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

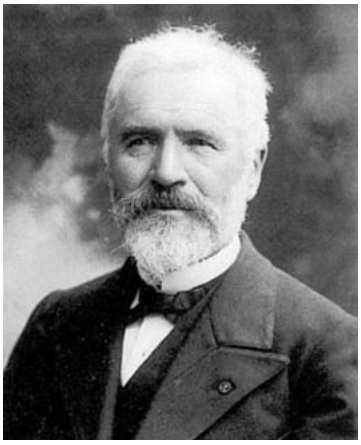
Année 2025–2026

M1 – MATHÉMATIQUES GÉNÉRALES III

Anne Moreau

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

***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.*



***Marie Ennemond Camille Jordan**, né le 5 janvier 1838 à Lyon, dans le quartier de la Croix-Rousse et mort le 21 janvier 1922 à Paris, est un mathématicien français, connu à la fois pour son travail fondamental dans la théorie des groupes et pour son influent Cours d'analyse.*

Table des matières

1 Théorie des corps

Prérequis : notions d'anneaux et de corps.
Sauf dans le théorème de Wedderburn (théorème 1.39), les corps sont supposés commutatifs.

Nous suivons pour une large part le chapitre III de [3] et les chapitres 15 et 18 de [6].

1.1. Caractéristique d'un corps

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

$$\sigma\colon \mathbb{Z} \longrightarrow K$$

l'unique morphisme d'anneaux défini par

$$n \longmapsto n.1 = \underbrace{1+1+\cdots+1}_{n \text{ fois}} \quad \text{si} \quad n > 0.$$

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 1.1 – 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 1.1.
(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 $\mathbf{F}_p(X)$.

1.2. Extension de corps, éléments algébriques

Définition 1.2 – 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 1.2. 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 1.1 (exemples d'extensions de corps). Citer des exemples variés d'extensions de corps.

EXERCICE DE COURS 1.2.

(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 le ***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 1.8.

Théorème 1.3 – 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 1.3. Si $[M : K]$ est un nombre premier, il n'existe aucun corps L tel que

$$K \subset L \subset M \quad \text{et} \quad K \neq L,\ L \neq M.$$

EXERCICE DE COURS 1.3. Démontrer ce théorème.

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

Définition 1.4 – 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,

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

EXERCICE DE COURS 1.4. 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 1.5 – 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 1.5. Vérifier que les nombres $\sqrt{2}$, i, $\sqrt[3]{2}$ de $\mathbb{C}$ sont algébriques sur $\mathbb{Q}$. Quels sont leurs polynômes minimaux ?

REMARQUE 1.4.
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.

EXERCICE DE COURS 1.6. Montrer que si x est transcendant sur K, alors $K[x] \cong K[X]$ (en tant qu'anneaux) et $K(x) \cong K(X)$ (en tant que corps). En particulier, $K[x]$ est distinct de $K(x)$.

Théorème 1.6 – différentes caractérisations des éléments algébriques

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

(i) x est algébrique sur K,

(ii) on a $K[x] = K(x)$,

(iii) on a $\dim_K K[x] < \infty$.

EXERCICE DE COURS 1.7 (démonstration du théorème 1.6).

(1) Démontrer l'implication (i) ⇒ (ii).

Indication : considérer l'isomorphisme

$$\overline{\varphi}\colon K[X]/(P) \to K[x],$$

où P est le polynôme minimal de x.

(2) Démontrer l'implication (ii) ⇒ (iii) à l'aide de l'exercice 1.6.

(3) Montrer que si $\dim_K K[x] < \infty$, alors le polynôme minimal P de x est irréductible et

$$\dim_K K[x] = [K[x] : K] = \deg P.$$

En déduire l'implication (iii) ⇒ (i).

Dans les notations de l'exercice précédent, le degré de P, égal à $\dim_K K[x]$, est appelé de ***degré*** de x sur K.

Définition 1.7 – 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 1.8. Déduire du théorème 1.6 que toute extension finie est algébrique.

Nous verrons plus loin que la réciproque est fausse : voir l'exemple 1.1 !

Théorème 1.8 – l'ensemble des éléments algébriques sur un corps est un sous-corps

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

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

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

EXERCICE DE COURS 1.9. Démontrer ce théorème à l'aide du théorème 1.6 et du théorème de la base téléscopique (théorème 1.3).

EXEMPLE 1.1. Soit

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

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 1.32 plus loin).

Définition 1.9 – 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 1.8, on a $M = K$.

EXERCICE DE COURS 1.10. Dans les notations du théorème 1.8, montrer que M est une extension algébrique de K, algébriquement fermée dans L.

Définition 1.10 – 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 1.11. 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 1.11 – corps algébriquement clos

Un corps K est dit ***algébriquement clos*** s'il vérifie l'une quelconque des propriétés équivalentes de l'exercice 1.11.

En particulier, K est algébriquement clos s'il est algébriquement clos dans toute extension de K.

EXEMPLE 1.2. 1) Le corps $\mathbb{C}$ est algébriquement clos d'après le théorème de d'Alembert-Gauss.

2) le corps $\mathbf{A}$ défini dans l'exemple 1.1 est lui aussi algébriquement clos. On montre aisément que $\mathbf{A}$ est dénombrable (exercice !) ce qui, puisque $\mathbb{R}$ ne l'est pas, prouve l'existence dans $\mathbb{R}$ de nombres transcendants sur $\mathbb{Q}$.

***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.*

1.3. 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.

1.3.1. Corps de rupture.

Définition 1.12 – 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 1.13 – 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 1.12. 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 1.14

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 1.13 (démonstration du lemme 1.14). 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 $\varphi = \tilde{u} \circ \overline{i} \circ u^{-1}$ est l'isomorphisme recherché, où

$$\overline{i}\colon K[X]/(P) \longrightarrow \tilde{K}[X]/(\tilde{P})$$

est l'isomorphisme induit par i.

EXERCICE DE COURS 1.14. 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 ?

1.3.2. Corps de décomposition.

L'exercice précédent nous conduit à la définition suivante.

Définition 1.15 – 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 1.16 – 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 1.15. 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 1.17

Soient $K, \tilde{K}$ et $i\colon K \to \tilde{K}$ comme dans le lemme 1.14, $P \in K[X]$ 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 1.16 (démonstration du lemme 1.17). 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 1.14.

EXERCICE DE COURS 1.17. Quel est le corps de décomposition du polynôme $P = X^3 - 2$ de $\mathbb{Q}[X]$? Et du polynôme $P = X^4 - 2$ de $\mathbb{Q}[X]$?

1.3.3. Clôture algébrique.

EXERCICE DE COURS 1.18. Soient $K \subset L$ une extension, et M la fermeture algébrique de K dans L (voir la définition 1.10). Montrer que si L est algébriquement clos, M l'est aussi.

Théorème 1.18

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 1.19 – 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 1.20 – Steinitz

Soit K un corps.

(i) K possède une clôture algébrique.

(ii) 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 (ii) du théorème 1.20 résulte du théorème 1.18. Les démonstrations du théorème 1.18 et de la partie (i) du théorème 1.20 sont assez délicates. Nous les présenterons si le temps le permet.

Par abus de langage, comme tenu du théorème 1.20 (ii), 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 1.3.
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 1.1) est la clôture algébrique de $\mathbb{Q}$. Comme $\mathbf{A}$ est dénombrable, il n'est pas isomorphe à $\mathbb{C}$.

REMARQUE 1.5. Tout corps algébriquement clos est infini.

1.4. Théorie des corps finis

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

EXERCICE DE COURS 1.19.

(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 1.21 – morphisme de Frobenius

Le morphisme de corps F de l'exercice 1.19 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 1.22 – 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 1.20. L'objectif de cet exercice est de démontrer le théorème 1.22.

(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 $X^q - X$.
   (a) Montrer à l'aide du morphisme de Frobenius que k est un corps.
   (b) 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 $\mathbf{F}_p$.

1.4.2. 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 1.21. Démontrer la relation pour tout $n \in \mathbb{N}^*$:

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

Théorème 1.23 – 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 1.22 (démonstration du théorème 1.23). 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 1.21.

REMARQUE 1.6. (1) On ne sait pas, en général, trouver explicitement des générateurs de $\mathbf{F}_q^*$, sauf des cas particuliers (voir l'exercice 1.23).

(2) Le même raisonnement que dans l'exercice 1.22 permet de démontrer que tout sous-groupe fini d'un corps commutatif est cyclique.

EXERCICE DE COURS 1.23. 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

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

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

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

EXERCICE DE COURS 1.24 (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 1.24 – 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 1.25. 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 1.24.

EXERCICE DE COURS 1.26. Supposons que $q = 7$. Le nombre 2 est-il un carré de $\mathbf{F}_q$? Et 3 ?

Corollaire 1.25

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

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

EXERCICE DE COURS 1.27. Démontrer le corollaire :

— comme application directe de la proposition 1.24,

— comme application du théorème de Sylow.

Théorème 1.26 – 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 1.28. Démontrer le théorème.

Indication : considérer un facteur premier de $(n!)^2+1$ et utiliser le corollaire 1.25.

1.5. 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 $K[X]$.

1.5.1. 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

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

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 1.27 – 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 $a=u\prod\limits_{p\in\mathscr{P}}p^{v_p(a)}$, 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 1.28 – 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 1.29 – 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 1.30 – 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 1.31 – 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 1.29 (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.

1.5.2. Quelques critères d'irréductibilité.

Théorème 1.32 – 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 1.30 (démonstration du critère d'Eisenstein). Démontrer le théorème 1.32.

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 1.31 (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 1.33 – 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 1.32. Démontrer le théorème.

EXERCICE DE COURS 1.33 (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 1.34 (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 1.34 – 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 1.35. 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 1.36.

(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 1.35 – 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 1.37. 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 1.31) ne l'est plus sur $\mathbb{Q}(i)$ car $X^4 + 1 = (X^2 + i)(X^2 - i)$.

EXEMPLE 1.4. Le polynôme $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$ et $\mathbb{Q}(i)$.

1.6. 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 1.7. 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 la caractéristique du corps K de divise par n.

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 1.6 (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 1.36 – 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 $d < n$. 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 1.37 – 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 1.38 (premières propriétés des polynômes cyclotomiques).

(1) Quel est le degré de Φ_n ?

(2) Démontrer la formule

$$X^n - 1 = \prod_{d \,|\, n} \Phi_d(X).$$

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

On a

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

EXERCICE DE COURS 1.39.

(1) Démontrer la proposition par récurrence sur n à l'aide de la formule de la question (2) de l'exercice 1.38.

(2) On revient au cas où K est un corps quelconque. Soit $\sigma\colon \mathbb{Z} \to K$ le morphisme d'anneau canonique (voir le paragraphe 1.1). 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 1.39 – 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 1.40 (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.

(a) 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.

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

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

(d) 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 1.40 – 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 1.8. Nous avons déjà vu ce théorème dans des cas particuliers : le cas où $n = p$ est un nombre premier ou encore le cas $n = 8$ (voir l'exercice 1.31).

EXERCICE DE COURS 1.41 (démonstration du théorème 1.40). 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.

(a) Montrer que fg divise Φ_n.

(b) Montrer que, dans $\mathbb{Z}[X]$,

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

(c) En projetant l'égalité de la question (b) 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 1.41

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 1.42. Démontrer le corollaire.

EXERCICE DE COURS 1.43 (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

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

2

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 et le suivant, nous allons nous intéresser aux sous-groupes finis du groupe linéaire $\mathbf{GL}(V)$ où V est un espace k-vectoriel de dimension finie et k est un corps commutatif. Nous allons voir que tout sous-groupe fini s'identifie naturellement à sous-groupe (fini) d'un groupe linéaire. Puis nous nous intéresserons au problème réciproque : quels sont les sous-groupes finis de $\mathbf{GL}(V)$? La question est difficile en général : on donnera des réponses assez précises dans des cas particuliers.

Dans ce chapitre, nous allons nous intéresser aux *représentations linéaires* des groupes finis, c'est-à-dire aux morphismes de groupes $G \to \mathbf{GL}(V)$, où V est un espace vectoriel (de dimension finie le plus souvent) défini sur un corps commutatif K et G est un groupe fini.

Sauf mention explicite du contraire, K est de caractéristique nulle.

Cette section suit pour une large part les premiers chapitres de [4].

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 qui se «plongent» naturellement dans un groupe linéaire.

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 $\mathfrak{A}_n$.

2.1.1. 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 $2k\pi/n$, $k = 0, \dots, n-1$; c'est le groupe des rotations du plan qui préservent un polygone régulier $\mathscr{P}_n$ à n côtés centré à l'origine O.

2.1.2. Le groupe diédral D_n. Il s'agit du groupe des isométries du plan affine qui préservent un polygone régulier $\mathscr{P}_n$ 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 2.1.

(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 2.2.

(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.

2.1.3. 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 2.3. 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
$$cxc^{-1} = z, \qquad czc^{-1} = y, \qquad cyc^{-1} = x.$$

EXERCICE DE COURS 2.4.

(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.

2.1.4. 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 2.5.

(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
$$\mathfrak{S}_4 \cong K \rtimes L.$$

2.1.5. Le groupe du cube. Considérons dans $\mathbb{R}^3$ le cube $\mathscr{C}$ dont les sommets ont pour coordonnées (x, y, z) avec $x = \pm 1$, $y = \pm 1$, $z = \pm 1$. Soit $\mathrm{Isom}(\mathscr{C})$ le groupe des isométries de $\mathbb{R}^3$ qui préservent $\mathscr{C}$, i.e., qui permutent ces 8 sommets.

Ce groupe peut être décrit de différentes façons.

a) En faisant opérer $\mathrm{Isom}(\mathscr{C})$ *sur l'ensemble des diagonales du cube.* Soit $\mathscr{D}$ l'ensemble des grandes diagonales du cube $\mathscr{C}$. 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 $(A_i B_i)$, $i = 1, 2, 3, 4$.

EXERCICE DE COURS 2.6.

(1) Déterminer le cardinal de $\mathrm{Isom}(\mathscr{C})$.

Indication : on pourra faire opérer $\mathrm{Isom}(\mathscr{C})$ sur l'ensemble des sommets de $\mathscr{C}$ et déterminer le cardinal du stabilisateur d'un sommet. Il y a d'autres façons de faire !

(2) Montrer que $\mathrm{Isom}(\mathscr{C})$ opère sur l'ensemble $\mathscr{D}$, et que le morphisme de groupes induit par cette opération,
$$\mathrm{Isom}(\mathscr{C}) \longrightarrow \mathfrak{S}(\mathscr{D}) \cong \mathfrak{S}_4,$$
est surjectif. Quel est son noyau ?

(3) Montrer que l'on a
$$\mathrm{Isom}(\mathscr{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}.$$
Combien y a-t-il de classes de conjugaison dans $\mathrm{Isom}(\mathscr{C})$?

(4) Montrer que le sous-groupe de $\mathrm{Isom}(\mathscr{C})$ formé par les rotations de $\mathbb{R}^3$ qui préservent le cube $\mathscr{C}$ est isomorphe à $\mathfrak{S}_4$.

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

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

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

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

EXERCICE DE COURS 2.7. En utilisant, par exemple, le cardinal de $\mathrm{Isom}(\mathscr{C})$, montrer que l'on a
$$\mathrm{Isom}(\mathscr{C}) = \mathrm{Isom}(\mathscr{T}) \times \{I, -I\}.$$

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

c) À l'aide du groupe $\mathfrak{S}_3$. Observons que le groupe $\mathrm{Isom}(\mathscr{C})$ 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 2.8.

(1) Vérifier que l'on a $\mathrm{Isom}(\mathscr{C}) = M \rtimes \mathfrak{S}_3$ (on retrouve ainsi que $\mathrm{Isom}(\mathscr{C})$ est d'ordre $8 \times 6 = 48$).

(2) Retrouver la décomposition $\mathrm{Isom}(\mathscr{C}) = M \rtimes \mathfrak{S}_3$ à partir de la décomposition $\mathrm{Isom}(\mathscr{C}) = \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et de la décomposition $\mathfrak{S}_4 = K \rtimes \mathfrak{S}_3$ (voir l'exercice 2.5).

(3) À l'aide du groupe d'isométries du cube, interpréter géométriquement les 2-groupes de Sylow de $\mathfrak{S}_4$. Combien y en a-t-il ?

Nous verrons à la fin de ce cours (section 3.5) d'autres exemples de groupes d'isométries de polyèdres réguliers.

2.1.6. Le groupe alterné $\mathfrak{A}_5$. Le groupe $\mathfrak{A}_5$ est le groupe des permutations paires de $\{1, 2, 3, 4, 5\}$. Il est isomorphe au groupe des rotations dans l'espace affine orienté $\mathbb{R}^3$ qui préservent un icosaèdre régulier (20 faces, 12 sommets, 30 arêtes) dont l'isobarycentre est l'origine O.

Il possède 60 éléments :

— l'identité,

— 15 double transpositions,

— 20 3-cycles,

— 24 5-cycles.

EXERCICE DE COURS 2.9. Soit $\mathrm{Isom}^+(\mathscr{I})$ le groupe des rotations de $\mathbb{R}^3$ qui préservent un icosaèdre régulier de $\mathbb{R}^3$ centré en l'origine.

(1) En faisant opérer $\mathrm{Isom}^+(\mathscr{I})$ sur l'ensemble de sommets $\{A_1, \ldots, A_{12}\}$, montrer que le cardinal de $\mathrm{Isom}^+(\mathscr{I})$ est 60.

(2) Show that $\mathrm{Isom}^+(\mathscr{I})$ is isomorphic to $\mathfrak{A}_5$.

Indication : remarquer que le groupe $\mathfrak{A}_5$ opère dans un ensemble à 5 éléments formé de groupes d'arrêtes (chacun de ces 5 groupes contient 6 éléments : chaque groupe contient des arêtes ou bien parallèles ou bien perpendiculaires).

On rappelle que pour q une puissance d'un nombre premier, le groupe spécial linéaire sur le corps $\mathbb{F}_q$ est défini par :

$$\mathbf{SL}_n(\mathbb{F}_q) = \{A \in \mathbf{GL}_n(\mathbb{F}_q) \colon \det(A) = 1\}.$$

Posons

$$\mathbf{PSL}_n(\mathbb{F}_q) = \mathbf{SL}_n(\mathbb{F}_q)/Z(\mathbf{SL}_n(\mathbb{F}_q)),$$

où $Z(\mathbf{SL}_n(\mathbb{F}_q))$ est le centre de $\mathbf{SL}_n(\mathbb{F}_q)$.

EXERCICE DE COURS 2.10.

(1) Décrire le centre $Z(\mathbf{SL}_n(\mathbb{F}_q))$.

(2) Quel est le cardinal de $\mathbf{GL}_n(\mathbb{F}_q)$? Et celui de $\mathbf{PSL}_n(\mathbb{F}_q)$? En déduire que le cardinal de $\mathbf{PSL}_2(\mathbb{F}_5)$ et de $\mathbf{PSL}_2(\mathbb{F}_4)$ est 60.

Théorème 2.1

On a les isomorphismes suivants :

$$\mathfrak{A}_5 \cong \mathbf{PSL_2}(\mathbb{F}_5) \cong \mathbf{PSL_2}(\mathbb{F}_4).$$

EXERCICE DE COURS 2.11. L'objectif de cet exercice est de démontrer le théorème 2.1.

(1) Montrer que $\mathbb{F}_5^2$ contient exactement 6 droites et décrire des générateurs de ces droites.

(2) Vérifier que le groupe $\mathbf{SL_2}(\mathbb{F}_5)$ opère sur l'ensemble $\mathscr{L}$ de ces droites et que le centre opère trivialement. En déduire un morphisme de groupes : $\mathbf{PSL_2}(\mathbb{F}_5) \hookrightarrow \mathfrak{S}_6$.

(3) Notons $\bar{A}$ et $\bar{B}$ les images dans $\mathbf{PSL_2}(\mathbb{F}_5)$ des matrices $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Montrer que $\bar{A}$ et $\bar{B}$ opèrent dans $\mathscr{L}$ comme (23456) et $(123)(456)$ respectivement. En déduire $\mathfrak{A}_5 \cong \mathbf{PSL_2}(\mathbb{F}_5)$.

(4) Rappelons que $\mathbb{F}_4$ est le corps $\{0, 1, x, y\}$ où $1 + x + x^2 = 0$ et $x^2 = y$. En procédant comme dans les questions précédentes avec cette fois l'ensemble des droites de $\mathbb{F}_4^2$ et les images dans $\mathbf{PSL_2}(\mathbb{F}_4)$ des matrices $\begin{pmatrix} x & y \\ x & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, montrer l'isomorphisme $\mathfrak{A}_5 \cong \mathbf{PSL_2}(\mathbb{F}_4)$.

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

Soient V un espace vectoriel défini sur le corps K, et $\mathbf{GL}(V)$ 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 2.2 – représentation linéaire d'un groupe fini

Une ***représentation linéaire*** (ou, simplement, ***représentation***) de G est un morphisme de groupes $\rho\colon G \to \mathbf{GL}(V)$ de G dans $\mathbf{GL}(V)$. Autrement dit, à tout élément s de G, on associe un élément $\rho(s)$ de $\mathbf{GL}(V)$ 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 2.1. (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 $\rho(s)$ est de module complexe 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 2.12 (représentations de degré 1 du groupe cyclique). Quelles sont les représentations de degré 1 groupe cyclique Γ_n (voir le paragraphe 2.1.1) ?

EXEMPLE 2.2. (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 $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$ et le groupe du cube $\mathrm{Isom}(\mathscr{C})$ 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 $\mathrm{Isom}(\mathscr{C})$.

Définition 2.3 – 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 2.13 (interprétation matricielle d'un isomorphisme de représentations). Soient $(e_1, \dots, e_n)$ une base de V, et $(e'_1, \dots, e'_n)$ 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 2.14.

(1) Soit (ρ^0, V) la représentation régulière de G. Vérifier que les images $\rho^0_s(e_1)$ forment une base de V lorsque s parcours G.

(2) Réciproquement, soit $\rho\colon G \to \mathbf{GL}(W)$ 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 2.3. 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 $\rho\colon G \to \mathbf{GL}(V)$ 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 $\rho^W_s : W \to W$ est alors un automorphisme de W et on a

$$\rho^W_{st} = \rho^W_s \circ \rho^W_t, \qquad \forall\, s, t \in G.$$

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

Définition 2.4 – 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 2.4. 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 2.5 – tout sous-espace stable admet un supplémentaire stable

Soient $\rho\colon G \to \mathbf{GL}(V)$ 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 2.15 (démonstration du théorème 2.5). 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
$$p^0 = \frac{1}{g}\sum_{t\in G} \rho_t \circ p \circ \rho_t^{-1}, \quad \text{où } g \text{ est l'ordre de } G.$$
(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 2.1 (une autre démonstration lorsque $K = \mathbb{R}$ ou $\mathbb{C}$). Supposons que $K = \mathbb{R}$ ou $\mathbb{C}$. Alors V est muni d'un produit scalaire hermitien $(x|y)$, i.e., $(-|-)$ est linéaire à gauche, semi-linéaire à droite et défini positif. 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 2.5.

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 2.5. 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 2.6 – 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 2.16. Interpréter matriciellement le théorème 2.5 et cette définition.

Définition 2.7 – représentation irréductible

Soit $\rho\colon G \to \mathbf{GL}(V)$ 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 2.5, une représentation est donc irréductible si et seulement si elle n'est pas somme directe de deux sous-représentations non triviales.

Théorème 2.8 – complète réductibilité des représentations

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

EXERCICE DE COURS 2.17. Démontrer ce théorème par récurrence et à l'aide du théorème 2.5.

REMARQUE 2.2. 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.

Toutefois, on peut montrer que le nombre de W_i isomorphes à une représentation irréductible donnée ne dépend pas de la décomposition choisie à l'aide de la théorie des *caractères* (voir le théorème 2.13).

EXERCICE DE COURS 2.18. 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 2.19 (représentations irréductibles de degré 1 et 2 du groupe diédral). On considère le groupe diédral D_n.

(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 2.2). 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^k 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 $h \in \mathbb{N}$:

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

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* $0 \leqslant h \leqslant n/2$.

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

(5) Interpréter géométriquement ce résultat à partir de la représentation naturelle de D_n dans $\mathbb{R}^2$, étendue à $\mathbb{C}^2$ (voir l'exemple 2.2).

Nous verrons plus loin que les représentations irréductibles obtenues dans cet exercice sont les seules représentations irréductibles du groupe diédral D_n (voir l'exercice 2.41).

2.3. Lemme de Schur

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

Proposition 2.9 – lemme de Schur

On suppose que le corps K est algébriquement clos. Soient $\rho^1 : G \to \mathbf{GL}(V_1)$ et $\rho^2 : G \to \mathbf{GL}(V_2)$ deux représentations irréductibles de G, et f une application linéaire de V_1 dans V_2 telle que $\rho^2_s \circ f = f \circ \rho^1_s$ pour tout $s \in G$.

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

(ii) 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 2.20 (démonstration du lemme de Schur).

(1) Comme le cas $f = 0$ est trivial, on suppose que $f \neq 0$. Montrer que le noyau et l'image de f sont stable par G ; en déduire la partie (i) du lemme de Schur.

(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 question (1), montrer que $f' = 0$ et conclure.

Corollaire 2.10 – 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

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

(i) Si ρ^1 et ρ^2 ne sont pas isomorphes, alors $h^0 = 0$,

(ii) 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 2.21. Démontrer le corollaire.

Voici pour terminer ce paragraphe une jolie application du lemme de Schur.

EXERCICE DE COURS 2.22 (les représentations irréductibles d'un groupe abélien sont de dégré 1). Soit G un groupe abélien fini. Montrer à l'aide du lemme de Schur que toute représentation irréductible complexe 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.*)

2.4. Théorie des caractères

2.4.1. 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 2.11 – 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 en un certain sens, comme nous le verrons plus loin (voir le corollaire 2.14).

EXERCICE DE COURS 2.23. 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 $f : G \to \mathbb{C}$ 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 2.23.

EXERCICE DE COURS 2.24. Soient $\rho^1 : G \to \mathrm{GL}(V_1)$ et $\rho^2 : G \to \mathrm{GL}(V_2)$ deux représentations de G, et χ_1, χ_2 les caractères associés. Que vaut le caractère de la représentation $\rho : G \to V = V_1 \oplus V_2$ définie par

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

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 2.25 (caractère de la représentation par permutations). Soit X un ensemble sur lequel agit le groupe G. On note $\rho : G \to \mathrm{GL}(V)$ la représentation par permutations associée à l'action de G (voir l'exemple 2.3), 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 2.26 (représentation contragrédiante). Soient $\rho : G \to \mathrm{GL}(V)$ 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 $\langle \lambda, x \rangle$ pour $\lambda(x)$ si $x \in V$ et $\lambda \in V^*$. Montrer qu'il existe une unique représentation $\rho^* : G \to \mathrm{GL}(V^*)$ telle que

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

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

2.4.2. 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 2.27. 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 $\phi : G \to \mathbb{C}$ et $\psi : G \to \mathbb{C}$ 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 2.12 – 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 majoré par g, le cardinal de G.

EXERCICE DE COURS 2.28 (démonstration du théorème 2.12). L'objectif de cet exercice est de démontrer le théorème. On commence par établir des relations matricielles qui découle du corollaire 2.10.

(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_t et ρ^2_t dans des bases de V_1 et V_2 respectivement, où $t\in G$; la première est d'ordre $n_1=\dim V_1$, la deuxième d'ordre $n_2=\dim V_2$.

(a) Dans le cas (i) du corollaire 2.10, montrer que l'on a

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

(b) Dans le cas (ii) du corollaire 2.10, montrer que l'on a

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

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

(2) On démontre dans cette question le théorème.

(a) À l'aide de l'exercice 2.23 (ii), observer que si χ est le caractère d'une représentation, alors pour toute fonction $\phi\colon G\to\mathbb{C}$,

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

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

(c) Déduire de la question (1)(a) que l'on a $(\chi|\chi')=0$ si χ et χ' sont les caractères de deux représentations irréductibles non isomorphes.

Théorème 2.13 – « 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 2.29. Démontrer le théorème à l'aide de l'exercice 2.24.

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

Corollaire 2.14 – deux représentations ayant le même caractère sont isomorphes

Deux représentations de G ayant le même caractère sont isomorphes.

EXERCICE DE COURS 2.30. 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

$$V = m_1 W_1 \oplus \cdots\cdots \oplus m_h W_h, \qquad m_i \in \mathbb{N}.$$

Le caractère ϕ de V est égale à $m_1\chi_1 + \cdots + m_h\chi_h$ d'après l'exercice 2.24 et, d'après le théorème 2.13,

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

De plus, les relations d'orthogonalité (voir le théorème 2.12) donnent :

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

Théorème 2.15 – 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 2.31. Démontrer le théorème.

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

EXERCICE DE COURS 2.32 (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 2.33 (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 $G.x = \{s.x : s \in G\}$ 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 2.34 (décomposition de la représentation régulière). Soit ρ^G la représentation régulière de G ; voir l'exemple 2.1 (2). Son degré est g, l'ordre du groupe G. On note χ^G son caractère.

(1) Montrer que l'on a

$$\begin{cases} \chi^G(1) = g, \\ \chi^G(s) = 0 \text{ if } s \neq 1. \end{cases}$$

(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 de la question (2)(a) de l'exercice 2.28.

(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

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

et que si $s \neq 1$,

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

REMARQUE 2.3. 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 2.35 (obtention de toutes représentations irréductibles du groupe diédral). Montrer que les représentations irréductibles de degré 1 et 2 construites lors de l'exercice 2.19 donnent toutes les représentations de D_n (à isomorphisme près). Déterminer les caractères de ces représentations.

2.4.3. 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 2.36 (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

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

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 2.37 (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 2.16 – 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 2.38 (démonstration du théorème 2.16). 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 $(f|\overline{\chi_i}) = 0$ pour tout $i \in \{1, \dots, h\}$.

(1) Dans les notations de l'exercice 2.36, 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.

2.5. 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 2.16).

► *On commence donc par calculer le nombre de ces classes.*

— Le caractère d'une représentation irréductible détermine entièrement celle-ci (corollaire 2.14), 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 $n_1, \ldots, n_k$ leur degré ; voir la question (3) de l'exercice 2.34.

— Pour vérifier qu'une représentation donnée de caractère χ est irréductible, on peut s'assurer que l'on a $(\chi|\chi) = 1$ (théorème 2.15). Le théorème 2.16 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 2.6 entre autres).

Il n'y a pas de recette pour cela, mais nous avons déjà vu quelques exemples.
Pour les groupes abéliens, voici un raffinement de l'exercice 2.22 qui donne une réponse complète.

Proposition 2.17 – 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 2.39. Démontrer la proposition à l'aide du théorème 2.16 et de la question (3) de l'exercice 2.34. *Cela donne une autre démonstration de la partie « seulement si » vue lors de l'exercice 2.22.*

EXERCICE DE COURS 2.40 (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 2.17, $\widehat{G}$ 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.

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 2.5. La table des caractères du groupe cyclique Γ_3 est la suivante, où $w = e^{2i\pi/3}$; voir l'exercice 2.12.

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

EXERCICE DE COURS 2.41. À l'aide de l'exercice 2.19, dresser la table des caractères du groupe diédral D_6.

EXEMPLE 2.6 (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 2.16 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 de la question (3) de l'exercice 2.34 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 de la question (1) de l'exercice 2.34.

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 2.15. 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 2.4. Nous avons construit une représentation irréductible de $\mathfrak{S}_3$ de degré 2 lors de l'exercice 2.18. Son caractère est donc θ, ce que l'on peut vérifier par ailleurs.

EXERCICE DE COURS 2.42 (table des caractères du groupe alterné $\mathfrak{A}_4$). On reprend les notations du paragraphe 2.1.3.

(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 2.15.

EXERCICE DE COURS 2.43 (table des caractères du groupe symétrique $\mathfrak{S}_4$). On reprend les notations du paragraphe 2.1.4.

(1) Déduire de la table des caractères de $\mathfrak{S}_3$ (voir l'exemple 2.6) 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 2.44 (table des caractères du groupe du cube). Dresser la table de caractères du groupe du cube $\mathrm{Iso}(\mathscr{C})$ (voir le paragraphe 2.1.5) à l'aide de celle de $\mathfrak{S}_4$.

2.6. 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 la table de caractère de ce groupe à la *fonction modulaire* [1] j, et qui fut prouvée par Richard Borcherds en 1992 grâce à la théorie des algèbres vertex.

1. i.e., une fonction holomorphe définie sur le demi-plan de Poincaré et invariante sour l'action du groupe modulaire $\mathbf{SL}_2(\mathbb{Z})$.

***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.

3

Structure des sous-groupes finis de $\mathrm{GL}(V)$

Nous avons vu en exercice que tout groupe fini peut, à l'aide de la représentation régulière, être réalisé comme groupe d'automorphismes d'un espace vectoriel. Dans ce chapitre, on aborde le problème inverse : étant donné un espace vectoriel V de dimension finie, quels sont les sous-groupes finis de $\mathbf{GL}(V)$?

On s'intéressera tout particulièrement au cas où V est un espace vectoriel de dimension finie sur $\mathbb{R}$ ou $\mathbb{C}$. Autrement dit, on va s'intéresser aux sous-groupes finis de $\mathbf{GL}_n(\mathbb{R})$ ou $\mathbf{GL}_n(\mathbb{C})$, où $n \in \mathbb{N}^*$.

EXERCICE DE COURS 3.1. Donner des exemples de sous-groupes finis de $\mathbf{GL}_n(\mathbb{R})$ et $\mathbf{GL}_n(\mathbb{C})$. Parmi eux, quels sont ceux qui sont abéliens ?

3.1. Sous-groupes abéliens finis

Nous avons vu quelques exemples de sous-groupes abéliens finis de $\mathbf{GL}_n(\mathbb{C})$. Nous allons maintenant étudier leur structure.

EXERCICE DE COURS 3.2. Soit G un sous-groupe abélien fini de $\mathbf{GL}_n(\mathbb{C})$ de cardinal $|G| = g$.

(1) À l'aide du théorème de Lagrange, montrer que les matrices d'un tel groupe sont diagonalisables.

(2) Montrer qu'il existe une base de $\mathbb{C}^n$ dans laquelle on peut diagonaliser simultanément les endomorphismes canoniquement associés aux matrices de G.

(3) En déduire que G est isomorphe à un sous-groupe de $(\mathbb{Z}/g\mathbb{Z})^n$.

La théorie des groupes abéliens (appelés également $\mathbb{Z}$-modules) de type fini, qui est une variante de celle des K-espaces vectoriels de dimension finie, permet de démontrer que tout sous-groupe de $(\mathbb{Z}/g\mathbb{Z})^n$ est le produit de $r \in \{1, \dots, n\}$ groupes cycliques. Ainsi, de l'exercice précédent, nous pouvons déduire qu'il existe $r \in \{1, \dots, n\}$ et des entiers $d_1, \dots, d_r \in \mathbb{N}^*$ tels que :

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_r\mathbb{Z}.$$

EXERCICE DE COURS 3.3. Réciproquement, montrer que tout produit de $r \in \{1, \dots, n\}$ groupes cycliques se plonge comme sous-groupe (abélien fini) de $\mathbf{GL}_n(\mathbb{C})$.

En combinant les deux exercices précédents, nous venons de démontrer la proposition suivante.

Proposition 3.1 – les sous-groupes abéliens finis de $\mathbf{GL}_n(\mathbb{C})$ sont des produits de groupes cycliques

Les sous-groupes abéliens finis de $\mathbf{GL}_n(\mathbb{C})$ sont isomorphes à des produits de r groupes cycliques $\mathbb{Z}/m\mathbb{Z}$ avec $r \in \{1, \dots, n\}$.

3.2. Sous-groupes finis de $\mathbf{GL}_n(\mathbb{R})$

Soient G un sous-groupe fini de $\mathbf{GL}_n(\mathbb{R})$ et $(-|-)$ un produit scalaire sur $\mathbb{R}^n$. La forme bilinéaire symétrique $(-|-)_G$ définie par

$$(x|y)_G = \sum_{g\in G}(gx|gy), \quad x, y \in \mathbb{R}^n,$$

est définie positive et invariante par G de sorte que G est contenu dans le groupe orthogonal euclidien $O(q_G)$ associé à la forme quadratique q_G donnée par $q_G(x) = (x|x)_G$ pour tout $x \in \mathbb{R}^n$.

EXERCICE DE COURS 3.4. Vérifier les assertions ci-dessus.

REMARQUE 3.1. Dans le cas complexe, on peut prendre un produit scalaire hermitien et on obtient alors que G est contenu dans un groupe unitaire.

L'avantage est que les groupes orthogonaux (ou unitaires) sont compacts, ce qui n'est pas le cas du groupe linéaire général. Si on ne s'intéresse qu'à la classe de conjugaison de G, a fortiori à son cardinal, on peut donc supposer que G est contenu dans $\mathbf{O}_n(\mathbb{R})$ (ou $\mathbf{U}_n(\mathbb{C})$ dans le cas complexe).

EXERCICE DE COURS 3.5 (le groupe des rotations en deux dimension est abélien). Décrire le groupe spécial orthogonal $\mathbf{SO}_2(\mathbb{R})$ et rappeler pourquoi c'est un groupe abélien.

3.2.1. Cas $n = 2$. L'intersection H de G et de $\mathbf{SO}_2(\mathbb{R})$ est au plus d'indice 2 (pourquoi ?). C'est un sous-groupe du groupe abélien $\mathbf{SO}_2(\mathbb{R})$. Si m est l'ordre de H, toutes les rotations de H ont donc un angle $2k\pi/m$, $k \in \mathbb{Z}$. On en déduit un isomorphisme $H \cong \mathbb{Z}/m\mathbb{Z}$ et H se réalise, par exemple, comme le groupe des rotations laissant stable un polygone régulier à m côtés (voir le paragraphe 2.1.1).

Si H est d'indice 2 et est engendré par un élément r d'ordre m, choisissons n'importe quel $s \in G \setminus H$. Comme s est une symétrie par rapport à une droite, $srs = r^{-1}$ et on en déduit que G est le groupe diédral D_m qui se réalise comme le groupe des isométries laissant stable un polygone régulier à m côtés (voir le paragraphe 2.1.2).

EXERCICE DE COURS 3.6. Vérifier les assertions ci-dessus. Conclure en décrivant tous les sous-groupes finis de $\mathbf{GL}_2(\mathbb{R})$.

3.2.2. Cas $n = 3$. Le cas $n = 3$ est plus subtil. Cherchons d'abord les cardinaux des sous-groupes finis de $\mathbf{SO}_3(\mathbb{R})$.

EXERCICE DE COURS 3.7. Rappeler la description géométrique des éléments de $\mathbf{SO}_3(\mathbb{R})$.

Soit G un sous-groupe fini de $\mathbf{SO}_3(\mathbb{R})$ de cardinal $g \geqslant 2$. On note X l'ensemble des points de la sphère unité $\mathbb{S}_2$ de $\mathbb{R}^3$ qui sont fixés par des éléments non triviaux de G, autrement dit X est l'ensemble des points d'intersection avec la sphère unité de l'axe des éléments non triviaux de G.

La stratégie est de classifier les groupes G possibles en faisant agir G sur X.

EXERCICE DE COURS 3.8. Montrer qu'il existe une action naturelle de G sur X et que $2 \leqslant |X| \leqslant 2(g-1)$.

On veut maintenant estimer le nombre d'orbites de cette action. Pour cela on rappelle la ***formule de Burnside***, valable pour toute action d'un groupe fini G sur un ensemble fini X : le nombre k d'orbites est donnée par la moyenne du nombre de points fixes des éléments de G :

$$k = \frac{1}{|G|}\sum_{s\in G}|\mathrm{Fix}(s)|,$$

où $\mathrm{Fix}(s) = \{x \in X : sx = x\}$.

Appliquons la formule de Burnside à l'action de notre sous-groupe fini $G \subset \mathbf{SO}_3(\mathbb{R})$ sur l'ensemble X. Comme toute rotation distincte de l'identité dans G fixe exactement deux points de X, et que l'identité fixe tous les éléments de X, la formule de Burnside donne l'estimation suivante pour le nombre k d'orbites de cette action :

$$k = \frac{1}{g}(2(g-1) + |X|) = 2 + \frac{|X|-2}{g} \geqslant 2.$$

On a aussi grâce à la majoration de l'exercice 3.8,

$$k \leqslant \frac{4(g-1)}{g} < 4.$$

En conclusion, $k \in \{2, 3\}$.

EXERCICE DE COURS 3.9. Montrer que si $k = 2$, alors G est cyclique.

EXERCICE DE COURS 3.10. On étudie dans cet exercice le cas $k = 3$. Notons ω_1, ω_2, ω_3 les trois orbites et n_1, n_2, n_3 les cardinaux des stabilisateurs correspondants. On peut supposer que $n_1 \leqslant n_2 \leqslant n_3$.

(1) À l'aide de la formule de Burnside et de la relation $|\omega_i| = \frac{g}{n_i}$, montrer que

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{g}.$$

(2) Montrer que $n_1 = 2$, puis que $n_2 \in \{2, 3\}$.

(3) Montrer que si $n_2 = 2$, alors $|G| = 2n_3 = |D_{n_3}|$.

(4) Sinon, montrer que l'on est dans l'un des situations suivantes :

- $(n_1, n_2, n_3) = (2, 3, 3)$ et $|G| = |\mathfrak{A}_4| = 12$,
- $(n_1, n_2, n_3) = (2, 3, 4)$ et $|G| = |\mathfrak{S}_4| = 24$,
- $(n_1, n_2, n_3) = (2, 3, 5)$ et $|G| = |\mathfrak{A}_5| = 60$.

Nous venons de déterminer les cas possibles. Remarquablement, tous les groupes apparaissant dans les exercices 3.9 et 3.10 peuvent être réalisés comme groupe d'isométries de certains polyèdres réguliers et donc comme sous-groupes finis de $\mathbf{SO}_3(\mathbb{R})$; nous en avons déjà vu certains.

Les cas obtenus sont décrits dans le tableau 1. La colonne « polyèdre » indique qu'on peut obtenir ces groupes comme des groupes d'isométries laissant stable une figure. Dans le cas I, on obtient les n rotations laissant stables un polygone régulier à n côtés. Dans les cas II (groupe diédral), on rajoute à ces rotations les symétries d'axe les droites joignant les milieux (ou sommets) du polygone, etc : voir la section 3.5 pour une description complète des autres polyèdres et leurs symétries.

	n_1	n_2	n_3	$\lvert G\rvert$	G	**polyèdre**
I	g	g		g	$\mathbb{Z}/g\mathbb{Z}$	$\mathscr{P}_g$
II	2	2	n	$2n$	D_n	$\mathscr{P}_g$
III	2	3	3	12	$\mathfrak{A}_4$	tétraèdre
IV	2	3	4	24	$\mathfrak{S}_4$	cube (octaèdre)
V	2	3	5	60	$\mathfrak{A}_5$	dodécaèdre (icosaèdre)

TABLE 1 – Valeurs possibles pour n_i

3.3. Sous-groupes finis de $\mathbf{GL}_n(\mathbb{Z})$

On trouve des groupes finis aussi grand qu'on veut dans $\mathbf{GL}_n(\mathbb{R})$ pour $n \geqslant 3$. Observons qu'ils sont « presque abéliens », au sens qu'ils contiennent un sous-groupe abélien normal d'indice petit, ici $\leqslant 60$. On verra plus bas (voir le théorème 3.4) que c'est toujours le cas. D'une certaine manière, si on veut plonger un groupe gros et compliqué dans un groupe $\mathbf{GL}_n$, il y a un prix à payer : n doit être grand !

Dans ce paragraphe, on étudie les sous-groupes finis de $\mathbf{GL}_n(\mathbb{Z})$ et nous allons voir qu'ils sont « petits ».

On pose

$$\mathbf{GL}_n(\mathbb{Z}) = \{A \in \mathbf{GL}_n(\mathbb{C}) \colon A \in \mathscr{M}_n(\mathbb{Z}) \text{ et } A^{-1} \in \mathscr{M}_n(\mathbb{Z})\}.$$

EXERCICE DE COURS 3.11 (le groupe $\mathbf{GL}_n(\mathbb{Z})$). Montrer que :

$$\mathbf{GL}_n(\mathbb{Z}) = \{A \in \mathscr{M}_n(\mathbb{Z}) \colon \det(A) \in \{-1, 1\}\}.$$

Justifier que $\mathbf{GL}_n(\mathbb{Z})$ est un sous-groupe de $(\mathbf{GL}_n(\mathbb{C}), \times)$.

Proposition 3.2 – Lemme de Serre

Soit p un entier premier plus grand que 3. Alors la restriction du morphisme

$$\mathbf{GL}_n(\mathbb{Z}) \longrightarrow \mathrm{GL}_n(\mathbf{F}_p)$$

à un sous-groupe fini G est injectif.

La démonstration de ce lemme est l'objet d'un problème de la fiche d'exercices.

***Jean-Pierre Serre**, né le 15 septembre 19262 à Bages (Pyrénées-Orientales), est un mathématicien français. Il reçoit de nombreuses récompenses pour ses recherches, et est en particulier lauréat de la médaille Fields en 1954, du prix Balzan en 1985, de la médaille d'or du CNRS en 1987, du prix Wolf de mathématiques en 2000, et le premier lauréat du prix Abel en 2003.*

Corollaire 3.3 – majoration du cardinal d'un sous-groupe fini de $\mathbf{GL}_n(\mathbb{Z})$

Le cardinal d'un sous-groupe fini de $\mathbf{GL}_n(\mathbb{Z})$ est majoré par

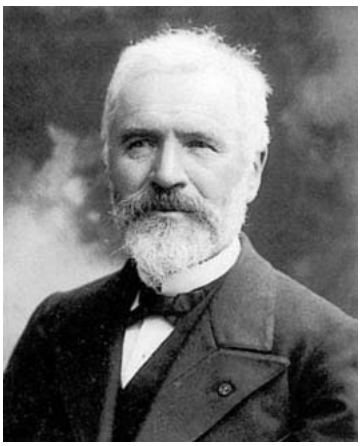
$$|\mathrm{GL}_n(\mathbf{F}_3)| = (3^n - 1)(3^n - 3^1)\cdots(3^n - 3^{n-1}).$$

EXERCICE DE COURS 3.12. Démontrer le corollaire à l'aide du lemme de Serre.

On déduit de cette étude que tout sous-groupe fini de $\mathbf{GL}_n(\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathbf{GL}_n(\mathbf{F}_3)$, ces derniers étant en nombre fini.

3.4. Un théorème de Jordan

Dans cette dernière section, on va démontrer un résultat dû à Jordan affirmant que, grosso modo, un sous-groupe fini de $\mathbf{GL}_n(\mathbb{C})$ n'est pas trop compliqué.



***Marie Ennemond Camille Jordan**, né le 5 janvier 1838 à Lyon, dans le quartier de la Croix-Rousse et mort le 21 janvier 1922 à Paris, est un mathématicien français, connu à la fois pour son travail fondamental dans la théorie des groupes et pour son influent Cours d'analyse.*

Théorème 3.4 – Jordan–Schur

Soit G un groupe fini de $\mathbf{GL}_n(\mathbb{C})$.
Alors G a un sous-groupe abélien normal d'indice $\leqslant (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}$.

Le reste de la section est dédié à la démonstration de ce théorème. Soit G un groupe fini de $\mathbf{GL}_n(\mathbb{C})$.

L'astuce de la moyenne permet de supposer $G \subset \mathbf{U}_n(\mathbb{C})$. On va voir que les matrices de G proches de I forment un sous-groupe abélien normal.

Commençons par prouver quelques lemmes élémentaires sur les matrices unitaires. On rappelle que deux matrices unitaires qui commutent sont simultanément unitairement semblables à des matrices diagonales de valeurs propres des racines de l'unité.

On munit $\mathscr{M}_n(\mathbb{C})$ de la norme L^2 définie par

$$\|A\| = \sqrt{\mathrm{Tr}(AA^*)},$$

qui est invariante par multiplication à gauche ou à droite par des matrices unitaires. C'est une norme multiplicative, et si A est unitaire, alors $\|A\| = \sqrt{n}$.

EXERCICE DE COURS 3.13. Vérifier ces assertions.

Lemme 3.5

Soient A, B deux matrices unitaires et supposons $\|I - B\| \leqslant 2$. Alors si A commute avec $(A, B) = ABA^{-1}B^{-1}$ alors A est B commutent.

EXERCICE DE COURS 3.14. Démontrer le lemme.

Indication : observer que A commute avec $A^{-1}(A, B) = BA^{-1}B^{-1}$ et BAB^{-1}, puis diagonaliser dans une même base.

Lemme 3.6 – si A est B sont voisines de l'identité, alors leur commutateur l'est encore plus

Soient A, B deux matrices unitaires. Alors

$$\|I - (A, B)\| \leqslant \sqrt{2}\|I - A\|\|I - B\|.$$

EXERCICE DE COURS 3.15. Démontrer le lemme.

Lemme 3.7 – si A est B sont suffisamment voisines de l'identité, alors elles commutent

Soient A, B deux matrices de G. Si $\|I - A\| < 1/\sqrt{2}$ et $\|I - B\| < 2$, alors A et B commutent.

EXERCICE DE COURS 3.16. L'objectif de cet exercice est de démontrer ce dernier lemme.

(1) On définit la suite de matrices B_i par

$$B_0 = B \quad \text{et} \quad B_{i+1} = (A, B_i).$$

Déduire du lemme 3.6 que $\lim_{i\to\infty} = I$. En déduire que $B_i = I$ pour i assez grand.

(2) Montrer par récurrence descendante que B_i et A commutent pour tout i. Conclure.

Notons alors H le sous groupe engendré par

$$\{A \in G \colon \|I - A\| < 1/\sqrt{2}\}.$$

Le lemme 3.7 assure que les éléments de H commutent deux à deux et donc que H est abélien. De plus, H est clairement normal (la norme unitaire est invariante par conjugaison unitaire). Reste à évaluer son indice. Soit $(R_i)_i$ un

système de représentant de G/H. Ils sont, comme on l'a vu, sur la sphère de rayon $\sqrt{n}$ de $\mathscr{M}_n(\mathbb{C}) \cong \mathbb{R}^{2n^2}$. D'autre part, si $i \neq j$, on a

$$\|R_i - Rj\| \geqslant 1/\sqrt{2}$$

car sinon $R_i^{-1}R_j \in H$. Notons $\mathscr{B}_i$ la boule de centre R_i et de rayon $1/(2\sqrt{2})$. On a $\mathscr{B}_i \cap \mathscr{B}_j = \varnothing$. Autrement dit, on a une réunion disjointe des $\mathscr{B}_i$ toutes contenues dans la couronne

$$\mathscr{C}(\sqrt{n} - 1/(2\sqrt{2}), \sqrt{n} + 1/(2\sqrt{2})).$$

Si v est le volume de la boule unité, on a donc

$$\sum_i v(\mathscr{B}_i) = [G : H](1/2\sqrt{2})^{2n^2} v \leqslant (\sqrt{n} + 1/(2\sqrt{2}))^{2n^2} v - (\sqrt{n} - 1/(2\sqrt{2}))^{2n^2} v. \tag{1}$$

EXERCICE DE COURS 3.17. Démontrer le théorème de Jordan–Schur à l'aide de l'inégalité (1).

Par exemple, ceci donne une borne pour les cardinaux des groupes finis simples contenus dans $\mathbf{GL}_n(\mathbb{C})$. Notons que ce théorème reste valable remplaçant $\mathbb{C}$ par un corps de caractéristique positive p pourvu qu'on se limite à des groupes d'ordre premier à p. La démonstration est tout autre, et nettement plus technique !

3.5. Digression sur les cinq solides platoniciens

Un polyèdre $\mathscr{P}$ est l'enveloppe convexe d'un nombre fini (non coplanaires) de points dans $\mathbb{R}^3$. En particulier, un tel polyèdre $\mathscr{P}$ est compact et d'intérieur non vide. On devrait dire *polyèdre convexe*, mais comme on ne considèrera que le cas convexe, on omet ici l'adjectif.

Dans ce cours on considèrera comme « intuitivement évidentes » les notions de sommets, arêtes et faces, et notamment le fait que les faces sont toujours des polygones (avec au moins 3 arêtes), et que chaque sommet appartient à au moins 3 arêtes et au moins 3 faces. La question de les définir rigoureusement se pose notamment lorsqu'on veut étendre ces notions en dimension arbitraire (à partir de la dimension 4 peu de choses sont « intuitivement évidentes » mais on va rester en dimension 3...).

Pour la proposition suivante on notera S, A, F les nombres de sommets, arêtes et faces d'un polyèdre $\mathscr{P}$ donné.

Proposition 3.8 – relation d'Euler

Pour tout polyèdre $\mathscr{P}$, on a la relation

$$S - A + F = 2.$$

Leonhard Euler, né le 15 avril 1707 à Bâle (Suisse) et mort le 7 septembre 1783 (18 septembre dans le calendrier grégorien) à Saint-Pétersbourg (Empire russe), est un mathématicien et physicien suisse, qui passa la plus grande partie de sa vie dans l'Empire russe et en Allemagne.

Euler est considéré comme un éminent mathématicien du XVIII$^{\text{e}}$ siècle et l'un des plus grands et des plus prolifiques de tous les temps. Une déclaration attribuée à Pierre-Simon de Laplace exprime l'influence d'Euler sur les mathématiques : « Lisez Euler, lisez Euler, c'est notre maître à tous ». Il était un fervent chrétien, croyant en l'inerrance biblique, et s'opposa avec force aux athées éminents de son temps.

EXERCICE DE COURS 3.18. Démontrer la proposition, en essayant d'imaginer que le polyèdre est plongé dans une piscine et qu'on le fait sortir petit à petit de l'eau, de telle façon que les sommets sortent de l'eau un par un...

Il existe une démonstration plus topologique, par récurrence sur le nombre d'arêtes ; voir par exemple [1, page 146].

Définition 3.9 – solide de Platon (polyèdre régulier)

Un polyèdre convexe est un ***solide de Platon*** (ou ***polyèdre régulier***) si :

(1) toutes ses faces sont des polygones réguliers convexes isométriques, c'est-à-dire superposables,

(2) aucune de ses faces ne se coupe, excepté sur les arêtes,

(3) le même nombre de faces se rencontre à chacun de ses sommets.

Solides de Platon. Depuis les mathématiques grecques, les solides de Platon furent un sujet d'étude des géomètres en raison de leur esthétique et de leurs symétries. Leur nom, donné en l'honneur du philosophe grec Platon, rappelle une de ses théories, associant quatre d'entre eux aux quatre éléments de l'ancienne physique et le cinquième à la quintessence ou Éther.

Dans ce portrait, par Jacopo de' Barbari, de Luca Pacioli, auteur de *De divina proportione*, un dodécaèdre régulier est représenté en bas à droite.

À chaque solide de Platon, on peut associer un symbole (p, q) où

p = le nombre de côtés de chaque face (ou le nombre de sommets sur chaque face),

q = le nombre de faces se rencontrant à chaque sommet (ou le nombre d'arêtes se rencontrant à chaque sommet).

Proposition 3.10

Si $\mathscr{P}$ est un solide de Platon, alors il n'y a que 5 possibilités pour le couple (p, q), qui sont $(3, 3)$, $(4, 3)$, $(3, 4)$, $(5, 3)$, $(3, 5)$.

EXERCICE DE COURS 3.19. Le but de l'exercice est de démontrer la proposition.

(1) Montrer la relation : $2A = Sq = Fp$.

(2) À l'aide de la formule d'Euler, obtenir que

$$\frac{1}{p} + \frac{1}{q} = \frac{1}{2} + \frac{1}{A} > \frac{1}{2}.$$

(3) Remarquer que $p, q \geqslant 3$ et en déduire que $p, q \leqslant 5$ et que p ou q doit être égal 3. Conclure.

Il se trouve que pour chacun des 5 couples (p, q) obtenus dans la proposition, il existe exactement un polyèdre régulier correspondant. Le théorème suivant donne la liste de ces « solides platoniciens » (« èdre » est la racine grecque pour « face », donc on peut dire « hexaèdre » au lieu de « cube » mais c'est moins courant !)

Théorème 3.11 – théorème de classification

Il n'existe que 5 polyèdres réguliers (les 5 solides de Platon) :

– le tétraèdre (4 faces),

– l'hexaèdre ou cube (6 faces),

– l'octaèdre (8 faces),

– le dodécaèdre (12 faces),

– l'icosaèdre (20 faces).

Le symbole (p, q), appelé le ***symbole de Schläfli***, donne une description combinatoire du polyèdre. Les symboles de Schläfli des cinq solides de Platon sont donnés dans la table 2, et ces cinq solides platoniciens sont représentés dans la figure 1.

polyèdre régulier	**sommets**	**arêtes**	**faces**	**symbole de Schläfli**
Tétraèdre régulier	4	6	4 triangles équilatéraux	$(3, 3)$
Hexaèdre régulier (cube)	8	12	6 carrés	$(4, 3)$
Octaèdre régulier	6	12	8 triangles équilatéraux	$(3, 4)$
Dodécaèdre régulier	20	30	12 pentagones réguliers	$(5, 3)$
Icosaèdre régulier	12	30	20 triangles équilatéraux	$(3, 5)$

TABLE 2 – Solides platoniciens

Soit $\mathscr{P}$ un polyèdre (quelconque). Notons $\mathrm{Isom}(\mathscr{P})$ le groupe des isométrie de $\mathbb{R}^3$ qui préservent $\mathscr{P}$, c'est-à-dire qui préservent les sommets de $\mathscr{P}$.

Nous avons déjà observé le fait suivant sur des examples (voir la section 2.1) : on a un morphisme injectif $\mathrm{Isom}(\mathscr{P}) \to \mathfrak{S}_n$ où n est le nombre de sommets du polyèdre de $\mathscr{P}$.

On peut alors donner une définition des polyèdres réguliers en terme d'isométries.

Définition 3.12 – polyèdre régulier

Un polyèdre $\mathscr{P}$ est dit ***régulier*** si le groupe des isométries $\mathrm{Isom}(\mathscr{P})$ agit transitivement sur les ***drapeaux*** de $\mathscr{P}$, c'est-à-dire les triplets (s, a, f) où s est un somment de $\mathscr{P}$, a une arête et f une face avec $s \in a \subset f$.

La condition de transitivité sur les drapeaux est très forte, elle implique la transitivité sur les sommets, sur les arêtes et sur les faces. On en déduit que pour un polyèdre régulier $\mathscr{P}$ donné :

- chaque face est isométrique à un même polygone régulier,
- de chaque sommet est issue le même nombre d'arêtes,
- tous les sommets sont à même distance du barycentre des sommets, appelé le ***centre*** du polyèdre ; en particulier $\mathscr{P}$ est inscrit dans une sphère.

On retrouve bien entendu les conditions de la définition 3.9.

On pourrait être tenté de définir un polyèdre régulier par la condition plus faible que toutes les faces sont isométriques à un même polygone régulier ; mais ceci n'exclurait pas par exemple les polyèdres obtenus en juxtaposant deux pyramides de base un polygone régulier à $n = 3$ ou 5 côtés (pour $n = 4$, c'est un octaèdre régulier, et pour $n \geqslant 6$, les faces ne pourraient plus être des triangles équilatéraux...). Ici le groupe d'isométrie (isomorphe au groupe diédral D_n à $2n$ éléments) agit transitivement sur les $2n$ faces, mais pas sur les $n + 2$ sommets ni les $3n$ arêtes.

Le dé à 10 faces, dont toutes les faces sont des triangles équilatéraux, n'est PAS un polyèdre régulier !

On remarque que les 2ème et 3ème lignes du tableau 2 sont symétriques, ainsi que les 4ème et 5ème (la 1ère est auto-symétrique). Un polyèdre régulier $\mathscr{P}$ admet en effet un polyèdre dual également régulier, construit en prenant l'enveloppe convexe des milieux des faces de $\mathscr{P}$. On peut vérifier que le dual d'un polyèdre admet le même groupe d'isométrie que le polyèdre initial. Du point de vue des groupes d'isométries il y a donc essentiellement 3 solides platoniciens :

- le tétraèdre, qui est auto-dual,
- le cube et l'octaèdre,
- le dodécaèdre et l'icosaèdre.

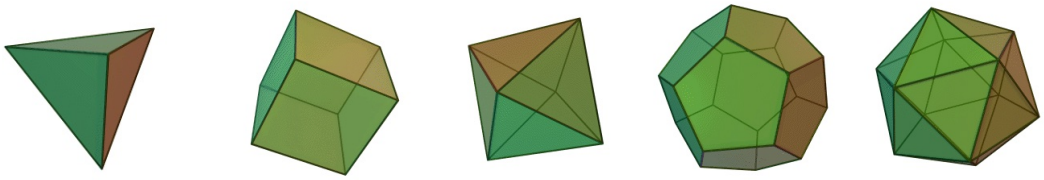
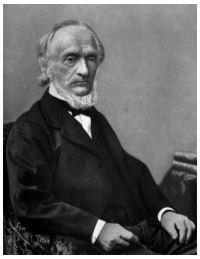


FIGURE 1 – Solides platoniniens



Ludwig Schläfli est un mathématicien suisse spécialiste en géométrie et en analyse complexe. Il a joué un rôle clé dans le développement de la notion d'espace de dimension quelconque.

Bibliographie

[1] François Combes. Algèbre et géométrie. Bréal, 1998.

[2] Yves Laszlo. Quelques exemples de sous-groupes de GL_n. https://www.cmls.polytechnique.fr/perso/laszlo/aussois/aussois.pdf

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

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

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

[6] Patrice Tauvel. Cours de géométrie, agrégation de mathématiques. Dunod, 2001.