\times \text{ ou } b \in A^\times\right),$$

où

$$A^\times = \{a \in A : \exists\, b \in A,\, ab = 1\}$$

est l'ensemble des ***inversibles*** de A.

On choisit un système de représentants $\mathscr{P}$ des irréductibles de A, c'est-à-dire un ensemble d'irréductibles de A tel que pour tout irréductible q de A, il existe $p \in \mathscr{P}$ et $u \in A^\times$ inversible tels que $q = up$.

Définition 43 – anneau factoriel

L'anneau A est dit ***factoriel*** si

1. A est intègre,
2. tout $a \in A \setminus \{0\}$ s'écrit sous la forme $a = u \prod_{p \in \mathscr{P}} p^{v_p(a)}$, avec $u \in A^\times$, $v_p(a) \in \mathbb{N}$ et les $v_p(a)$ sont tous nuls sauf un nombre fini,
3. cette écriture est unique.

Rappelons aussi qu'un anneau A est dit ***principal*** s'il est intègre et si tout idéal de A est principal. Par exemple, $K[X]$ est principal si K est un corps (nous avons déjà utilisé ce résultat). La réciproque est vraie !

Proposition 44 – l'anneau de polynômes $A[X]$ est principal si seulement si A est corps

Soit A un anneau. Alors $A[X]$ est principal si seulement si A est corps.

En revanche, la factorialité se conserve.

Théorème 45 – Gauss

Si A est factoriel, alors $A[X]$ est factoriel.

La démonstration (que nous omettons ici) utilise d'une part le fait que $K[X]$, avec $K = \mathrm{Frac}(A)$, est principal donc factoriel, et d'autre part la notion de *contenu*.

On rappelle que si $P \in A[X]$, $P \neq 0$, s'écrit $P = a_n X^n + \cdots a_1 X + + a_0$, son ***contenu***,

$$c(P) = \mathrm{pgcd}(a_0, \ldots, a_n),$$

est le pgcd des coefficients de P. Il est défini modulo $A^\times$.

Définition 46 – polynôme primitif

Un polynôme $P \in A[X]$, $P \neq 0$, est dit ***primitif*** si $c(P) = 1$.

Le proposition suivante décrit les irréductibles de $A[X]$.

Proposition 47 – polynômes irréductibles de $A[X]$

On suppose que l'anneau A est factoriel. Les polynômes irréductibles de $A[X]$ sont :

1. les constantes $p \in A$, irréductibles dans A,
2. les polynômes de degré $\geqslant 1$, primitifs et irréductibles dans $K[X]$.

Compte tenu de la proposition précédente, il est donc important d'étudier les irréductibles de $K[X]$ lorsque K est un corps.

On suppose désormais que K est un corps (commutatif) quelconque.

Rappelons que si $P \in K[X]$ est irréductible de degré > 1, alors P n'a pas de racine dans K. En particulier, si K est algébriquement clos, les polynômes irréductibles de $K[X]$ sont exactement les $X - a$, avec $a \in K$.

⚠ La réciproque est fausse en général ! Par exemple, $(X^2+1)^2$ n'a pas de racines dans $\mathbb{R}$ mais est réductible. Elle est toutefois vraie si $\deg P \leqslant 3$.

Exercice de cours 69 (polynômes irréductibles de $\mathbb{R}[X]$). On suppose que $K = \mathbb{R}$. Montrer que les polynômes irréductibles de $\mathbb{R}[X]$ sont

— les polynômes $X - a$, avec $a \in \mathbb{R}$,

— les polynômes de degré 2 sans racine réelle.

5.2. Quelques critères d'irréductibilité.

Théorème 48 – critère d'Eisenstein

Soient A un anneau factoriel et $K = \mathrm{Frac}(A)$ son corps de fractions. Soient $P(X) = a_n X^n + \cdots + a_0$, avec $a_i \in A$, et $p \in A$ un élément irréductible de A. On suppose

1. p ne divise pas a_n,
2. pour tout $i \in \{0, \ldots, n-1\}$, p divise a_i,
3. p^2 ne divise pas a_0.

Alors P est irréductible dans $K[X]$. En particulier, si $c(P) = 1$ (par exemple si P est unitaire), alors P est irréductible dans $A[X]$.

⚠ Si $c(P) \neq 1$, le polynôme P peut-être réductible dans $A[X]$. C'est le cas par exemple si $A = \mathbb{Z}$, $p = 5$ et $P = 2X + 10$.

***Ferdinand Gotthold Max Eisenstein**, (16 avril 1823 – 11 octobre 1852) est un mathématicien prussien. Comme Galois et Abel, Eisenstein est mort avant l'âge de 30 ans, et comme Abel, sa mort est due à la tuberculose. Il est né et mort à Berlin, Allemagne. Il fit ses études à l'Université de Berlin où Dirichlet était son professeur. Gauss aurait déclaré : « Il n'y a que trois mathématiciens qui feront date : Archimède, Newton et Eisenstein. » Le choix par Gauss d'Eisenstein, lequel s'était spécialisé dans la théorie des nombres et l'analyse, peut sembler étrange à certains, mais il est justifié par le fait qu'Eisenstein avait prouvé facilement plusieurs résultats jusqu'alors inaccessibles, même à Gauss, comme d'étendre son théorème de réciprocité biquadratique au cas général.*

Exercice de cours 70 (démonstration du critère d'Eisenstein). Démontrer le théorème 48.
(*Indication : supposer que* $P = QR$ *est réductible, avec* $\deg Q < \deg P$ *et* $\deg R < \deg P$*, et projeter l'égalité dans* $B[X]$*, où* B *est l'anneau intègre* $A/(p)$ *et obtenir une contradiction dans* $L[X]$ *où* $L = \mathrm{Frac}(B)$.)

⚠ Attention, $B[X]$ n'est pas a priori factoriel car B ne l'est pas !

Exercice de cours 71 (quelques applications du critère d'Eisenstein).

1. Montrer que le polynôme $P(X) = 3X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$.
2. Montrer que le polynôme $P(X) = X^2 + X + 2$ est irréductible dans $\mathbb{Z}[X]$.
   (*Indication : effectuer un « changement de variable » de la forme* $Y = X + a$*, avec* a *bien choisi.*)
3. Montrer que le polynôme $X^4 + 1$ est irréductible dans sur $\mathbb{Z}[X]$.
4. Soit p un nombre premier. Montrer que le polynôme
   $$X^{p-1} + \cdots + X + 1$$
   est irréductible dans $\mathbb{Z}[X]$.
   (*Indication : on pourra poser* $X = Y + 1$.)
5. Soit $a \in \mathbb{Z}$, $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ tel que l'un des α_i soit égale à 1. Montrer que $X^n - a$ est irréductible dans $\mathbb{Z}[X]$.
6. Pour quelle(s) valeur(s) de λ le polynôme $Y^2 - X(X-1)(X-\lambda)$ est-il irréductible dans $\mathbb{Q}[X, Y]$?
7. Le polynôme $XY^4 + YZ^4 + ZX^4$ est-il irréductible dans $\mathbb{Q}[X, Y, Z]$?

Théorème 49 – réduction modulo un idéal

Soient A un anneau factoriel, $K = \mathrm{Frac}(A)$ et I un idéal premier de A. Soit
$$P(X) = a_n X^n + \cdots + a_1 X + a_0$$
un polynôme de $A[X]$ et
$$\overline{P} = \overline{a}_n X^n + \cdots + \overline{a}_1 X + \overline{a}_0$$
sa *réduction modulo* I, c'est-à-dire son image via la projection canonique $A[X] \to B[X]$, où $B = A/I$ est un anneau intègre. On suppose que $\overline{a}_n \neq 0$ dans B. Alors, si P est irréductible sur B ou $\mathrm{Frac}(B)$, le polynôme P est irréductible sur K.

⚠ Attention, P n'est pas nécessairement irréductible dans $A[X]$, comme le montre l'exemple du polynôme $2X \in \mathbb{Z}[X]$ avec $I = (3)$.

Exercice de cours 72. Démontrer le théorème.

Exercice de cours 73 (applications du critère de réduction).

1. Montrer que le polynôme $X^2 + Y^2 + 1$ est irréductible dans $\mathbb{R}[X, Y]$.
2. Montrer que le polynôme $X^3 + 6982X^2 + 455X - 7351$ est irréductible sur $\mathbb{Z}$.

Exercice de cours 74 (le polynôme $X^p - X - 1$, avec p premier, est irréductible sur $\mathbb{Z}$). Soit p un nombre premier.

1. Soient K un corps de décomposition de $P(X) = X^p - X - 1$ sur $\mathbf{F}_p$, et $\alpha \in K$ une racine de P. Montrer que pour tout $i \in \{0, \dots, p-1\}$, $\alpha + i$ est encore une racine de P dans K.
2. On suppose dans cette question que $P = QR$ est réductible dans $\mathbf{F}_p[X]$, avec $d = \deg Q < p$ et $\deg R < p$. En remarquant que, dans $K[X]$,
   $$Q(X) = \prod_{k=1}^{d} (X - \alpha - i_k),$$

avec $i_k \in \{0, \dots, p-1\}$, obtenir une contradiction.
(*Indication : considérer le terme en X^{d-1} de Q.*)

3. En déduire que le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

Dans cet exercice, nous avons eu recours à une extensions de corps.

Dans la même veine, nous allons voir maintenant quelques critères d'irréductibilité qui utilisent des extensions de corps, souvent commodes dans le cas des corps finis.

Théorème 50 – un critère d'irréductibilité à l'aide d'extensions de degré au plus $n/2$, où $n = \deg P$

Soit $P \in K[X]$ de degré $n > 0$. Alors P est irréductible sur K si et seulement si P n'a pas de racine dans les extensions L de K qui vérifient $[L : K] \leqslant n/2$.

Exercice de cours 75. Le but de l'exercice est de démontrer le théorème.

1. Supposons que P soit irréductible, et soit x une racine de P dans une extension L de K. Montrer que $[L : K] \geqslant n$.

2. Supposons que $P = QR$ ne soit pas irréductible sur K, avec $\deg Q < n$ et $\deg R < n$. En observant que $\deg Q \leqslant n/2$ ou $\deg R \leqslant n/2$, trouver une extension de K de degré $\leqslant n/2$ contenant une racine de P.

3. Conclure.

Exercice de cours 76.

1. Montrer que le polynôme $X^4 + X + 1$ est irréductible sur $\mathbf{F}_2$.

2. En déduire que le polynôme $X^4 + 8X^2 + 17X - 1$ est irréductible sur $\mathbb{Z}$.

Théorème 51 – un critère de conservation de l'irréductibilité par extension de corps

Soient $P \in K[X]$ un polynôme irréductible de degré n, et L une extension de degré m avec $(m, n) = 1$. Alors P est encore irréductible sur L.

Exercice de cours 77. Démontrer le théorème.

⚠ Attention, sans l'hypothèse $(m, n) = 1$, le théorème est faux ! Par exemple X^4+1 qui est irréductible sur $\mathbb{Q}$ (voir l'exercice 71) ne l'est plus sur $\mathbb{Q}(i)$ car $X^4 + 1 = (X^2 + i)(X^2 - i)$.

Exemple 10. Le polynôme $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$ et $\mathbb{Q}(i)$.

6. Polynômes cyclotomiques et applications

Soient K un corps et $n \in \mathbb{N}^*$. On pose

$$P_n(X) = X^n - 1 \in K[X].$$

Remarque 10. La dérivée de P_n est nX^{n-1}. En particulier,

— si la caractéristique p de K ne divise pas n, alors P_n n'a que des racines simples,

— si p divise n, alors $n = mp$ et $X^n - 1 = (X^m - 1)^p$ par Frobenius donc P_n a des racines multiples dans tout corps de décomposition.

Dans toute la suite, on suppose que n ne divise pas la caractéristique du corps K.

On note

$$\mu_n(K) = \{\zeta \in K : \zeta^n = 1\}$$

l'ensemble des ***racines n-ième de l'unité*** dans K. C'est un sous-groupe de K^*, de cardinal $\leqslant n$, donc cyclique ; voir la remarque 9 (2).

Soit $\mathbb{D}_n = \mathbb{D}_n(K)$ un corps de décomposition de P_n sur K. On a

$$|\mu_n(\mathbb{D}_n)| = n \quad \text{et} \quad \mu_n(\mathbb{D}_n) \cong \mathbb{Z}/n\mathbb{Z}.$$

De plus, comme $\mu_n(K)$ est inclus dans $\mu_n(\mathbb{D}_n)$ on a

$$\mu_n(K) \cong \mathbb{Z}/d\mathbb{Z}$$

où d est un diviseur de n.

Définition 52 – racine primitive n-ième de l'unité

Une racine n-ième ***primitive*** de l'unité est un élément ζ de $\mathbb{D}_n$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < 0$. Autrement dit, ζ est un générateur du groupe $\mu_n(\mathbb{D}_n)$ de sorte qu'il y a $\varphi(n)$ racines primitives n-ième de l'unité.

Leur ensemble sera noté $\mu_n^\times(\mathbb{D}_n)$.

Définition 53 – polynôme cyclotomique

Le ***n-ième polynôme cyclotomique*** $\Phi_{n,K} \in \mathbb{D}_n[X]$ est donné par :

$$\Phi_{n,K} = \prod_{\zeta \in \mu_n^\times(\mathbb{D}_n)} (X - \zeta).$$

Lorsqu'il n'y a pas d'ambiguïté sur K, on écrira simplement Φ_n pour $\Phi_{n,K}$.

Exercice de cours 78 (premières propriétés des polynômes cyclotomiques).

1. Quel est le degré de Φ_n ?

2. Démontrer la formule

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X). \tag{4}$$

Cette formule permet de calculer les Φ_n par récurrence pour les petites valeurs de n.

3. Calculer $\Phi_1, \Phi_2, \ldots, \Phi_8$.

Proposition 54 – les polynômes cyclotomiques sur $\mathbb{Q}$ sont à coefficients entiers

On a

$$\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X].$$

Exercice de cours 79.

1. Démontrer la proposition par récurrence sur n à l'aide de la formule (4).

2. On revient au cas où K est un corps quelconque. Soit $\sigma : \mathbb{Z} \to K$ le morphisme d'anneau canonique (voir le paragraphe 1). Montrer, toujours par récurrence sur n, que l'on a :

$$\Phi_{n,K}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X)).$$

En particulier, $\Phi_{n,\mathbf{F}_p}$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction modulo p.

Théorème 55 – application : théorème de Wedderburn

Tout corps fini est commutatif.

Joseph Henry Maclagen Wedderburn *(1882–1948) est un mathématicien écossais du XXème siècle. Membre de la Royal Society, il avait commencé à 16 ans ses études à l'université d'Édimbourg. Ses travaux portent sur les structures algébriques et tout particulièrement la théorie des corps, dans laquelle il met en évidence des exemples de corps non commutatifs.*

Exercice de cours 80 (démonstration du théorème de Wedderburn). On suppose que K est un corps fini, pas nécessairement commutatif. On pose

$$Z = \{a \in K : ax = xa \text{ pour tout } x \in K\},$$

le ***centre*** de K. On note q son cardinal.

1. Vérifier que $q \geqslant 2$, que Z est un sous-corps de K et que $|K| = q^n$ avec $n \in \mathbb{N}^*$.

2. On suppose dans cette question $n > 1$, c'est-à-dire que K n'est pas commutatif.

2.1 Posons

$$K_x = \{y \in K : yx = yx\}, \qquad K_x^* = K_x \cap K^*.$$

On note $\omega(x)$ l'orbite de $x \in K^*$ pour l'action de K^* sur lui-même par conjugaison. Montrer que l'on a :

$$|\omega(x)| = \frac{K^*}{K_x^*} = \frac{q^n - 1}{q^d - 1},$$

pour un certain diviseur d de n.

2.2 Montrer que $\Phi_n(q)$ divise $\dfrac{q^n - 1}{q^d - 1}$ pour $d \neq n$.

2.3 Écrire l'équation des classes, et en déduire que $|\Phi_n(q)| \leqslant q - 1$.

2.4 En remarquant que pour toute racine n-ième primitive ζ de l'unité,

$$|q - \zeta| > q - 1 \quad \text{(faire un dessin !)},$$

obtenir une contradiction.

3. Conclure.

Théorème 56 – irréductibilité des polynômes cyclotomiques sur $\mathbb{Z}$

Le polynôme cyclotomique $\Phi_n(X) \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Remarque 11. Nous avons déjà vu ce théorème dans des cas particuliers : le cas où $n = p$ est un nombre premier ou encore le cas $n = 4$ (voir l'exercice 71).

Exercice de cours 81 (démonstration du théorème 56). Soient K un corps de décomposition de Φ_n sur $\mathbb{Q}$, $\zeta \in K$ une racine primitive n-ième de l'unité, et p un nombre premier de divisant pas n.

1. Montrer que ζ^p est une autre racine primitive n-ième de l'unité.

2. Soient f et g les polynômes minimaux sur $\mathbb{Q}$ de ζ et ζ^p respectivement. Montrer que

$$f, g \in \mathbb{Z}[X]$$

et que f, g divisent tout deux Φ_n dans $\mathbb{Z}[X]$.

3. Le but de cette question est de montrer que $f = g$. On suppose que ce n'est pas le cas.

3.1 Montrer que fg divise Φ_n.

3.2 Montrer que, dans $\mathbb{Z}[X]$,

$$g(X^p) = f(X)h(X) \text{ avec } h \in \mathbb{Z}[X]. \tag{5}$$

3.3 En projetant l'égalité (5) dans $\mathbf{F}_p$, obtenir une contradiction.

4. Déduire de la question précédente que f admet toutes les racines primitive de l'unité comme racines. En déduire que $f = \Phi_n$.

5. Conclure.

Corollaire 57

Si ζ est une racine primitive n-ième de l'unité dans un corps de caractéristique nulle, son polynôme minimal sur $\mathbb{Q}$ est Φ_n et donc $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Exercice de cours 82. Démontrer le corollaire.

Exercice de cours 83 (intersection de deux extensions de $\mathbb{Q}$ par des racines primitive de l'unité « premières entre elles »).

1. Soit $K \subset L$ une extension de corps, et K_1, K_2 deux corps intermédiaires. On note K_1K_2 le sous-corps de L engendré par K_1 et K_2. Montrer :

$$[K_1K_2 : K_2] \leqslant [K_1 : K].$$

2. Montrer à l'aide de la question (1) que si α (resp. β) est une racine n-ième (resp. m-ième) primitive de l'unité dans $\mathbb{C}$ avec $(m, n) = 1$, alors

$$\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}.$$

3

Corps des fractions rationnelles à une indéterminée sur un corps

La référence principale pour ce chapitre est le chapitre 16 de [3].

Nous avons déjà rencontré le *corps de fractions* de plusieurs anneaux commutatifs intègres : $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$, $K(X) = \mathrm{Frac}(K[X])$, $K(x) = \mathrm{Frac}(K[x])$ où $x \in L$ est un élément d'une extension de K, etc.

On commence par rappeler la construction rigoureuse de ce corps dans un cadre un peu plus général.

1. Corps des fractions d'un anneau commutatif intègre

Soit A un anneau commutatif intègre (par exemple $\mathbb{Z}$, l'anneau $K[X]$ des polynômes à coefficients dans un corps K). Nous allons définir un corps à partir de A, contenant A, construit en « inversant » les éléments non nuls de A.

Sur l'ensemble $A \times (A \setminus \{0\})$, on définit une relation d'équivalence par :

$$(a, b) \sim (c, d) \iff ad = bc.$$

Exercice de cours 84. Vérifier que la relation $\sim$ est bien une relation d'équivalence.

On note $\frac{a}{b}$ la classe de $(a, b) \in A \times (A \setminus \{0\})$. Autrement dit, $\frac{a}{b} = \frac{c}{d}$ si et seulement si $ad = bc$. On note $\mathrm{Frac}(A)$ l'ensemble de ces classes d'équivalence, appelées ***fractions de*** A. On définit sur $\mathrm{Frac}(A)$ une addition et une multiplication par :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Exercice de cours 85. Vérifier que ces opérations sont bien définies.

Théorème 58 – l'ensemble des fractions de A est un corps

L'ensemble $\mathrm{Frac}(A)$, muni de l'addition et de la multiplication, est un corps, appelé le ***corps des fractions de*** A. L'application $A \to \mathrm{Frac}(A)$ qui envoie a sur $\frac{a}{1}$ est un morphisme injectif d'anneaux, qui permet d'identifier A à un sous-anneau de $\mathrm{Frac}(A)$.

Avec cette identification, tout élément non nul b de A a un inverse $b^{-1} = \frac{1}{b}$ dans $\mathrm{Frac}(A)$, et $\frac{a}{b} = a \times b^{-1}$.

Exemple 11.

1. Le corps des fractions de $\mathbb{Z}$ est bien sûr $\mathbb{Q}$.
2. Le corps des fractions rationnelles en X à coefficients dans le corps K est le corps de fractions de $K[X]$, que l'on note $K(X)$.

2. Corps des fractions rationnelles

Soit K un corps commutatif. On étudie dans cette section plus en détail le corps des fractions rationnelles $K(X)$.

On peut choisir un représentant privilégié pour une fraction rationnelle.

Définition 59 – forme réduite

Une fraction rationnelle est dite sous ***forme réduite*** quand elle est écrite sous la forme $\frac{A}{B}$ où A et B sont des polynômes premiers entre eux et B est unitaire. Une fraction rationnelle a une unique forme réduite.

Si $F = \frac{P}{Q}$, on trouve sa forme réduite en calculant un pgcd D de P et Q ; on a alors $Q = \lambda DB$ avec B polynôme unitaire et $\lambda \in K$ une constante non nulle. On définit A par $P = \lambda DA$. La forme réduite de F est alors $\frac{A}{B}$.

Selon l'usage, on dit que P est le ***numérateur*** et Q le ***dénominateur*** de la fraction F. Mais ceci est un abus de langage car le numérateur et le dénominateur sont associés à un représentant de la fraction, et non à la fraction elle-même.

On peut cependant parler du ***numérateur*** et du ***dénominateur*** de la forme réduite d'une fraction rationnelle grâce à l'unicité de celle-ci.

Exercice de cours 86 (forme réduite et degré d'une fraction rationnelle).

1. Mettre sous forme réduite les fractions rationnelles suivantes :
$$\frac{X^3+4X^2+X-6}{X^4-X^3-5X^2-X-6}, \qquad \frac{X^4+X^2+1}{X^3+3X^2+3X+2}.$$

2. Pour $F = \frac{A}{B} \in K(X)$, on pose
$$\deg(F) = \deg(A) - \deg(B).$$
Montrer que $\deg(F)$ est bien défini, c'est-à-dire ne dépend pas du représentant de la fraction rationnelle choisi, et que pour $F, G \in K(X)$,
$$\deg(F \times G) = \deg(F) + \deg(G) \quad \text{et} \quad \deg(F+G) \leqslant \max(\deg(F), \deg(G)).$$

3. Montrer que les fractions rationnelles de degré $\leqslant 0$ forment une sous-K-algèbre de $K(X)$.

Proposition 60 – le corps $K(X)$ n'est pas algébriquement clos

Le corps $K(X)$ n'est pas algébriquement clos.

Exercice de cours 87. Démontrer la proposition en observant que si tel était le cas, il existerait $F \in K(X)$ tel que $F^2 = X$.

3. Fonctions rationnelles

Définition 61 – pôles et zéros d'une fraction rationnelle

Soit $F \in K(X)$ une fraction rationnelle de forme réduite $F = \frac{A}{B}$.
Un ***pôle*** de F (dans K) est une racine de B (dans K). La ***multiplicité du pôle*** est sa multiplicité en tant que racine de B.
Un ***zéro*** de F (dans K) est une racine de A (dans K). La ***multiplicité du zéro*** est sa multiplicité en tant que racine de A.

Une fraction rationnelle a un nombre fini de pôles. Une fraction rationnelle non nulle a un nombre fini de zéros.

Si $F = \dfrac{A}{B}$ est une fraction rationnelle sous forme réduite, et x un élément de K qui n'est pas un pôle de F, alors on peut définir la valeur de F en x par

$$F(x) = \frac{A(x)}{B(x)} \in K.$$

EXERCICE DE COURS 88. Vérifier que $F(x)$ ne dépend pas du choix du représentant de F.

On obtient ainsi la ***fonction rationnelle*** $x \mapsto F(x)$ associée à la fraction rationnelle F. Cette fonction rationnelle est définie sur K privé de l'ensemble fini des pôles de F. On a $F(x) = 0$ si et seulement si x est un zéro de F.

3.1. Substitution. Si x n'est ni un pôle de $F \in K(X)$ ni de $G \in K(X)$, on a :

$$(F+G)(x) = F(x) + G(x) \quad \text{et} \quad (F \times G)(x) = F(x) \times G(x).$$

Théorème 62 – la fonction rationnelle détermine « presque » la fraction rationnelle

On suppose que le corps K est infini (par exemple, $K = \mathbb{R}$ ou $\mathbb{C}$). Soient F et G deux fractions rationnelles telles que pour tout $x \in K$ qui n'est ni pôle de F ni de G, on ait $F(x) = G(x)$. Alors

$$F = G.$$

On peut substituer une fraction rationnelle non constante à l'indéterminée dans une autre fraction rationnelle. Soit $G = \dfrac{A}{B}$ non constante sous forme réduite, et

$$F = \frac{a_0 + a_1 X + \cdots a_n X^n}{b_0 + b_1 X + \cdots b_q X^q},$$

alors on pose

$$\begin{aligned} F \circ G = F(G) &= (a_0 + a_1 G + \cdots a_n G^n) \times (b_0 + b_1 G + \cdots b_q G^q)^{-1} \\ &= B^{q-n} \frac{a_0 B^n + a_1 A B^{n-1} + \cdots a_n A^n}{b_0 B^q + b_1 A B^{q-1} + \cdots b_q A^q}. \end{aligned}$$

Cette substitution est bien licite car la fraction rationnelle $b_0 + b_1 G + \cdots b_q G^q$ n'est pas la fraction rationnelle nulle.

Proposition 63 – l'application de substitution est un morphisme d'algèbres

Soit G une fraction rationnelle non constante. L'application $F \to F(G)$ de $K(X)$ dans lui-même est un morphisme de K-algèbres.

EXERCICE DE COURS 89. Démontrer la proposition.

La substitution correspond à la composition des fonctions rationnelles, là où la composée est définie : si $x \in K$ n'est pas un pôle de G et $G(x)$ n'est pas un pôle de F, alors x n'est pas un pôle de $F(G)$ et $F(G)(x) = F(G(x))$.

EXERCICE DE COURS 90. Soit $x \in K$. L'ensemble des fractions rationnelles de $K(X)$ dont x n'est pas pôle est-il une sous-K-algèbre de $K(X)$? L'ensemble des fractions rationnelles de $K(X)$ dont x est un zéro est-il une sous-K-algèbre de $K(X)$?

EXERCICE DE COURS 91. Soit $x \in K$. Comparer les pôles et les zéros de $F(X + a)$ à ceux de F.

EXERCICE DE COURS 92. Soit $G = \dfrac{aX + b}{cX + d}$ avec $ad - bc \neq 0$. Montrer que $F \to F(G)$ est un morphisme bijectif de $K(X)$ sur lui-même, et trouver la bijection réciproque.

3.2. Dérivations. Rappelons que si $A = \sum_{n\leqslant 0} a_n X^n \in K[X]$, le ***polynôme dérivé*** de A est le polynôme

$$A' = \sum_{n\leqslant 0} (n+1)a_{n+1}X^n.$$

L'application $\Delta\colon A \mapsto A'$ est une ***dérivation*** de la K-algèbre $K[X]$, c'est-à-dire que pour tous $A, B \in K[X]$,

$$\Delta(AB) = \Delta(A)B + A\Delta(B).$$

De plus, pour tous $A, B \in K[X]$,

$$(A \circ B)' = (A' \circ B)B'.$$

Proposition 64 – dérivations sur le corps des fractions rationnelles

Il existe une unique dérivation $\tilde{\Delta}$ de $K(X)$ qui prolonge Δ. Pour tous $A, B \in K[X]$, on a

$$\tilde{\Delta}\left(\frac{A}{B}\right) = \frac{B\Delta(A) - A\Delta(B)}{B^2}.$$

Exercice de cours 93. Démontrer la proposition.

Soit $F \in K(X)$. Si $F' = 0$ alors l'ensemble $\mathrm{Pol}(F)$ des pôles de F est vide. Supposons $F' \neq 0$. Soient $F = \dfrac{A}{B}$ et $F' = \dfrac{C}{D}$ des formes réduites de F et F'. Par définition, D divise B^2, d'où

$$\mathrm{Pol}(F') \subset \mathrm{Pol}(F).$$

Lorsque le corps K est de caractéristique nulle, on peut préciser ces observations.

Proposition 65 – pôles de la fraction dérivée en caractéristique nulle

On suppose que K est de caractéristique nulle. Soit $F \in K(X)$.

1. On a $F' = 0$ si et seulement si $F \in K$.
2. On suppose que $F \notin K$. Soit $\alpha \in K$ un pôle de F d'ordre $n \geqslant 1$. Alors α est un pôle de F' d'ordre $n+1$.

Exercice de cours 94. Démontrer la proposition.

Exercice de cours 95 (la proposition 65 est fausse en caractéristique > 0). On suppose que la caractéristique de K est $p > 0$. On considérant les fractions rationnelles

$$F = \frac{1}{X^p} \quad \text{et} \quad G = \frac{1}{X^p(X+1)},$$

montrer que les assertions (1) et (2) de la proposition 65 sont mises en défaut en caractéristique > 0.

Proposition 66 – l'application dérivée pour les fractions rationnelles n'est pas surjective

Soit $\alpha \in K$. Il n'existe aucune fraction rationnelle F telle que

$$F' = \frac{1}{X - \alpha}.$$

En particulier, l'application $\tilde{\Delta}$ n'est donc pas surjective. Cette proposition est une observation clé dans la notion de *résidus*.

Exercice de cours 96.

1. On suppose que K est de caractéristique nulle. Démontrer la proposition à l'aide de la proposition 65.

2. On suppose que K est de caractéristique $p > 0$. En remarquant que si $A \in K[X]$ est tel que $A' = 0$ alors il existe $B \in K[X]$ tel que $A(X) = B(X^p)$, démontrer la proposition.

4. Décomposition en éléments simples

Voici tout d'abord l'énoncé général.

Théorème 67 – décomposition en éléments simples

Soit $F \in K(X)$ une fraction rationnelle. Alors F s'écrit de façon unique sous la forme

$$F = E + \sum_{i=1}^{n} \left(\sum_{j=1}^{\nu(i)} \frac{R_j^{(i)}}{P_i^j} \right),$$

où $E \in K[X]$, $P_1, \dots, P_n$ sont des polynômes unitaires irréductibles deux à deux distincts, $\nu(i) \in \mathbb{N}^*$ pour $i \in \{1, \dots, n\}$, $\deg R_i^{(j)} < \deg P_i$ pour tous i, j, et $R_{\nu(i)}^{(i)} \neq 0$ pour tout i.

On dit que E est la ***partie entière*** de F, que les $\dfrac{R_j^{(i)}}{P_i^j}$ en sont les ***éléments simples*** et que

$$\sum_{j=1}^{\nu(i)} \frac{R_j^{(i)}}{P_i^j}$$

est la ***partie P_i-fractionnaire*** de F. Lorsque P_i est de la forme $X - \alpha_i$, $\alpha_i \in K$, cette partie est aussi appelée la ***partie polaire*** de F relativement au pôle α_i.

Corollaire 68 – décomposition en éléments simples sur un corps algébriquement clos

On suppose que K est algébriquement clos, par exemple $K = \mathbb{C}$, alors tout $F \in K(X)$ s'écrit

$$F = E + \sum_{i=1}^{n} \left(\sum_{j=1}^{\nu(i)} \frac{\lambda_j^{(i)}}{(X - \alpha_i)^j} \right),$$

où $E \in K[X]$, $\alpha_1, \dots, \alpha_n \in K$ deux à deux distincts, $\nu(i) \in \mathbb{N}^*$, $\lambda_j^{(i)} \in K$ et $\lambda_{\nu(i)}^{(i)} \neq 0$ pour tous i, j.

Corollaire 69 – décomposition en éléments simples sur $\mathbb{R}$

Tout $F \in \mathbb{R}(X)$ s'écrit

$$F = E + \sum_{i=1}^{m} \left(\sum_{k=1}^{\mu(i)} \frac{\lambda_k^{(i)}}{(X - \alpha_i)^k} \right) + \sum_{j=1}^{n} \left(\sum_{l=1}^{\nu(i)} \frac{R_l^{(j)}}{(X^2 + a_j X + b_j)^l} \right),$$

où $E \in K[X]$, $\alpha_1, \dots, \alpha_m$ sont des réels deux à deux distincts, $\mu(i) \in \mathbb{N}^*$, $\nu(j) \in \mathbb{N}^*$, $\lambda_k^{(i)} \in \mathbb{R}$ avec $\lambda_{\mu(i)}^{(i)} \neq 0$, les $R_l^{(j)}$ sont des polynômes de degré au plus un, avec $R_{\nu(j)}^{(j)} \neq 0$, et les $X^2 + a_j X + b_j$ des éléments irréductibles de $\mathbb{R}[X]$, c'est-à-dire $a_j^2 - 4b_j < 0$ pour tout j, deux à deux distincts.

4.1. Démonstration du théorème 67. Dans ce paragraphe, nous allons démontrer le théorème 67. À tout polynôme $P \in K[X]$, on peut associer une relation d'équivalence $\mathscr{R}_P$ sur $K[X]$ en convenant que

$$A \mathscr{R}_P B \iff P \text{ divise } A - B.$$

Les classes d'équivalence pour cette relation seront appelées les ***classes modulo*** P.

On note $K_n[X]$ l'ensemble des polynômes de degré au plus n, pour $n \in \mathbb{N}$.

Lemme 70

Soit $P \in K[X]$ de degré $d > 0$. Alors $K_{d-1}[X]$ contient un et un seul représentant de toutes les classes modulo P.

Exercice de cours 97. Démontrer le lemme.

Lemme 71

Soient $n \in \mathbb{N}^*$ et $P \in K[X]$ un polynôme unitaire irréductible de degré d. Dans chaque classe de $K[X]$ modulo P^n, il existe un et seul polynôme de la forme

$$R_0 + R_1 P + \cdots + R_{n-1} P^{n-1},$$

avec $\deg(R_i) < d$ pour $i \in \{0, \ldots, n-1\}$.

Exercice de cours 98. Démontrer le lemme à l'aide du lemme 70.

Lemme 72

Soient $A \in K[X]$, $n \in \mathbb{N}^*$ et $P \in K[X]$ un polynôme unitaire irréductible premier avec A. Il existe une unique suite de polynômes $(R_0, R_1, \ldots, R_n) \in K[X] \times (K_{d-1}[X])^n$ tels que :

$$\frac{A}{P^n} = R_0 + \frac{R_1}{P} + \cdots + \frac{R_n}{P^n} \quad \text{et} \quad R_n \neq 0.$$

Exercice de cours 99. Démontrer le lemme à l'aide du lemme 71.

Lemme 73

Soit $F \in K(X)$. Il existe des polynômes irréductibles unitaires $P_1, \ldots, P_n$, $E \in K[X]$ et, pour chaque $i \in \{1, \ldots, n\}$, des entiers strictement positifs n_i et des polynômes A_i, non divisibles par P_i, tels que :

$$F = E + \sum_{i=1}^{n} \frac{A_i}{P_i^{n_i}}.$$

L'ensemble $\{P_1, \ldots, P_n\}$ (éventuellement vide) et les n_i sont uniquement déterminés par ces conditions.

⚠ Il n'y a l'unicité des polynômes A_i et du polynôme E à ce stade !

Exercice de cours 100. Le but de cet exercice est de démontrer le lemme 73.

1. On démontre dans cette question l'existence d'une telle décomposition.
   - **1.1** On suppose que $F \in K[X]$. Montrer que $E = F$ convient (sans P_i).
   - **1.2** On suppose que $F \notin K[X]$. On note $F = \dfrac{A}{B}$ sa forme réduite, avec B unitaire. En écrivant B sous la forme
     $$B = P_1^{n_1} \ldots P_s^{n_s},$$
     où les P_i sont des polynômes unitaires irréductibles deux à deux distincts, obtenir la décomposition souhaitée.
2. Démontrer l'unicité de l'ensemble $\{P_1, \ldots, P_n\}$ (éventuellement vide) et des n_i du lemme.

Les lemmes 72 et 73 démontrent l'existence de la décomposition en éléments simples dans le théorème 67.

Exercice de cours 101. Démontrer l'unicité de la décomposition en éléments simples dans le théorème 67 à l'aide du lemme 73 (et de sa démonstration : exercice 100).

4.2. Pratique de la décomposition en éléments simples sur $\mathbb{C}$. On conserve les notations du théorème 67, et on note $F = \dfrac{A}{B}$ une forme réduite de F avec B unitaire.

On remarque que si l'on soustrait à F sa partie polaire relative au pôle α_i, on obtient une fraction rationnelle qui n'a plus α_i pour pôle. Le nombre $\lambda^{(i)}_{\nu(i)}$ se détermine ainsi facilement.

Exercice de cours 102 (exemples de décompositions en éléments simple avec pôles simples ou doubles).

1. Trouver la décomposition en éléments simples de
$$F = \frac{5X^3 + 11X^2 - 2X - 2}{X^4 + 2X^3 - X^2 - 2X}.$$
2. Trouver la décomposition en éléments simples de
$$F = \frac{3X^2 - X + 1}{X^2(X+1)}.$$

Plus généralement, on peut calculer la partie polaire de F relative à un pôle α en amenant ce pôle en 0 par la substitution de $\alpha + Y$ à X et en utilisant la *division des polynômes suivant les puissances croissantes*.

Théorème 74 – division des polynômes suivant les puissances croissantes

Soient A et S deux polynômes de $K[X]$, avec $S(0) \neq 0$. Soit n un entier naturel. Alors il existe un unique couple (Q, R) de polynômes tel que
$$A = SQ + X^{n+1}R \quad \text{et} \quad \deg(Q) \leqslant n.$$
Le polynôme Q est le ***quotient de la division suivant les puissances croissantes de A par S à l'ordre n***. Le reste de cette division est $X^{n+1}R$.

Exercice de cours 103 (exemples de décompositions en éléments simple avec pôles $\geqslant 3$). Trouver la décomposition en éléments simples de
$$F = \frac{2X^5 + 10X^3 + 12X}{(X+1)^3(X-1)^3}.$$

4.3. Pratique de la décomposition en éléments simples sur $\mathbb{R}$. Pour effectuer la décomposition en éléments simples sur $\mathbb{R}$ d'une fraction rationnelle à coefficients réels, on peut effectuer la décomposition sur $\mathbb{C}$ puis regrouper les parties polaires correspondant aux pôles conjugués $\alpha_j + i\beta_j$ et $\alpha_j - i\beta_j$, ce qui est facile si ces pôles sont simples. On peut parfois utiliser d'autres méthodes.

Exercice de cours 104 (exemples de décompositions en éléments simple sur $\mathbb{R}$). Trouver la décomposition en éléments simples de
$$F = \frac{X(2X^4 + 3X^3 + 7X^2 + 4X + 4)}{(X^2+1)(X^2+X+1)^2}.$$

5. Applications

On termine ce chapitre par quelques applications de la décomposition en éléments simples.
Une première application est le calcul de et d'intégrales. Voici une illustration.

Exercice de cours 105 (un calcul d'intégrales). On se propose de calculer les intégrales
$$J_{m,n} = \int_0^{+\infty} \frac{u^{m-1}}{1+u^{2n}}\,du, \qquad I_p = \int_0^{+\infty} \frac{dt}{1+t^p},$$

où $m, n \in \mathbb{N}^*$ sont tels que $m < 2n+1$ et $p \geqslant 2$.

1. Montrer qu'il suffit de calculer les $J_{m,n}$.

2. Décomposer en éléments simples la fraction rationnelle

$$\frac{X^m}{X^{2n}+1}.$$

3. En déduire que

$$J_{m,n} = \frac{\pi}{2n \sin \dfrac{m\pi}{2n}}.$$

(*On pourra commencer par calculer* $\displaystyle\int_0^a \frac{u^{m-1}}{1+u^{2n}}\,du$, *pour* $a > 0$.).

4. Montrer que

$$I_p = \frac{\pi}{p \sin \dfrac{\pi}{p}}.$$

Voici une autre application. Si $P \in \mathbb{C}[X]$ est un polynôme non constant, on note $\delta(P)$ le nombre de racines distinctes de P.

Théorème 75 – théorème de Mason

Soient $P, Q, R \in \mathbb{C}[X]$, non constants, premiers entre eux deux à deux, et tels que :

$$P + Q = R.$$

Alors

$$\max(\deg P, \deg Q, \deg R) \leqslant \delta(PQR) - 1.$$

Bibliographie

[1] Daniel Perrin. Cours d'algèbre. Collection de l'École Normale Supérieure de Jeunes Filles, Paris, 1982.

[2] Jean-Pierre Serre. Représentations linéaires des groupes finis. Hermann, Paris, 1978.

[3] Patrice Tauvel. Cours d'algèbre, agrégation de mathématiques. Dunod, 1999.