Algèbre 1

Gaëtan Chenevier

21 juin 2024

Table des matières

1 Ensembles Quotients **2**
1.1 Partitions et Relations d'Equivalence 2
1.2 Passage au Quotient 3
1.3 Sections et systèmes de représentants 3
1.4 Lemme de Zorn 4

2 Généralités sur les Groupes **5**
2.1 Exemples de Groupes 5
2.2 Morphismes 6
2.3 Groupes Cycliques et Monogènes 7
2.4 Théorème de Lagrange 8
2.5 Sous-groupes finis de $k^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ 8
2.6 Groupes Quotients 9

3 Groupes Abéliens de Type Fini **11**
3.1 Caractères 11
3.2 Décomposition de Fourier finie 11
3.3 Structure des groupes abéliens finis 12
3.4 Existence 12
3.5 Exemple 12
3.6 Unicité 12
3.7 Groupes Abéliens de Type Fini 13

4 Groupe Symétrique et Dévissage **14**
4.1 Actions de Groupes 14
4.2 Groupes Symétriques et Alternés 15
4.3 Les suites exactes 16
4.4 Dévissage de S_n 16
4.5 Commutateur et Groupes Dérivés 17
4.6 Dévissage en Produit Semi-Direct 17

5 Groupes et Symétries **19**
5.1 Sous-groupes Finis de $O(2)$ et $SO(3)$ 19
5.2 Le Groupe $SP(1)$ 21
5.2.1 L'algèbre des quaternions de Hamilton 21
5.2.2 Le groupe $Sp(1)$ 22

5.2.3 L'espace euclidien $\mathbb{H}$ . . . 22
5.3 Groupes Linéaires et Simplicité de $PSL_n(k)$ . . . 22
5.3.1 Transvections . . . 22
5.3.2 Centre et Groupe Dérivé de $SL_n(k)$ . . . 23
5.3.3 Le critère de Simplicité d'Iwasawa . . . 23
5.3.4 Groupes Linéaires sur les Corps Finis . . . 23
5.4 Le groupe $PGL_2(k)$ et quelques (iso)morphismes miraculeux . . . 24

6 Elements de structures des groupes finis **25**
6.1 p-groupes . . . 25
6.2 Les Théorèmes de Sylow . . . 26
6.3 Le Théorème de Schur-Zassenhaus . . . 27
6.4 Théorèmes de Hall . . . 27
6.5 Extensions et Cohomologie . . . 27

7 Arithmétique des Anneaux **29**
7.1 Les anneaux $\mathbb{Z}[\sqrt{d}]$ . . . 29
7.2 Divisibilité . . . 30
7.3 Anneaux Factoriels . . . 30
7.4 Idéaux . . . 31
7.5 Anneaux euclidiens et principaux . . . 31
7.6 L'anneau $\mathbb{Z}[i]$ et sommes de deux carrés . . . 32

8 Modules sur les Anneaux Principaux **32**
8.1 Modules sur un Anneau . . . 32
8.2 Classes d'équivalence de matrices sur un anneau principal . . . 33
8.3 Modules de type fini sur un anneau principal . . . 34

9 Représentations Linéaires des Groupes Finis **35**
9.1 Représentations Linéaires . . . 35
9.2 Le point de vue $k[G]$-modules . . . 35
9.3 Décomposition en Irréductibles . . . 36
9.4 Théorie des Caractères . . . 37
9.5 Tables de Caractères . . . 40
9.6 Propriété d'intégralité des caractères . . . 42

1 Ensembles Quotients

1.1 Partitions et Relations d'Equivalence

Définition 1.1: Partition

Une *partition* d'un ensemble X est un ensemble de parties non vides de X de réunion disjointe X.

Définition 1.2: Fibre

On appelle *fibre* d'une application $f : X \to Y$ en $y \in Y$ l'ensemble $f^{-1}(y) = \{x \in X \mid f(x) = y\}$. Il s'agit d'une partition de X indexée par Y. Toute partition de X s'obtient ainsi.

Définition 1.3: Relations

Une *relation d'arité n* sur un ensemble X est la donnée d'un ensemble $R \subseteq X^n$. Une relation binaire R i.e. une partie de $X \times X$ est dite d'*équivalence* si elle est réflexive, transitive et symétrique. On appelle *classe de R-équivalence* de x l'ensemble $[x]_R = \{y \in X \mid \{x, y\} \in R\}$

Proposition 1.1: Partition en Classe d'Équivalence

Les classes d'équivalences d'une relation R sur X forment une partition de X.

Définition 1.4: Quotient

Si R est une relation d'équivalence sur X, le sous-ensemble de $P(X)$ constitué des classes de R-équivalence est appelé *ensemble quotient* de X par R, noté X/R. L'application $\pi_R : X \to X/R, x \mapsto [x]_R$ est appelée *projection canonique* associée à R. C'est une surjection dont les fibres sont par définition les classes d'équivalences de R.

Exemple 1.1.1. *On définit $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation $n \mid b - a$. On note $\overline{k}$ la classe de k.*

1.2 Passage au Quotient

Théorème 1.1: Propriété Universelle du Quotient

Soient $f : X \to Y$ une application et R une relation d'équivalence sur X. On suppose que f est constante sur chaque classe d'équivalence sur X. Alors, il existe une unique application $g : X/R \to Y$ telle que $g([x]_R) = f(x)$ pour tout $x \in X$, i.e. vérifiant $g \circ \pi_R = f$.

Démonstration. Par surjectivité de π_R, g est unique. De plus, si C est une classe de R-équivalence, il y a un sens à poser $g(C) = f(x)$ car C est une classe d'équivalence sur laquelle f est constante. ■

1.3 Sections et systèmes de représentants

Définition 1.5: Section

Une *section* de $f : X \to Y$ est une application $s : Y \to X$ telle que $f \circ s = \mathrm{id}_Y$

Proposition 1.2

f possède une section $\Rightarrow$ f est surjective

Définition 1.6: Axiome du Choix

Pour tout ensemble X il existe une application $\tau : P(X) \setminus \{\varnothing\} \to X$ telle que $\tau(E) \in E$ pour toute partie non vide E de X. On appelle τ fonction de choix sur X.

Proposition 1.3: Equivalence à l'AC

Les propositions suivantes sont équivalentes à l'axiome du choix (donc fausses) :

1. Toute surjection admet une section.
2. Pour toute famille d'ensembles non vides $\{X_i\}_{i \in I}$, $\pi_{i \in I} X_i$ est non vide.

Définition 1.7: Représentants de Classes

Un *représentant* d'une classe de R-équivalence d'un ensemble X est un élément de cette classe. Un *système de réprésentants* de (X, R) est la donnée d'une partie de X contenant un et un seul représentant de chaque classe de R-équivalence. C'est l'image d'une section de π_R.

Remarque 1.3.0.1. *Ceci est également équivalent à 1.6*

1.4 Lemme de Zorn

Définition 1.8: Ordres

- Un *relation d'ordre* sur un ensemble X est une relation binaire $\leq$ réfléxive, transitive et antisymétrique. On dit alors que X est ordonné.
- L'ordre $\leq$ est total quand tous deux éléments de X sont comparables.
- On appelle majorant d'une partie Y de X, tout élément $x \in X$ tel que $y \leq x$ pour tout $y \in Y$. On parle de plus grand élément dans le cas $Y = X$.
- $x \in X$ est un élément maximal si le seul $y \in X$ tel que $y \leq x$ est x. Un plus grand élément est nécessairement maximal, et unique s'il existe.
- On appelle X inductif si tout sous-ensemble totalement ordonné admet et majorant.
- On appelle bon ordre un ordre pour lequel toute partie non vide admet un plus petit élément.

Théorème 1.2: Lemme de Zorn

Un ensemble ordonné inductif possède au moins un élément maximal. Ceci est équivalent à l'axiome du choix 1.6.

Corollaire 1.1

Tout espace vectoriel possède une base.

Corollaire 1.2: Théorème de Zermelo

Tout ensemble peut être muni d'un bon ordre.

Démonstration. C'est équivalent à l'axiome du choix donc faux et les preuves prennent trois plombes. ∎

2 Généralités sur les Groupes

2.1 Exemples de Groupes

Définition 2.1: Loi Interne

Une *loi de composition interne* est une application $\star : X \times X \to X$.

Définition 2.2: Groupe

Un groupe est un ensemble G muni d'une loi de composition associative, unifère et inversible, i.e. :

1. $\forall\ (x, y, z) \in G,\ x \star (y \star z) = (x \star y) \star z$
2. $\exists\ e \in G,\ \forall x \in G,\ e \star x = x \star e = x.$
3. $\forall x \in G,\ \exists y \in G,\ x \star y = y \star x = e$

Remarque 2.1.0.1. *Le neutre est unique.*

Exemple 2.1.1 (Groupe Symétrique)**.** *On note :* $\mathfrak{S}_X = X^X$ *le groupe muni de la loi* $\circ$ *de composition des applications, appelé* groupe symétrique *de* X*, de neutre* id_X*. L'inverse d'une bijection* σ *est sa bijection réciproque* σ^{-1}*. On note* $\mathfrak{S}_n = |1, n|^{|1,n|}$ *et alors* $|\mathfrak{S}_n| = n!$.

Définition 2.3: Groupe Abélien

Un groupe est dit *abélien* lorsque tous deux élements commutent.

Définition 2.4: Sous-Groupe

Une partie H d'un groupe G est un *sous-groupe* de G lorsque la loi induite par le produit dans G fait de H un groupe. On le notera ici $H \leq G$.

Exemple 2.1.2 (Groupes d'ordre n)**.** *Pour* $n \geq 1$*, on note* μ_n *le sous-groupe de* $\mathbb{C}^\times$ *composé des racines* n*-ièmes de l'unité. C'est un sous-groupe d'ordre* n*. L'application* $\mathbb{Z}/n\mathbb{Z} \to \mu_n, \overline{k} \mapsto e^{2ik\pi/n}$ *est un isomorphisme de groupe.*

Définition 2.5: Anneau

Un *anneau* est un groupe abélien $(A, +)$ muni d'une loi associative unifère et distributive sur $+$, notée $\times$. Il est dit commutatif lorsque la loi produit est commutative.

Définition 2.6: Groupe des Inversibles

On note $A^\times$ le groupe des inversibles du monoïde $(A, \cdot)$.

Proposition 2.1: Groupe Réel

La loi d'un groupe vérifie les propriété de la loi produit usuelle sur $\mathbb{R}$.

Définition 2.7: Groupe Engendré

On appelle groupe engendrée par une partie X de G le plus petit sous groupe de G contenant X. C'est l'ensemble des produits de puissances d'éléments de X.

2.2 Morphismes

Définition 2.8: Morphisme

On appelle *morphisme* une application entre deux groupes qui préserve le produit. On note $Hom(G, G^{'})$ l'ensemble des morphismes de G dans $G^{'}$. Ce n'est à priori pas naturellement un groupe si $G^{'}$ n'est pas abélien.
On dit que G et $G^{'}$ sont isomorphes lorsqu'il existe un morphisme bijectif de l'un vers l'autre. La réciproque d'un isomorphisme est un isomorphisme. On note alors $G \simeq G^{'}$.

Proposition 2.2: Transport de Structure

Si G est un groupe, $\varphi : X \to G$ une bijection, il existe une unique loi de groupe sur X telle que φ soit un isomorphisme, à savoir $x \star y = \varphi^{-1}(\varphi(x)\varphi(y))$. On dit que la loi est *déduite* de celle de G par transport de structure via φ.

Définition 2.9: Automorphisme

On appelle *automorphisme* de G un isomorphisme de G dans G. L'ensemble des automorphismes $Aut(G)$ est un sous groupe de S_G. On appelle automorphisme intérieur associé à $g \in G$ l'application : $h \in G \mapsto ghh^{-1}$.

Définition 2.10: Noyau

On appelle *noyau* d'un morphisme $\ker(f) = f^{-1}(1) = \{g \in G \mid f(g) = 1\}$. C'est un sous-groupe de G.

Proposition 2.3: Groupe des Homomorphismes

Si $f \in Hom(G, G^{'})$:

1. $H \leq G \Rightarrow f(H) \leq G^{'}$
2. $H \leq G^{'} \Rightarrow f^{-1}(H) \leq G$ Avec $\mathcal{A}$ l'ensemble des sous-groupes de G contenant $\ker f$ et $\mathcal{B}$ celui des sous-groupes de $G^{'}$ inclus dans $\mathrm{Im} f$, alors :
3. $\mathcal{A} \to \mathcal{B}, H \mapsto f(H)$ est une bijection croissante.

Proposition 2.4: Fibres d'un Morphisme

Les fibres non vides de f sont en bijection avec $\ker f$. En particulier :

- f injective $\Leftrightarrow \ker f = \{1\}$.
- Si G est fini, $|G| = |\mathrm{Im}\ f|\,|\ker f|$.

Théorème 2.1: Cayley

Tout groupe d'ordre fini n est isomorphe à un sous-groupe de S_n.

Lemme 2.2.1. *Si $\varphi : X \to Y$ est bijective, l'application : $\varphi_{X,Y} : S_X \to S_Y, \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ est un isomorphisme de groupes.*

Définition 2.11: Morphisme d'Anneau

Un morphisme d'anneau est un morphisme des groupes additifs et des monoïdes multiplicatifs (en particulier, il envoie 1 sur 1).

2.3 Groupes Cycliques et Monogènes

Proposition 2.5: Sous-Groupes de Z

Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$.

Proposition 2.6: Groupes Finis

Si $g \in G$ est d'ordre fini n, alors $\langle g \rangle$ a exactement n éléments et est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Définition 2.12: Groupes Monogènes

Un groupe G est *monogène* s'il est engendré par un seul élément, appelé *générateur*. Il est *cyclique* s'il est fini.

Corollaire 2.1: Groupes Monogènes

Un groupe G est monogène infini si et seulement si il est isomorphe à $\mathbb{Z}$. Il est cyclique d'ordre $n \geq 1$ si et seulement si isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.7: Générateurs d'un Groupe Cyclique

- Les générateurs de $\mathbb{Z}, +$ sont les $k \in \mathbb{Z}$ tels que $\mathbb{Z} = k\mathbb{Z}$, i.e. $k = \pm 1$.
- Pour $k \in \mathbb{Z}$, $G = \langle g \rangle$ un groupe cyclique d'ordre n, on a équivalence entre :
  1. $\left\langle g^k \right\rangle = G$
  2. $g \in \left\langle g^k \right\rangle$
  3. $\exists k' \in \mathbb{Z},\ kk' = 1 \bmod n$
  4. $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$
  5. $k \wedge n = 1$

Corollaire 2.2: Nombre de Générateurs

Un groupe cyclique d'ordre n a exactement $\varphi(n)$ générateurs.

Corollaire 2.3: Isomorphisme aux Automorphismes

Si G est cyclique d'ordre n : $Aut(G) = \left\{ g \mapsto g^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times \right\}$. On a alors un isomorphisme de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans $Aut(G)$.

Remarque 2.3.0.1. *Si $g \in G$ est d'ordre fini n, si $d \geq 1$, g^d est d'ordre fini $\frac{n}{n \wedge d}$.*

Proposition 2.8: Diviseurs d'un Groupe

Si G est cyclique d'ordre n, $d \mapsto G_d = \left\{ g^d \mid g \in G \right\}$ est une bijection de l'ensemble des diviseurs de n sur l'ensemble des sous-groupes de G.

Théorème 2.2: Chinois

Soient $m, n \in \mathbb{Z}$ premiers entre eux. L'application $\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, $k \mapsto (k \mod n, k \mod m)$ définit un isomorphismepar par passage au quotient de par la propriété universelle 1.1.

2.4 Théorème de Lagrange

Définition 2.13: Produit de Parties

Si A, B sont deux parties d'un groupe, $AB = \{ab \mid a \in A, b \in B\}$. Si $A = \{g\}$, on le note gB.

Lemme 2.4.1. $H \leq G \Leftrightarrow \left(H \neq \varnothing, HH = H, H^{-1} = H\right)$.

Définition 2.14

On pose $g \sim_H g^{'}$ si $g^{'} \in gH$. C'est une relation d'équivalence. On note G/H son ensemble quotient, et on appelle indice de H dans G son cardinal noté $[G : H]$.

Théorème 2.3: Lagrange

Si H est un sous-groupe de G, $G \sim H \times (G/H)$. En particulier, si deux des trois ensembles $G, H, G/H$ sont finis, $|G| = |H|\,[G : H]$.

Corollaire 2.4

- Si H est un sous-groupe du groupe fini G, $|H| \mid |G|$.
- Si G est fini, $g \in G$, $g^{|G|} = 1$.
- $n^{p-1} \cong 1 \bmod p$ pour $n \in \mathbb{Z}, p \in \mathbb{P}$.
- Tout groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Théorème 2.4: Cauchy

Soit G un groupe fini, p un nombre premier divisant $|G|$. G possède un élément d'ordre p. Si G est abélien, on peut généraliser immédiatement à tout $p \in \mathbb{Z}$.

2.5 Sous-groupes finis de $k^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times$

Théorème 2.5: Sous-Groupes Finis d'un Corps

Si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.

Lemme 2.5.1 (Cauchy)**.** *Soit G un groupe, x, y deux éléments qui commutent d'ordres a et b premiers entre eux. Alors, xy est d'ordre ab.*

Théorème 2.6: Gauss

Pour p premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Définition 2.15: Logarithme Discret

Un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^{times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ est appelé un logarithme discret.

Définition 2.16: Groupe des Puissances

Pour un groupe, on note $G^{(n)}$ le groupe des puissances n-ièmes.

Proposition 2.9: Ordre du Groupe des Puissances

Soient $p \in \mathbb{P}$, $n \geq 1$ et $m = (p-1) \wedge n$.

1. $(\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ est cyclique d'ordre $\frac{p-1}{m}$ et égal à $(\mathbb{Z}/p\mathbb{Z})^{\times,(m)}$
2. Pour $x \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, on a $x \in (\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ si et seulement si $x^{\frac{p-1}{m}} = 1$, i.e. $X^{\frac{p-1}{m}}$ a au plus $\frac{p-1}{m}$ racines dans $\mathbb{Z}/p\mathbb{Z}$ et donc ses racines sont exactement les puissances n-èmes.

Proposition 2.10: Groupe Quotient Puissance

Si p est premier impair, $m \geq 1$, alors $(\mathbb{Z}/p^m\mathbb{Z})^{\times}$ est cyclique. Si $m \geq 2$, $(\mathbb{Z}/2^m\mathbb{Z})^{\times} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$

2.6 Groupes Quotients

Définition 2.17: Groupe Distingué

Un sous-groupe H de G est dit *distingué*, noté $H \lhd G$ si l'une des conditions équivalentes suivantes est vérifiée :

1. $gHg^{-1} \subset H, \ \forall g \in G$
2. $gHg^{-1} = H, \ \forall g \in G$
3. $gH = Hg, \ \forall g \in G$.

Remarque 2.6.0.1. *Tous les sous-groupes d'un groupe abélien sont distingués. Un groupe d'indice* 2 *dans G est distingué.*

Définition 2.18: Normalisateur

Le normalisateur de H dans G est le sous-groupe de G défini par $N_G(H) = \left\{g \in G \mid gHg^{-1} = H\right\}$.

Théorème 2.7: Projection de loi

Soit H un sous groupe d'un groupe G.

1. Il existe au plus une loi de groupe sur G/H telle que la projection canonique $G \to G/H$ soit une loi de groupe.
2. Une telle loi existe si, et seulement si, on a $H \lhd G$, auquelle cas c'est la loi induite par le produit sur $P(G)$.

Définition 2.19: Groupe Quotient

Si $H \lhd G$, le groupe quotient G/H est la donnée de l'ensemble G/H muni de son unique loi de groupe telle que la projection canonique est un morphisme de groupes.

Définition 2.20: Symbole de Legendre

On pose $\left(\frac{x}{p}\right) = 1$ si x est un carré non nul, 0 si x est nul et -1 sinon. $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme multiplicatif.

On va étudier les groupes en chercher à étudier des groupes plus simples : étant donné un groupe G, on cherche $H \subsetneq G$ un groupe distingué non trivial pour étudier H et G/H, d'ordres plus petits.

Définition 2.21: Groupes Simples

Un groupe G est dit *simple* si ses seuls groupes distingués sont $\{1\}$ et G.

Théorème 2.8: Propriété Universelle des Groupes Quotients

Si $H \lhd G$, et si $f : G \to G^{'}$ est un morphisme, $g = f \circ \pi$ est un morphisme de G/H dans $G^{'}$ tel que $g(H) = 1$.

Théorème 2.9: Premier Théorème d'Isomorphisme

Si f est un morphisme de G dans $G^{'}$, alors f induit par passage au quotient un isomorphisme de groupes de $G/\ker f$ dans Imf

Proposition 2.11: Troisième Théorème d'Isomorphisme

Soit $H \lhd G$:

1. $H \mapsto K/H$ induit une bijection croissante entre sous groupes de G contenant H et sous-groupes de G/H.
2. Dans cette bijection, $K/H \lhd G/H \Leftrightarrow K \lhd G$ auquel cas le morphisme naturel $G/H \to G/K$ induit un isomorphisme $(G/H)\,/\,(K/H) \to G/K$.

3 Groupes Abéliens de Type Fini

3.1 Caractères

Définition 3.1: Caractère d'un Groupe

Un *caractère* d'un groupe G est un morphisme de G dans $\mathbb{C}^\times$.

Proposition 3.1: Caractères d'un Groupe Cyclique

Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. Pour $\zeta \in \mu_n$, il existe un unique caractère χ_ζ de G tel que $\chi_\zeta(g) = \zeta$. De plus, $\zeta \mapsto \chi_\zeta$ est un isomorphisme de groupes.

3.2 Décomposition de Fourier finie

Définition 3.2: Espace Hermitien L^2

Si G est un groupe fini, on note $L^2(G)$ le $\mathbb{C}$-espace vectoriel des fonctions $G \to \mathbb{C}$ muni du produit hermitien. C'est un espace de dimension finie $|G|$. On note $\hat{G}$ l'ensemble des caractères de G. On rappelle que $\mathbb{C}^\times$ étant abélien, $\hat{G} = Hom(G, \mathbb{C}^\times)$

Théorème 3.1: Orthogonalité des Caractères

Soit G un groupe fini.

1. L'ensemble $\hat{G}$ est une famille livre et orthonormée de $L^2(G)$ (Orthogonalité des Caractères)
2. Si G est abélien, $\hat{G}$ est une base de $L^2(G)$.

Corollaire 3.1

Soit G abélien fini

1. On a $\left|\hat{G}\right| = |G|$
2. Pour toute fonction $f : G \to \mathbb{C}$ on a $f = \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi$

Proposition 3.2: Extension de Caractère

Soit G abélien fini, $H \subset G$ un sous-groupe. Pour tout caractère χ de H, il existe $\tilde{\chi}$ de G tel que $\tilde{\chi_{|H}} = \chi$

Définition 3.3: Divisibilité d'un Groupe

Un groupe abélien D est *divisible* si le morphisme de groupes $x \mapsto x^n$ est surjectif pour tout $n \geq 1$.

Proposition 3.3: Prolongement des Morphismes

Soient G, H, D des groupes abéliens avec D divisible, $H \subset G$ et $f : H \to D$ un morphisme de groupes. Alors il existe un morphisme de groupes $\tilde{f} : G \to D$ tel que $\tilde{f_{|H}} = f$.

3.3 Structure des groupes abéliens finis

Théorème 3.2: Structure des Groupes Abéliens Finis

Soit G abélien fini, il existe un unique entier $n \geq 0$ et des uniques entiers $a_i > 1$ vérifiant $a_1 \mid a_2 \mid \ldots \mid a_n$ et $G \simeq \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$.

Définition 3.4: Exposant d'un Groupe

L'*exposant* d'un groupe fini G est le plus petit entier $e \geq 1$ vérifiant $g^e = 1$ pour tout $g \in G$. C'est le ppcm des ordres des éléments de G.

3.4 Existence

Lemme 3.4.1. *Si G est abélien fini, il existe un élément d'ordre l'exposant.*

Proposition 3.4: Produit de Groupes

Soit G un groupe, $H \leq G, K \leq G$. On suppose $H \cap K = 1,\ G = HK$ et enfin $hk = kh$ pour tout $h \in H,\ k \in K$. L'application produit sur $H \times K$ définit un isomorphisme de groupes.

De ces deux propositions, on peut prouver la partie existence du théorème.

3.5 Exemple

Définition 3.5: Groupe Élémentaire

Soit p un nombre premier. Un groupe abélien fini est p-élémentaire si on a $g^p = 1$ pour tout $g \in G$.

Définition 3.6: Espace Vectoriel d'un Groupe

On définit $G^\sharp$ le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel dont G est le groupe additif.

Proposition 3.5: Groupe Élémentaire et Générateurs

Soit p premier, G abélien fini. G est p-élémentaire si et seulement si $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ pour un certain $n \geq 1$. Le nombre minimal de générateurs de G est $\dim_{\mathbb{Z}/p\mathbb{Z}} G^\sharp$.

3.6 Unicité

Définition 3.7

On note $\min(G)$ le nombre minimal de générateurs de G. Il est fini si et seulement si G est de type fini.

Proposition 3.6

Supposons qu'on écrit une décomposition de G comme dans le théorème 3.2. On a $n = \min(G)$

Définition 3.8: Torsion d'un Groupe

Soit G abélien. Le sous-ensemble $G[n] = \{g^n = 1\}$ est un sous groupe de G appelé n-torsion de G.

Lemme 3.6.1. *Soit G et H abéliens et $n \geq 1$.*

1. *On a $(G \times H)[n] = G[n] \times H[n]$*
2. *Tout (iso-)morphisme $G \to H$ induit un (iso-)morphisme $G[n] \to H[n]$.*
3. *Supposons G cyclique d'ordre m et p premier. Alors $G[p] = \{1\}$ sauf si $p \mid m$ auquel cas $G[p] \simeq \mathbb{Z}/p\mathbb{Z}$ et $G/G[p] \simeq \mathbb{Z}/m/p\mathbb{Z}$.*

3.7 Groupes Abéliens de Type Fini

On note ici G un groupe abélien additif

Définition 3.9: Familles libres, génératrices, bases

Soit $\mathcal{F} = \{g_1, \ldots, g_n\}$ une famille d'éléments de G et

$$f : \mathbb{Z}^n \to G, (m_i) \mapsto \sum_{i=1}^{n} m_i g_i$$

On dit que $\mathcal{F}$ est libre (ou $\mathbb{Z}$-libre) si f est injectif. On dit que $\mathcal{F}$ est génératrice si f est surjectif, et est une base si f est bijectif.

Définition 3.10: Groupe Libre

Un groupe abélien est dit *libre de rang n* s'il possède une $\mathbb{Z}$ base à n éléments, i.e. s'il est isomorphe à $\mathbb{Z}^n$. Par conventions, $\{0\}$ est libre de rang 0.

Lemme 3.7.1. *Pour tout entier $n \geq 0$, $\min(\mathbb{Z}^n) = n$. En particulier, $\mathbb{Z}^n \simeq Z^m \Leftrightarrow n = m$.*

Définition 3.11: Sous-Groupe de Torsion

On appelle *sous-groupe de torsion* de G, le sous-groupe de G noté $G_{\text{tor}} = \{g \in G \mid \exists n \geq 1,\ ng = 0\}$

Théorème 3.3: Dirichlet

Si G est abélien de type fini, G_{tor} est fini et il existe un unique $n \in \mathbb{N}$ tel que $G \simeq G_{\text{tor}} \times \mathbb{Z}^n$.

Corollaire 3.2

Un groupe abélien de type fini sans torsion est libre

Lemme 3.7.2. *Si $f : G \to \mathbb{Z}$ est surjectif, $G \simeq \mathbb{Z} \times \ker f$.*

Lemme 3.7.3. *Si A, B sont deux groupes abéliens avec A fini et B libre de rang fini, alors, avec $G = A \times B$: $G_{tor} = A \times \{0\}$ et $G/G_{tor} \simeq B$.*

4 Groupe Symétrique et Dévissage

4.1 Actions de Groupes

Définition 4.1: Action de Groupe

Une action de G sur X est une application : $\cdot : G \times X \to X$ vérifiant : $1 \cdot x = x$ et $g \cdot (h \cdot x) = (gh) \cdot x$.

Définition 4.2: Orbite et Stabilisateur

Soit G agissant sur X, et $x \in X$.

- $O_x = \{gx \mid g \in G\} \subset X$ est l'*orbite* de x sous G, aussi notée Gx.
- Le sous-groupe $G_x = \{g \in G \mid gx = x\}$ est appelé *stabilisateur* de x ou *groupe d'isotropie de x*, noté $\mathrm{Stab}_G(x)$.

Lemme 4.1.1. *On a :* $G_{gx} = gG_xg^{-1}$.

Proposition 4.1: Orbites d'une Action

- Les orbites sous G forment une partition de X.
- Pour tout $x \in X$, on a une bijection $G/G_x \xrightarrow{\sim} O_x$ envoyant gG_x sur gx. En particulier, si G est fini, on a $|G| = |G_x|\,|O_x|$

Corollaire 4.1: Système de Représentants

On note x_i des représentants des orbites de G dans X. On a :

$$|X| = \sum_{i\in I} |O_{x_i}| = \sum_{i\in I} |G| \,/\, |G_{x_i}|$$

Théorème 4.1: Premier Théorème de Sylow

Soit G fini d'ordre $p^n m$ avec p premier et $m \wedge p = 1$. Alors G possède un sous-groupe d'ordre p^n, appelé un p-Sylow de G.

Définition 4.3: Action Transitive

Une action de G sur X est *transitive* si on a $X \neq \varnothing$ et si $\forall\, x, y \in X,\ \exists\, g \in G,\ y = gx$, i.e. que X a une et une seule orbite sous l'action de G.

Définition 4.4: Action Fidèle

Le noyau d'une action est le noyau du morphisme $G \to S_X$ associé à l'action. C'est un sous-groupe distingué de G. Une action est dite *fidèle* si son noyau est $\{1\}$.

Définition 4.5: Action Libre

Une action est *libre* si on a toujours $G_x = \{1\}$.

Définition 4.6: Isomorphisme d'Actions

Deux actions d'un même groupe sur deux ensembles X et Y sont *isomorphes* s'il existe une bijection f vérifiant $f(g \cdot x) = g \star f(x)$.

Proposition 4.2: Action par Translations

Une action transitive $(X, \cdot)$ est isomorphe à l'action par translations de G sur G/G_x

Proposition 4.3: Isomorphisme et Stabilisateurs

Deux actions transitives sont isomorphes si et seulement si elles ont les mêmes stabilisateurs.

4.2 Groupes Symétriques et Alternés

Proposition 4.4: Décomposition en Cycle

Toute permutation σ de S_n s'écrit comme un produit de cycles à supports disjoints. L'ordre de σ est alors le ppcm des longueurs des cycles.

Proposition 4.5: Transpositions

Les transpositions engendrent S_n

Lemme 4.2.1. *Si $\sigma \in S_n$, $c = (i_1, \ldots, i_k)$ est un k-cycle : $\sigma c \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$.*

Proposition 4.6: Générateurs de Coxeter

- Les $(i, i+1)$ engendrent S_n. Ils sont appelés générateurs de Coxeter.
- La transposition $(1, 2)$ et le cycle $(12 \ldots n)$ engendrent S_n.

En particulier, $\min S_n = 2$.

Définition 4.7: Partition d'un Entier

- Une partition de l'entier n est une suite décroissante $n_1 \geq \ldots \geq n_r$ d'entiers strictement positifs de somme n.
- Le type de $\sigma \in S_n$ est la partition de l'entier n définie par les cardinaux des orbites de σ.

Proposition 4.7: Conjugaison et type

Deux éléments de S_n sont conjugués si et seulement si ils ont même type.

Définition 4.8: Action Transitive et Permutations

Pour $k \geq 1$ entier, G agissant sur X avec $|X| \geq k$, G agit k-transitivement sur X si pour deux k-uplets d'éléments distincts de X il existe $g \in G$ tel que $gx_i = y_i$ pour tout i.

Définition 4.9: Signature

La *signature* de $\sigma \in S_n$ est :

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j}$$

C'est un morphisme de groupes $S_n \to \{\pm 1\}$ valant -1 sur les transpositions. On note A_n son noyau. C'est un sous-groupe distingué.

Proposition 4.8: Conjugaison de Cycles

Pour $n \geq 3$, A_n agit $(n-2)$-transitivement sur $|1, n|$. Les k-cycles sont conjugués sous l'action de A_n pour $k \in |2, n-2|$.

4.3 Les suites exactes

Définition 4.10: Suite Exacte

Une suite de $n \geq 2$ morphismes de groupes $(f_1, \ldots, f_n)$ est *exacte* si $\operatorname{Im} f_i = \ker f_{i+1}$ pour tout i.

Définition 4.11: Suite Exacte Courte

Une suite exacte de la forme $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ est une suite exacte *courte*.

Proposition 4.9: S.E.C. et Groupes Distingués

Il est équivalent de se donner :

- Une suite exacte $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$
- Un sous-groupe distingué $H' \subset G$ et des isomorphismes $i' : H \xrightarrow{\sim} H'$ et $\pi' : G/H' \xrightarrow{\sim} K$.

Définition 4.12: Groupe Diédral

Pour $n \geq 3$, on définit le groupe diédral D_{2n} comme le sous groupe de S_n engendré par $(12 \ldots n)$ et l'élément τ défini par $\tau(i) = n + 1 - i$.

Définition 4.13: Extension de Groupes

Si G, H, K sont des groupes donnés, G est extension de K par H s'il existe une suite exacte courte $1 \to H \to G \to K \to 1$.

4.4 Dévissage de S_n

Théorème 4.2: Groupes Distingués de S_n

Les seuls sous-groupes distingués de S_n sont $\{1\}, A_n, S_n$ et K_4 dans le cas $n = 4$.

Théorème 4.3: Simplicité du Groupe Alterné

Pour $n \geq 5$, A_n est simple non abélien.

Corollaire 4.2: Actions du Groupe Alterné

- Pour $n \neq 4$, toute action de A_n est fidèle ou triviale.
- Une action transitive de S_n sur un ensemble à $m > 2$ éléments est fidèle, sauf peut-être si $n = 4$ et $m = 3$ ou 6.

4.5 Commutateur et Groupes Dérivés

Définition 4.14: Groupe Dérivé

Le *groupe dérivé* d'un groupe G est le sous-groupe $D(G) = [G, G]$ engendré par les $[x, y] = xyx^{-1}y^{-1}$. On a $D(G) = \{1\}$ si et seulement si G est abélien.

Corollaire 4.3

$D(G)$ est un sous-groupe caractéristique de G.

Corollaire 4.4

Soit G un groupe.

- Tout morphisme $f : G \to G^{'}$ avec $G^{'}$ abélien vérifie $D(G) \subset \ker f$.
- Pour $H \lhd G$ alors G/H est abélien si et seulement si, $D(G) \subset H$.

Proposition 4.10: Dérivation du Groupe Symétrique

On a :

- $D(S_n) = A_n$
- $D(A_n) = A_n$ pour $n \geq 5$.
- $D(A_4) = K_4$ et $D(A_n) = \{1\}$ pour $n \leq 3$

Définition 4.15: Résolubilité

Un groupe G est résoluble s'il existe n tel que $D^n(G) = \{1\}$. Le plus petit n est appelé classe de résolubilité de G.

Proposition 4.11: Résolubilité et Quotient

Si G est un groupe et $H \lhd G$, G est résoluble si et seulement si H et G/H le sont. Alors, la classe de G est inférieure à la somme des classes de H et de G/H.

Proposition 4.12: Résolubilité des Groupes Triangulaires

Le groupe $T_n(k)$ est résoluble de classe $\leq 1 + \lceil \log_2(n) \rceil$.

4.6 Dévissage en Produit Semi-Direct

Définition 4.16: Complément

Si $H \leq G$, un *complément* de H dans G est $K \leq G$ tel que $G = HK$ et $H \cap K = \{1\}$

Remarque 4.1: Complément et Structure

Soit $N \lhd G$, et K un complément de N dans G. Pour tout $n, n^{'} \in N$, $k, k^{'} \in K$, on a :

$$(nk)(n^{'}k^{'}) = n(kn^{'}k^{-1})kk' \text{ avec } kn^{'}k^{-1} \in N$$

Autrement dit :

$$(nk)(n^{'}k^{'}) = n\mathrm{int}_k(n')kk'$$

La structure de groupe de G se déduit de celle de N, K et de la connaissance de l'application : $\alpha : k \in K \mapsto \mathrm{int}_{k|N}$

On se fixe dans la suite deux tels groupes N et K, et un morphisme de groupe α de K dans $\mathrm{Aut}(N)$.

Définition 4.17: Produit Semi-Direct Externes

La loi $\star_\alpha : (N \times K) \times (N \times K) \to N \times K, (n,k), (n^{'}, k^{'}) \mapsto (n\alpha_k(n^{'}), kk^{'})$ est une loi de groupe, qui munit $N \times K$ d'une structure de groupe noté $N \rtimes_\alpha K$ et appelé produit semi-direct (externe) de K par N associé à α.

Proposition 4.13: Produit Semi-Direct Interne

Soit G un groupe, $N \lhd G$ et K un complément de N dans G. Soit $\alpha : K \to \mathrm{Aut}(N)$, $k \mapsto \alpha_k$. La bijection $N \times K \to G, (n,k) \mapsto nk$ est un isomorphisme de groupes : $N \rtimes_\alpha K \xrightarrow{\sim} G$. On dit aussi que G est *produit semi-direct interne* de K par N

Proposition 4.14: Suivi des Isomorphismes

Soit $G = N \rtimes_\alpha K$, $a : N^{'} \xrightarrow{\sim} N$ et $b : K^{'} \xrightarrow{\sim} K$ des isomorphismes. La bijection $N^{'} \times K^{'} \to G, (n^{'}, k^{'}) \mapsto a(n^{'})b(k^{'})$ est un isomorphisme de groupes de $N^{'} \rtimes_{\alpha'} K^{'}$ dans G, où $\alpha^{'} : k^{'} \mapsto \alpha_{k'} = a^{-1} \circ \alpha_{b(k')} \circ a$.

Proposition 4.15: Groupe d'Ordre $2p$

Un groupe d'ordre $2p$ avec p premier impair est soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$ soit à D_{2p}.

Proposition 4.16: Petits Groupes Non Abéliens

Les groupes non abéliens d'ordre ≤ 8 sont S_3, D_8 et H_8.

5 Groupes et Symétries

5.1 Sous-groupes Finis de $O(2)$ et $SO(3)$

. Ici, E est un espace euclidien de dimension $n \geq 1$

Définition 5.1: Réflexion

On définit la *réflexion* par rapport à H un hyperplan de E, l'application $s_H \in O(E)$ définie par : $s_H(h+d) = h - d$ où $h, d \in H \times H^{\perp}$. Pour $v \in E$ non nul, on appelle aussi *réflexion de vecteur* v la réflexion $s_v = s_{v^{\perp}}$.

Théorème 5.1: Cartan-Dieudonné

Tout élément de $O(E)$ est produit d'au plus n réflexions. En particulier, tout élément de $SO(E)$ est produit d'au plus $n/2$ produits de deux réflexions.

Remarque 5.1.0.1. *$SO(2)$ est isomorphe au groupe S^1 des rotations du plan. On peut également montrer que $O(2) \simeq SO(2) \rtimes_{\alpha} \mathbb{Z}/2\mathbb{Z}$ avec $\alpha_{\bar{1}}(g) = g^{-1}$.*

Corollaire 5.1: Droites Fixes

Tout élément non trivial de $SO(3)$ possède une et une seule droite fixe dans E.

Lemme 5.1.1. *Si $g \in O(E)$ préserve $F \subset E$, il préserve $F^{\perp}$.*

Définition 5.2: Isométries Orthogonales

Pour $P \subset E$, on note $\mathrm{Iso}(P) = \{g \in O(E) \mid g(P) = P\}$ le sous-groupe des isométries orthogonales de P.

Définition 5.3: Polygones Réguliers

On note $\mathscr{P}_m$ un polygone régulier du plan à $m \geq 3$ côtés centré en 0.

Proposition 5.1: Action sur les Sommets

$\mathrm{Iso}(\mathscr{P}_m)$ agit sur l'ensemble $\mathscr{S}$ des sommets de $\mathscr{P}_m$, puisque ce sont les points à distance maximale de 0. Cette action définit un morphisme f qui induit un isomorphisme $\mathrm{Iso}(\mathscr{P}_m) \xrightarrow{\sim} D_{2m}$. De plus, $\mathrm{Iso}^+(\mathscr{P}_m) \simeq \mathbb{Z}/m\mathbb{Z}$.

En considérant les groupes d'isométries de figures planes bien choisies, on trouve trois autres classes de conjugaison.

Proposition 5.2: Groupes Finis des Symétries du Plan

Soit $G \leq O(2)$ fini. Alors, soit G est isomorphe à 1, $\mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$, soit il existe un polygone régulier $\mathscr{P}$ du plan euclidien tel que $G = \mathrm{Iso}(\mathscr{P})$ ou $G = \mathrm{Iso}^+(\mathscr{P}_)$

Remarque 5.1.1.1. *Le groupe des isométries de $[-1, 1] \times \{0\}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, qu'on note parfois D_4.*

Définition 5.4: Groupes Irréductibles Orthogonaux

$G \leq O(E)$ est dit irréductible, s'il n'existe aucun sous-espace non-dégénéré stable par G.

On suppose désormais $n = 3$.

Remarque 5.1.1.2. *Un groupe est irréductible s'il stabilise un plan ou, de manière équivalente, une droite. On a donc un morphisme injectif* diagonal *:*
$$\begin{array}{rcl} O(2) & \to & SO(3) \\ g & \mapsto & \begin{pmatrix} g & 0 \\ 0 & \det g \end{pmatrix} \end{array}$$

Définition 5.5: Solide de Platon

Soit $P \subset E$ un *solide de Platon* [a]. On définit ses sommets, ses arêtes et ses faces comme ses parties extrémales de dimension 0, 1 et 2 :

$$\forall x, y \in P,\ ]x, y[\ \cap F \neq \varnothing \Rightarrow [x, y] \subset F$$

L'action de $\mathrm{Iso}(P)$ préserve l'ensemble $\mathscr{S}$ des sommets, celui $\mathscr{A}$ des arêtes et celui $\mathscr{F}$ des faces. On note que l'action de $\mathrm{Iso}(P)$ sur $\mathscr{S}$ engendre E. Notons que dès que $-1 \in \mathrm{Iso}(P)$, $\mathrm{Iso}(P) = \{\pm 1\} \times \mathrm{Iso}^+(P)$.

a. polyèdre régulier

- Le Tétraèdre Régulier T : En regardant l'action sur les sommets, on obtient :

  Proposition 5.3

  $\mathrm{Iso}(T) \simeq S_4$ et $\mathrm{Iso}^+(T) \simeq A_4$.

  Le déterminant sur $\mathrm{Iso}(T)$ correspond à la signature sur S_4. En regardant de plus les paires d'arêtes orthogonales, on fournit un morphisme $\mathrm{Iso}(T) \to S_3$.
- Le Cube ou Hexaèdre Régulier C : En regardant l'action sur les paires de sommets, on obtient :

  Proposition 5.4

  $\mathrm{Iso}^+(C) \simeq S_4$ et $\mathrm{Iso}(C) = \{\pm 1\} \times \mathrm{Iso}^+(C)$.

  En considérant l'action sur les paires de faces opposées, on retrouverait un morphisme $S_4 \to S_3$.
- L'Octaèdre Régulier O : En regardant les centres des faces, on trouve un cube C appelé cube dual et dont les centres des faces sont les sommets d'un nouvel octaèdre O'. On en déduit que :

  Proposition 5.5

  $\mathrm{Iso}(O) = \mathrm{Iso}(C) = \mathrm{Iso}(O')$
- Le Dodécaèdre Régulier D : En regardant l'action sur les sommets, et en regardant les triplets de diarête [1] deux à deux orthogonales, on obtient :

  Proposition 5.6

  $\mathrm{Iso}^+(D) \simeq A_5$ et on conclut car $-1 \in \mathrm{Iso}(P)$.
- L'Icosaèdre Régulier I : On vérifie comme pour le cube que le dual de I est un dodécaèdre et que l'on a :

1. couples d'arêtes parallèles

Proposition 5.7

$\mathrm{Iso}(I) = \mathrm{Iso}(D)$.

En regardant l'action sur les faces opposées, on retrouve l'action sur les pentagones mystiques.

Théorème 5.2: Klein

Tout sous-groupe fini irréductible de $SO(3)$ est le groupe des isométries directes d'un solide de Platon, et donc isomorphe à A_4, S_4 ou A_5.

Lemme 5.1.2 (Burnside-Frobenius)**.** *Soit G fini agissant sur un ensemble fini X. On note r le nombre de G-orbites dans X et pour $g \in G$ on note $Fix(g)$ l'ensemble des points fixes de g dans X. On a alors :*

$$r = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Lemme 5.1.3. *Si $G \leq SO(3)$ est fini, soit $X \subset S^2$ l'ensemble des pôles*[2] *des éléments non triviaux de G, soient $x_1, \ldots, x_r$ des représentants des orbites de G dans X et $n_i = |G_{x_i}|$ triés dans l'ordre croissant. Alors, on a soit $r = 2$, $|X| = 2$ et $G = G_{x_1} = G_{x_2}$ soit $r = 3$ et $|G|$ et les n_i sont données par :*

$\lvert G\rvert$	n_1	n_2	n_3	$\lvert O_{x_1}\rvert$	$\lvert O_{x_2}\rvert$	$\lvert O_{x_3}\rvert$	$\lvert X\rvert$
$2m$	2	2	m	m	m	2	$2m+2$
12	2	3	3	6	4	4	14
24	2	3	4	12	8	6	26
60	2	3	5	30	20	12	60

5.2 Le Groupe $SP(1)$

5.2.1 L'algèbre des quaternions de Hamilton

Définition 5.6: Algèbre des Quaternions de Hamilton

On se place dans $\mathscr{M}_2\left(()\,\mathbb{C}\right)$ et considère :

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } K = IJ = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

On définit alors $\mathbb{H} = \mathrm{Vect}_{1,I,J,K}\left(\mathbb{R}\right) \subset \mathscr{M}_2\left(\mathbb{C}\right)$

On définit de plus :

$$t(q) = \mathrm{Tr}(q), n(q) = \det q \text{ et } q^\star = {}^{\mathsf{t}}\overline{q} = t(q)1 - q \in \mathbb{H}$$

Proposition 5.8: Corps Gauche

$\mathbb{H}$ est un corps gauche de centre $\mathbb{R}$.

Proposition 5.9: Caley-Hamilton

Par théorème de Cayley-Hamilton sur $\mathscr{M}_2\left(\mathbb{C}\right)$: $q^2 t(q) q + n(q)1 = 0$ ce qui ici vaut :

$$qq^\star = q^\star q = n(q)1$$

2. couples de points fixes

5.2.2 Le groupe $Sp(1)$

Définition 5.7: Groupe Spécial Projectif

On pose $Sp(1) = \{q \in \mathbb{H} \mid n(q) = 1\}$. C'est un sous-groupe de $\mathbb{H}^\times$

Remarque 5.2.0.1. *L'application :*

$$\begin{array}{ccc} \mathbb{R}^4 & \to & \mathbb{H} \\ (t, x, y, z) & \mapsto & t + xI + yJ + zK \end{array}$$

identifie la sphère unité euclidienne S^3 à $Sp(1)$, ce qui munit S^3 d'une loi de groupe non commutative par transfert de structure. On sait que S^1 et S^3 sont les deux seules sphères euclidiennes que l'on peut munir d'une loi de groupe topologique.

Remarque 5.2.0.2. *$Sp(1)$ s'identifie à* $\left\{ \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \mid |\alpha|^2 + |\beta|^2 = 1 \right\}$ *de $SL_2(\mathbb{C})$.*

Proposition 5.10: Décomposition Polaire

Par décomposition polaire : $\mathbb{H}^\times = \mathbb{R}_{>0} \times Sp(1)$

Proposition 5.11: Élément d'Ordre 2

L'élément -1 est l'unique élément d'ordre 2 de $Sp(1)$

Proposition 5.12: Éléments d'ordre fixés

Un élément $q \in Sp(1)$ est d'ordre $m > 2$ si et seulement si $t(q) = 2\cos(2k/m)$ avec $k \in \mathbb{Z}$ et $k \wedge m = 1$

5.2.3 L'espace euclidien $\mathbb{H}$

Définition 5.8: Espace Euclidien $\mathbb{H}$

On définit sur $\mathbb{H}$ un produit scalaire réel par $\langle() \, q, q^{'} \rangle = \frac{1}{2} t(q^\star q^{'})$

Proposition 5.13: Translations sur le Groupe SP

L'application $Sp(1) \times Sp(1) \to O(\mathbb{H})$ qui à $(q_1, q_2) \mapsto L_{q_1} R_{q_2}$ est un morphisme d'image $SO(\mathbb{H})$ et de noyau $\langle (-1, -1) \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ où L_q désigne la translation à gauche par q et R_q la translation à droite.

Proposition 5.14

L'application $Sp(1) \to SO(\mathbb{H}^0)$, $q \mapsto \mathrm{int}_{q_{|\mathbb{H}^0}}$ où $\mathbb{H}^0 = 1^\perp = \{q \in \mathbb{H} \mid t(q) = 0\}$.

5.3 Groupes Linéaires et Simplicité de $PSL_n(k)$

5.3.1 Transvections

Définition 5.9: Transvection

Soit V un k-espace vectoriel de dimension $n \geq 2$. Une transvection de V est un élément t de $SL(V)$ tel que $\dim \ker(t - \mathrm{id}_V) = n - 1$.

Proposition 5.15: Transvections Standards

Les transvections standards $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ sont des transvections de k^n d'hyperplan fixe $x_j = 0$. On fixe $t_n = T_{n,n-1}(1)$. Les transvections standards engendrent $SL_n(k)$.

Proposition 5.16: Conjugaison des Transvections

1. Un élément de $GL_n(k)$ est une transvection si et seulement il est conjugué à t_n.
2. Si $n > 2$, les transvections sont conjuguées dans $SL_n(k)$

5.3.2 Centre et Groupe Dérivé de $SL_n(k)$

Proposition 5.17: Homothétie et Centre

Pour $g \in GL_n(k)$, il y a équivalence entre :

1. g commute avec tous les éléments de $SL_n(k)$
2. g préserve toutes les droites de k^n
3. g est une homothétie

Corollaire 5.2: Centre

Le centre de $GL_n(k)$ est $k^\times$ et celui de $SL_n(k)$ est $\mu_n(k)$.

Proposition 5.18: Groupes Dérivés

Pour $n \neq 2$ ou $|k| > 3$, on a :

$$D(GL_n(k)) = SL_n(k) \text{ et } D(SL_n(k)) = SL_n(k)$$

5.3.3 Le critère de Simplicité d'Iwasawa

Proposition 5.19: Critère de Simplicité d'Iwasawa

Soit G agissant 2-transitivement sur X. On suppose qu'il existe $x \in X$ et $A \subset G_x$ avec :

1. A un sous-groupe abélien distingué de G_x
2. $\cup_g gAg^{-1}$ engendre G

Si N est un sous-groupe distingué de G, alors soit N contient $D(G)$ soit N est inclus dans le noyau de l'action de G sur X.

5.3.4 Groupes Linéaires sur les Corps Finis

Lemme 5.3.1. *Soit k un corps fini de cardinal q. Alors,*

$$|GL_n(k)| = \prod_{i=0}^{n-1} \left(q^n - q^i\right) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} q^{i-1}$$

Corollaire 5.3

$$|SL_n(k)| = \frac{|GL_n(k)|}{q-1}$$

Corollaire 5.4

$\mu_n(k)$ est cyclique d'ordre $n \wedge q - 1$ et donc : $|PSL_n(k)| = \frac{|SL_n(k)|}{n\wedge(q-1)}$

Définition 5.10: Groupe Projectif Linéaire

On pose $PGL_n(k) = GL_n(k)/k^\times I_n$. Ce groupe agit fidèlement sur $P^{n-1}(k) = \{$ droites de $k^n\}$.

5.4 Le groupe $PGL_2(k)$ et quelques (iso)morphismes miraculeux

Définition 5.11: Droite Projective

On appelle $\hat{P}(k)$ l'ensemble des droites de k^2. On définit $\hat{k} = k \sqcup \{\infty\}$. On définit :

$$\beta : \begin{cases} \hat{k} & \longrightarrow & \hat{P}(k) \\ x \in k & \longmapsto & k\begin{pmatrix} x \\ 1 \end{pmatrix} \\ \infty & \longmapsto & k\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{cases}$$

Proposition 5.20: Droite et Droites Projectives

β est une bijection. Si on se donne une matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $GL_2(k)$ envoie le point $x \in \hat{k}$ sur :

$$g.x = \beta^{-1}(g\beta(x)) = \frac{ax+b}{cx+d} \in \hat{k}$$

Définition 5.12: Homographies

Les bijections de $\hat{k}$ de la forme $x \mapsto \frac{ax+b}{cx+d}$ sont appelées homographies. Elles forment un sous-groupe de $S_{\hat{k}}$ isomorphe à $PGL_2(k)$.

Proposition 5.21: Droite Projective et Plan

Pour tout triplet (α, β, γ). Il existe une et une seule homographie $g \in PGL_2(k)$ telle que $(g(\alpha), g(\beta), g(\gamma)) = (0, 1, \infty)$

Exemple 5.4.1. *L'ensemble $\hat{\mathbb{C}}$ peut être vu comme la sphère de Riemann. $GL_2(\mathbb{R}) \subseteq GL_2(\mathbb{C})$ agit sur $\hat{\mathbb{C}}$ par restriction en préservant $\hat{\mathbb{R}}$ donc aussi $\mathbb{C} \setminus \mathbb{R}$ son complémentaire. Cet ouvert de $\mathbb{C}$ a deux composantes connexes, l'une d'elle étant le demi-plan de Poincaré $\mathbb{H} = \{\tau \in \mathbb{C} \mid \Im\tau > 0\}$. $\mathbb{H}$ est préservé par $SL_2(\mathbb{R})$.*

Proposition 5.22: Groupe Projectif et Groupe Symétrique

Pour p premier, l'action fidèle de $PGL_2(\mathbb{Z}/p\mathbb{Z})$ induit un morphisme injectif de dans S_{p+1}.

Corollaire 5.5: Miracle !

Comme $(p+1)! = (p+1)p(p-1)(p-2)!$, le morphisme de la proposition ci-dessus induit des isomorphismes $PGL_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ et $PGL_2(\mathbb{Z}/3\mathbb{Z}) \simeq S_4$. Les morphismes naturels :

$$PSL_2(\mathbb{Z}/2\mathbb{Z}) \leftarrow SL_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow GL_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow PGL_2(\mathbb{Z}/2\mathbb{Z})$$

De même, $PSL_2(\mathbb{Z}/3\mathbb{Z}) \simeq A_4$.

Proposition 5.23: Sous-Groupes d'Indices Finis de S_n

Tout sous-groupe d'indice 2 de S_n est isomorphe à A_n. Tout sous-groupe d'indice n de S_n est isomorphe à S_{n-1}.

Corollaire 5.6

$PGL_2(\mathbb{Z}/5\mathbb{Z}) \simeq S_5$ et $A_n \simeq PSL_2(\mathbb{Z}/p\mathbb{Z})$ si et seulement si $n = p = 5$.

Remarque 5.4.0.1. *Parmi les groupes simples de la forme A_n et $PSL_n(\mathbb{Z}/p\mathbb{Z})$ on a seulement :*

$$A_5 \simeq PSL_2(\mathbb{Z}/5\mathbb{Z}),\ PSL_2(\mathbb{Z}/7\mathbb{Z}) \simeq PSL_3(\mathbb{Z}/2\mathbb{Z}) \text{ et } PSL_4(\mathbb{Z}/2\mathbb{Z}) \simeq A_8$$

Pour des corps plus généraux :

$$A_5 \simeq PSL_2(\mathbb{F}_4),\ A_6 \simeq PSL_2(\mathbb{F}_9)$$

Théorème 5.3: Galois

$PSL_2(\mathbb{Z}/p\mathbb{Z})$ agit transitivement sur un ensemble à p éléments si et seulement si $p \leq 11$.

6 Elements de structures des groupes finis

6.1 p-groupes

On fixe $p \in \mathcal{P}$

Définition 6.1: p-Groupe

Un p-groupe est un groupe fini d'ordre $p^n, n \geq 0$.

Proposition 6.1: Sous-Groupes d'un p-Groupe

Un sous-groupe d'un p-groupe est un p-groupe. Un produit fini de p-groupes est un p-groupe. Un p-sous-groupe d'un groupe G est un sous-groupe de G qui est un p-groupe. Si G est fini quelconque, $p \mid |G|$, les p-Sylow de G sont des p-sous-groupes.

Définition 6.2: Groupe Unipotent Supérieur

Le sous-groupe unipotent supérieur $U_n(\mathbb{Z}/p\mathbb{Z})$ des matrices triangulaires supérieures de diagonale égale à 1 est d'ordre $p^{\frac{n(n-1)}{2}}$.

Proposition 6.2: Action d'un p-groupe

Soit P un p-groupe agissant sur un ensemble fini X. On note $FixX = \{x \in X \mid gx = x \forall g\}$. Alors, $|X| \equiv |FixX| \mod p$.

Proposition 6.3: p-Groupe Linéaires

Pour tout p-groupe $P \subset GL_n(\mathbb{Z}/p\mathbb{Z})$, il existe $g \in GL_n(\mathbb{Z}/p\mathbb{Z})$ tel que gPg^{-1} est inclus dans $U_n(\mathbb{Z}/p\mathbb{Z})$.

Corollaire 6.1

Tout p-groupe fini est isomorphe à un sous-groupe de $U_n(\mathbb{Z}/p\mathbb{Z})$ pour n assez grand.

Proposition 6.4: Centre d'un p-Groupe

Si P est un p-groupe non trivial, son centre est non trivial.

Corollaire 6.2

Un groupe d'ordre p^2 est abélien, donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou $\mathbb{Z}/p^2\mathbb{Z}$.

Remarque 6.1.0.1. *Il existe des groupes d'ordre p^3 non-abéliens, comme le p-groupe $U_3(\mathbb{Z}/p\mathbb{Z})$ appelé Groupe de Heisenberg.*

Corollaire 6.3: Résolubilité

Les p-groupes sont résolubles.

6.2 Les Théorèmes de Sylow

Rappel : Si $|G| = p^\alpha m$ avec $p \wedge m = 1$, un p-sylow de G est un p-sous-groupe de G de cardinal p^α.

Théorème 6.1: Sylow

Soient G un groupe fini et p premier divisant $|G|$:

1. G possède des p-Sylow.
2. Tout p-sous-groupe de G est inclus dans un p-Sylow de G.
3. Deux p-Sylow de G sont conjugués (en particulier, isomorphes.)

Lemme 6.2.1 (Alignement des p-Sylow)**.** *Soient G un groupe fini, $H \leq G$ et $p \mid |H|$ premier. Si P est un p-Sylow de G, il existe $g \in G$ tel que $gPg^{-1} \cap H$ est un p-Sylow de H.*

Définition 6.3: Nombre de p-Sylow

On notera $n_p(G)$ le nombre de p-Sylow de G et $Syl_p(G)$ l'ensemble des p-Sylow de G.

Corollaire 6.4

On a : $n_p(G) = 1 \Leftrightarrow G$ possède un p-Sylow distingué.

Théorème 6.2: 3ème Théorème de Sylow

oit G un groupe $fini$ de cardinal $p^\alpha m$. On a : $n_p(G) \mid m$ et $n_p(G) \equiv 1 \mod p$

Lemme 6.2.2 (Frattini)**.** *Soient G un groupe fini, $N \lhd G$, P un p-Sylow de N et $N_G(P)$ le normalisateur de P dans G. On a $G = NN_G(P)$.*

6.3 Le Théorème de Schur-Zassenhaus

Théorème 6.3: Schur-Zassenhaus

Soient G un groupe fini d'ordre mn avec $m \wedge n = 1$ et possédant $N \lhd G$ d'ordre n. Alors N admet un complément dans G (nécessairement d'ordre m).

Lemme 6.3.1. *Le cas particulier où N est abélien du théorème implique le cas général.*

6.4 Théorèmes de Hall

Théorème 6.4: P.Hall

Soit G un groupe fini résoluble. Si $|G| = mn, m \wedge n = 1$, alors G possède un sous groupe d'ordre m.

Théorème 6.5: P.Hall

Soit G un groupe fini d'ordre d. Si pour toute factorisation $d = mn$ avec $m \wedge n = 1$, G possède un sous-groupe d'ordre m, alors G est résoluble.

6.5 Extensions et Cohomologie

Si A et G sont fixés, on veut classifier les suites exactes courtes :

$$1 \to A \xrightarrow{i} \tilde{G} \xrightarrow{\pi} G \to 1 \tag{1}$$

Etant donné une telle sec est-ce que $i(A)$ admet un complément dans $\tilde{G}$?

Lemme 6.5.1. *Soit une extension comme ci-dessus. Il y a équivalence entre :*

1. *$i(A)$ admet un complément dans $\tilde{G}$*
2. *π admet une section ensembliste qui est un morphisme de groupes.*

Définition 6.4: S.E.C. Scindée

On dit que la suite exacte courte est scindée si les conditions équivalentes du lemme précédent sont satisfaites.

Théorème 6.6: Schur-Zassenhaus

Toute extension de G par A avec $|G| \wedge |A| = 1$ est scindée

Dans la suite, on suppose que A est abélien.

Définition 6.5: G-Module

Un G-module est la donnée d'un groupe abélien $(A, +)$ muni d'une action de G sur A vérifiant $g(a+b) = ga + gb$ ou, ce qui revient au même, telle que le morphisme $G \to S_A$ associé soit à valeurs dans $Aut(A)$.

Proposition 6.5: Extension et Module

La donnée de la suite exacte courte 1 munit le groupe abélien A d'une structure de G-module par :

$$g.a = i^{-1}\left(\tilde{g}i(a)\tilde{g}^{-1}\right)$$

où $\tilde{g} \in \tilde{G}$ est un relevé de g par π.

Exemple 6.5.1 (Extensions Centrales)**.** *Une extension 1 de G par A est dite* centrale *si $i(A) \subseteq Z(\tilde{G})$.*

On fixe une extension 1 de G par A, et on considère une section ensembliste $s : G \to \tilde{G}$. Il existe un unique élément $c(g, g^{'})$ dans A tel que :

$$s(g)s(g^{'}) = i(c(g, g^{'}))s(gg^{'})$$

On remarque qu'alors s est un morphisme si et seulement si $c = Ob(s)$ est nulle.

Lemme 6.5.2. *Soient s une section ensembliste de π et $c = Ob(s)$. On a :*

$$g.c(g^{'}g^{''}) - c(gg^{'}, g^{''}) + c(g, g^{'}g^{''}) - c(g, g^{'}) = 0, \ \forall g, g^{'}, g^{''} \in G$$

Définition 6.6: Cocycles

Si A est un G-module, on note $Z^2(G, A)$ l'ensemble des fonctions vérifiant l'identité du lemme précédent. Une telle fonction est appelée 2-cocycle de G à valeurs dans A.

Une autre section de π que s est de la forme $s_\varepsilon : g \mapsto i(\varepsilon(g))s(g)$ où ε est une fonction arbitraire de G dans A. Les deux 2-cocycles $c = Ob(s)$ et $c_\varepsilon = Ob(s_\varepsilon)$ sont alors liés par :

$$c_\varepsilon(g, g^{'}) = c(g, g^{'}) + g.\varepsilon(g^{'}) - \varepsilon(gg^{'}) + \varepsilon(g)$$

Définition 6.7: Cobords

Si A est un G-module, on note $B^2(G, A)$ l'ensemble des fonctions $\partial\varepsilon : G \times G \to A$ de la forme $g, g^{'} \mapsto g.\varepsilon(g^{'}) - \varepsilon(gg^{'}) + \varepsilon(g)$ avec $\varepsilon : G \to A$. Une telle fonction f est appelée 2-cobord de G à valeurs dans A.

Définition 6.8: Groupe de Cohomologie

Pour tout G-module A, le groupe $B^2(G, A)$ est un sous-groupe de $Z^2(G, A)$ et on définit le 2-ème groupe de cohomologie de G à valeurs dans A comme le groupe abélien quotient :

$$H^2(G, A) = Z^2(G, A)/B^2(G, A)$$

Proposition 6.6: Classes et Sections

Si s est une section de π, la classe de $Ob(s)$ ne dépend pas du choix de la section s. On la note $[E]$ et on l'appelle classe de cohomologie assoicée à 1. La sec 1 est scindée si, et seulement si sa classe $[E]$ est nulle.

Théorème 6.7: Schur-Zassenhaus, Cohomologique

Soient G un groupe et A un G-module :

1. Si G est fini, alors $|G|\, x = 0$ pour tout $x \in H^2(G, A)$
2. Si A est fini, alors $|A|\, x = 0$ pour tout $x \in H^2(G, A)$

En particulier, si G et A sont finis avec $|G| \wedge |A| = 1$, on a $H^2(G, A) = 0$.

Proposition 6.7

Pour tout G-module A et $x \in H^2(G, A)$, il existe une extension de G par A vérifiant $[E] = x$.

Proposition 6.8

Soient A un G-module et $E_k = \left(\tilde{G}_k, i_k, \pi_k\right)$ pour $k = 1, 2$ deux extensions de G par le même G-module A. On a $[E_1] = [E_2]$ si et seulement si il existe un isomorphisme $\varphi : \tilde{G}_1 \to \tilde{G}_2$ vérifiant $\varphi \circ i_1 = i_2$ et $\pi_2 \circ \varphi = \pi_1$

Corollaire 6.5

Soit A un G-module, l'application $(E) \mapsto [E]$ induit une bijection entre l'ensemble $\mathcal{E}(G, A)$ des classes d'isomorphisme d'extensions de G par le G-module A et l'ensemble $H^2(G, A)$.

Théorème 6.8: Schur

Considérons $\mathbb{Z}/2\mathbb{Z}$ comme A_n-module trivial. On a, pour $n \geq 4$:

$$H^2(A_{n,\mathbb{Z}/2\mathbb{Z}}) \simeq \mathbb{Z}/2\mathbb{Z}$$

7 Arithmétique des Anneaux

7.1 Les anneaux $\mathbb{Z}[\sqrt{d}]$

On fixe dans la suite un entier $d \in \mathbb{Z}$ non carré[3] dans $\mathbb{Z}$.

Définition 7.1

On définit, pour $z = x + y\sqrt{d}$:

$$\begin{cases} \bar{z} = x - y\sqrt{d} & \text{le conjugué de } z \\ T(z) = z + \bar{z} = 2x & \text{la trace de } z \\ N(z) = z\bar{z} = x^2 - dy^2 & \text{la norme de } z \end{cases}$$

On a donc : $z^2 - T(z)z + N(z) = 0$, c'est l'identité de Cayley-Hamilton

Lemme 7.1.1. *1. $z \mapsto \bar{z}$ est un automorphisme*

2. $\mathbb{Q}\left[\sqrt{(d)}\right]$ est le corps des fractions de $\mathbb{Z}[\sqrt{d}]$

3. $N : \mathbb{Q}[\sqrt{d}]^\times \mapsto \mathbb{Q}^\times$ est un morphisme de groupes et $N\left(\mathbb{Z}\left[\sqrt{d}\right]\right) \subseteq \mathbb{Z}$.

Lemme 7.1.2. *On a $\mathbb{Z}\left[\sqrt{d}\right]^\times = \left\{z \in \mathbb{Z}\left[\sqrt{d}\right] \mid N(z) = \pm 1\right\}$*

Corollaire 7.1

On a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbb{Z}\left[\sqrt{d}\right]^\times = \{\pm 1\}$ pour $d < -1$.

Remarque 7.1.2.1. *On appelle équation de Pell-Fermat l'équation $x^2 - dy^2 = 1$ pour $d > 0$.*

3. z négatif convient

Proposition 7.1: Base Algébrique

Soit $d > 0$ non carré. Tout élément > 1 de $\mathbb{Z}\left[\sqrt{d}\right]^\times$ est de la forme $x+y\sqrt{d}$ avec $x, y \in \mathbb{Z}_{\geq 1}$. De plus il existe un plus petit tel élément η_d appelé unité fondamentale de $\mathbb{Z}\left[\sqrt{d}\right]$, et on a $\mathbb{Z}\left[\sqrt{d}\right]^\times = \langle -1, \eta_d\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

7.2 Divisibilité

Définition 7.2: Unités et Diviseurs

Pour un anneau A commutatif intègre, si $a, b \in A$, on a $a \mid b$ s'il existe $c \in A$ tel que $b = ac$. Les diviseurs de 1 sont appelés les unités de A.

Définition 7.3: Nombres Associés

On dit que $a, b \in A$ sont associés noté $a \sim b$ si $b \mid a$ et $a \mid b$.

Lemme 7.2.1. *Pour $a, b \in A$, $a \sim b \Leftrightarrow \exists u \in A^\times, a = bu$*

Définition 7.4: Irréductibilité

Un élément non nul $\pi \in A$ est dit irréductible si ce n'est pas une unité et si pour tout $a, b \in A$, $\pi = ab$ implique $a \in A^\times$ ou $b \in A^\times$.

Définition 7.5: Nombre Premier

Un élément non nul $\pi \in A$ est dit premier si ce n'est pas une unité et s'il satisfait la propriété d'Euclide-Gauss :

$$\forall a, b \in A, \pi \mid ab \implies \pi \mid a \text{ ou } \pi \mid b$$

7.3 Anneaux Factoriels

Définition 7.6

On convient qu'un produit vide dans un anneau vaut 1 et aussi que l'on a $a^0 = 1$ pour tout $a \in A$. On choisit un ensemble arbitraire $\mathcal{P}$ de représentants des éléments irréductibles pour la relation d'association.

Définition 7.7: Factorisation et Anneaux Factoriels

1. On dit que A a la *propriété de factorisation* (**PF**) si tout élément de $A \setminus \{0\}$ est un produit fini d'éléments irréductibles et d'une unité.
2. On dit que A est *factoriel* si pour tout $a \in A \setminus \{0\}$, il existe un unique $u \in A^\times$ et une unique fonction $(\nu_\pi(a)) \in \mathbb{N}^{(\mathcal{P})}$

Exemple 7.3.1.
1. *$\mathbb{Z}$ et $\mathbb{K}[X]$ sont factoriels*
2. *Les $\mathbb{Z}\left[\sqrt{d}\right]$ sont* ***(PF)***
3. *L'anneau $H(\mathbb{C})$ des séries entières convergentes sur $\mathbb{C}$ est intègre par le principe des zéros isolés. On peut montrer que les unités de $H(\mathbb{C})$ sont exactement les fonctions qui ne s'annulent pas sur $\mathbb{C}$ et ses irréductibles sont les associés des $z - a, a \in \mathbb{C}$. Mais certains éléments de $H(\mathbb{C})$ comme $\sin(\pi z)$ ont une infinité de zéros donc l'anneau $H(\mathbb{C})$ ne vérifie pas (**PF**).*

Proposition 7.2: Anneau Factoriel et PF

Supposons que A satisfait **(PF)**. Alors, A est factoriel si et seulement si tout irréductible de A est premier.

Lemme 7.3.1. *Les pgcd et ppcm existent dans un anneau factoriel.*

7.4 Idéaux

Définition 7.8: Idéal

Un idéal de A est un sous-groupe additif stable par produit gauche.

Lemme 7.4.1. *Soit* $f : A \to B$

1. $\ker f$ *est un idéal de* A.
2. *Si* I *est un idéal de* B *alors* $f^{-1}(I)$ *est un idéal de* A.
3. *Si* f *est surjective et si* I *est un idéal de* A*, alors* $f(I)$ *est un idéal de* B.

Définition 7.9: Anneau Noethérien

Un anneau est dit *noethérien* si ses idéaux sont de type fini, i.e. finiment engendrés.

Proposition 7.3: Anneaux Noethériens et Suites d'Idéaux

Soit A un anneau commutatif. Il y a équivalence entre :

1. A est noethérien
2. toute suite croissante d'idéaux est stationnaire.
3. toute famille non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Proposition 7.4: Anneaux Intègres Noethériens

Si A est intègre noethérien alors A vérifie PF.

7.5 Anneaux euclidiens et principaux

Définition 7.10: Anneau Euclidien

Un anneau commutatif A est di *euclidien* s'il possède une fonction $\varphi : A \setminus \{0\} \to \mathbb{N}$ telle que $\forall a, b \in A \setminus \{0\}$, il existe q et $r \in A$ tels que $a = bq + r$ avec :

1. soit $r = 0$
2. soit $r \neq 0$ et $phi(r) < \varphi(b)$

Proposition 7.5: Entiers Algébriques et Euclidianité

Pour $d = -2, -1, 2$ l'anneau $\mathbb{Z}\left[\sqrt{d}\right]$ est euclidien pour $|N|$.

Définition 7.11: Anneau Principal

Un anneau principal est un anneau intègre dont tous les idéaux sont principaux.

Proposition 7.6: Anneau Intègre Euclidien

Un anneau intègre euclidien est principal.

Proposition 7.7: Théorème de Bézout

Soient A un anneau principal et $a, b \in A$. Alors, a et b admettent un pgcd d dans A et il existe $u, v \in A$ tels que $au + bv = d$.

Théorème 7.1: Anneau Principal

Un anneau principal est un anneau factoriel.

Corollaire 7.2

Les anneaux $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{-2}]$ ainsi que $k[X]$ quand k est un corps sont principaux, et donc, factoriels.

7.6 L'anneau $\mathbb{Z}[i]$ et sommes de deux carrés

Théorème 7.2: Nombres Irréductibles dans $\mathbb{Z}[i]$

Tout irréductible de $\mathbb{Z}[i]$ divise un et un seul nombre premier $p \in \mathbb{Z}$ usuel. De plus, pour un tel p, on est dans un et un seul des cas suivants :

1. $p = 2$ et on a $2 = -(i+1)^2$ avec $1 + i$ irréductible, de norme 2.
2. $p \equiv 3 \mod 4$ et p est irréductible dans $\mathbb{Z}[i]$ de norme p^2.
3. $p \equiv 1 \mod 4$ et on a $p = \pi\bar{pi}$ des irréductibles de $\mathbb{Z}[i]$ non associés.

Lemme 7.6.1. *Soient $d \in \mathbb{Z}$ non carré, et $p \in \mathbb{Z}$ premier. Les diviseurs de p dans $\mathbb{Z}[\sqrt{d}]$ qui ne sont ni des unités ni associés à p, sont les éléments de $\mathbb{Z}[\sqrt{d}]$ de nomre $\pm p$. Ils sont nécessairement irréductibles.*

Proposition 7.8: Somme de Deux Carrés

Tout nombre premier $p \equiv 1 \mod 4$ s'écrit de manière unique sous la forme $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$.

8 Modules sur les Anneaux Principaux

8.1 Modules sur un Anneau

Définition 8.1: A-Module

Soit A un anneau. Un A-module est la donnée d'un groupe abélien $(M, +)$ et d'une application $A \times M \to M$ telle que pour tout $a, a^{'} \in A, m, m^{'} \in M$:

1. $a.(m + m^{'}) = a.m + a.m^{'}$
2. $(a + a^{'}).m = a.m + a^{'}.m$
3. $a.(a^{'}.m) = (a.a^{'})m$
4. $1.m = m$

Proposition 8.1: Module et Endomorphismes

Soient A un anneau et M un groupe abélien. Il est équivalent de se donner une structure de A-module sur M et un morphisme d'anneaux $A \to \mathrm{End}_{\mathbb{Z}}(M)$.

Définition 8.2: Sous-Module

Soient A un anneau et M un A-module. Un sous-module de M est un sous-groupe $N \subseteq M$ tel que $an \in N$ pour tout $a \in A, n \in N$.

Définition 8.3: Application Linéaire

Soient M et N des A-modules. Un morphisme de M vers N aussi appelé application A-linéaire est une application $f : M \to N$ telle que $f(m + m^{'}) = f(m) + f(m^{'})$ et $f(am) = af(m)$.

Définition 8.4: Module Monogène

Un A-module M est dit monogène si on a $M = Am$ pour un certain m.

Définition 8.5: Module de Type Fini

Un A-module est de type fini s'il possède une famille fini génératrice. Un A-module est dit libre de rang n s'il possède une base à n éléments.

Théorème 8.1: Isomorphisme de Modules des Puissances

Supposons A commutatif non nul. Les A-modules A^n et A^m sont isomorphes si et seulement si on a $n = m$. En particulier, toutes les bases d'un A-module libre de rang fini ont même cardinal.

8.2 Classes d'équivalence de matrices sur un anneau principal

Dans la suite, A est un anneau commutatif et $n \geq 1$ un entier.

Définition 8.6: Groupe Linéaire d'un Anneau

On définit $GL_n(A) = M_n(A)^\times$ et

$$\begin{array}{rccl} \det : & M_n(A) & \to & A \\ & (m_{i,j}) & \mapsto & \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} m_{\sigma(j),j} \end{array}$$

Lemme 8.2.1. *Pour tout anneau commutatif A et tout $M, N \in M_n(A)$ on a :*

$$\det MN = \det M \det N \text{ et } M{}^{t}Co(M) = {}^{t}Co(M)M = \det M I_n$$

Proposition 8.2: Caractérisation par le Déterminant

Pour tout anneau commutatif A on a :

$$GL_n(A) = \left\{ M \in M_n(A) \mid \det M \in A^\times \right\}$$

Théorème 8.2: Forme Normale de Smith

Soient A un anneau principal, et $M \in M_{p,q}(A)$ avec $p, q \geq 1$ et $r = \min(p, q)$. Il existe $P \in GL_p(A), Q \in GL_q(A)$ et $a_1, \ldots, a_r \in A$ avec $a_1 \mid \cdots \mid a_r$ et

$$PMQ = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_r \end{pmatrix}$$

On appelle les éléments a_i non nuls, uniques modulo $A^\times$, les facteurs invariants de la matrice M.

Définition 8.7: Groupe Spécial Linéaire

On note $SL_n(A)$ le noyau du morphisme det. C'est un sous-groupe distingué de $GL_n(A)$.

Définition 8.8: Contenu d'ordre

Soit $M \in M_{p,q}(A)$ et $k \in \mathbb{Z}$. Le contenu d'ordre de k de M est l'idéal $c_k(M)$ de A engendré par les mineurs de taille k de M avec les conventions $c_k(M) = A$ pour $k \leq 0$ et $c_k(M) = \{0\}$.

Lemme 8.2.2. *Soient A un anneau commutatif ainsi que $M, N \in M_{p,q}(A)$ deux matrices équivalentes. Pour tout $k \in \mathbb{Z}$ on a $c_k(M) = c_k(N)$*

8.3 Modules de type fini sur un anneau principal

Théorème 8.3: Matrice d'une Application Linéaire

Soient E et F des A-modules et $u : E \to F$ une application A-linéaire. On suppose A principal, E et F libres sur A de rangs respectifs q et p. On pose $r = \min p, q$. Alors, il existe une base $e = (e_1, \ldots, e_q)$ de E et une $f = (f_1, \ldots, f_p)$ de F et des éléments $a_1, \ldots, a_r$ de A avec $a_1 \mid \ldots \mid a_r$ vérifiant :

$$u(f_i) = a_i e_i \text{ pour } i \leq r \text{ et } u(f_i) = 0 \text{ pour } i > r$$

Théorème 8.4: Bases d'un Module

Soient A un anneau principal, M un A-module libre de rang fini m et N un sous-module de M. Il existe une base $e_1, \ldots, e_m$ de M, un entier $0 \leq p \leq m$ et des élements $a_1, \ldots, a_p \in A$ non nuls tels que :

- $a_1 e_1, \ldots, a_p e_p$ est une base de N.
- $a_1 \mid \ldots \mid a_p$

En particulier, N est libre sur A de rang $p \leq n$.

Théorème 8.5: Décomposition en Somme de Sous-Modules

Soient A un anneau principal et M un A-module de type fini. Il existe un unique entier $r \geq 0$ appelé rang de M, un unique entier $n \geq 0$ et des éléments non nuls $a_1, \ldots, a_n \in A$ uniques modulo association avec :

$$M \simeq A^r \bigoplus A/a_1A \bigoplus \cdots \bigoplus A/a_nA, a_1 \mid \cdots \mid a_n \text{ et } a_1 \notin A^\times$$

Théorème 8.6: Invariants de Similitude

Soient k un corps et V un k-ev de dimension finie :

1. Pour tout endomorphisme u de V, il existe un unique entier $s \leq \dim V$ et une unique suite de polynômes $P_1, \dots, P_s \in k[X]$ unitaires de degré ≥ 1 avec $P_1 \mid \cdots \mid P_s$ tels que dans une base e convenable de V on ait :

$$Mat_e(u) = \begin{pmatrix} C(P1) & & \\ & \ddots & \\ & & C(P_s) \end{pmatrix}$$

   On appelle ces polynômes les invariants de similitude de u.

2. Deux endomorphismes sont conjugués si et seulement si ils ont même invariants de similitudes.

9 Représentations Linéaires des Groupes Finis

9.1 Représentations Linéaires

Définition 9.1: Représentation Linéaire

Une représentation k-linéaire de G est la donnée d'un k-espace vectoriel V et d'un morphisme $\rho : G \to GL(V)$.
La dimension ou le degré de V, ρ est la dimension de V. Il est équivalent de se donner une représentation de G sur V et une action de G sur V telle que L_g est k-linéaire.

Définition 9.2: Isomorphisme de Représentations

Deux représentations k-linéaires de G de même dimension sont isomorphes ou équivalentes s'il existe des bases e_1 et e_2 de V_1 et V_2 telles que $\rho_1^{e_1} = \rho_2^{e_2}$ où ρ^e est l'application qui à $g \in G$ associe la matrice dans la base e de $\rho(g)$.

Définition 9.3: Représentation d'une Action

Si G agit sur X, la représentation ci-dessus de G sur kX est appelée représentation de permutation associée. Dans la base (e_x) de kX, la matrice de chaque $\rho(g)$ a un unique coefficient non nul égal à 1 sur chaque colonne et sur chaque ligne.

9.2 Le point de vue $k[G]$-modules

Définition 9.4: k-Algèbre

Une k-algèbre est un k-espace vectoriel muni d'une loi de composition μ k-bilinéaire qui fait de $A, +, \mu$ un anneau. Un morphisme de k-algèbres est un morphisme d'anneaux k-linéaire.

On construit une k-algèbre sur le k-ev kG en la munissant de μ qui dans la base des e_g est donnée par $e_g e_h = e_{gh}$.

Définition 9.5: k-Algèbre d'Espace Sous-Jacent

Soient k un corps et G un groupe. La k-algèbre d'espace sous-jacent kG s'appelle l'algèbre du groupe G à coefficients dans k et est notée $k[G]$. Sa dimension comme k-ev est $|G|$.

Proposition 9.1: Représentation et $k[G]$-Modules

Il est équivalent de se donner une représentation k-linéaire de G et un $k[G]$ module :

1. Si V est un $k[G]$-module, il existe une unique représentation k-linéaire de G sur le k-ev sous-jacent à V notée ρ_V et telle que $\rho_V(g)(v) = g.v$. On l'appelle représentation associée à V.
2. Si V, ρ est une représentation k-linéaire de G, il existe une unique structure de $k[G]$-module sur V étendant celle de k-espace vectoriel et vérifiant $g.v = \rho(g)(v)$. On l'appelle $k[G]$-module associé à V, ρ, et on le note en général simplement V.

Définition 9.6: Homomorphismes de Modules

Si V_1, V_2 sont des $k[G]$-modules, on note $Hom_{k[G]}(V_1, V_2)$ le k-ev des applications $k[G]$-linéaires de V_1 vers V_2.

Proposition 9.2: Isomorphismes de $k[G]$ modules et Représentations

Deux $k[G]$ modules U et V de dimension finie sont isomorphes si et seulement si les représentations associées le sont.

9.3 Décomposition en Irréductibles

Définition 9.7: Espace Invariant

Soit V un $k[G]$-module. Un sous-k-ev $W \subseteq V$ est dit G-invariant si on a $g.w \in W$ pour tout $w \in W, g \in G$, i.e. si c'est un sous-module de V. Soient $e = (e_1, \dots, e_{p+q})$ où $e_1, \dots, e_p$ est une base de W. Alors W est G-invariant si et seulement si :

$$\mathrm{Mat}_e\, \rho_V(g) = \left[\begin{pmatrix} \star_p & \star \\ 0 & \star_q \end{pmatrix}\right], \forall g \in G$$

Définition 9.8: Irréductibilité

Soit V un $k[G]$-module. On dit que V est irréductible (ou simple) si on a $V \neq 0$ et si les seuls sous-modules de V sont $\{0\}$ et V.

Proposition 9.3: Dimension des Irréductibles

Si k est algébriquement clos, G abélien et V un $k[G]$-module irréductible de dimension finie. Alors V est de dimension 1.

Proposition 9.4: Caractérisation de l'Irréductibilité

Un $k[G]$-module V non nul est irréductible si et seulement si $k[G]v = V$ pour tout $v \neq 0$ dans V.

Proposition 9.5: Dimension maximale des Irréductibles

Tout $k[G]$-module irréductible est de dimension $\leq |G|$.

Proposition 9.6: Sous-Modules de la Représentation de Permutation

Les seuls sous-modules de la représentation de permutation naturelle de S_n sur k^n sont $\{0\}, \mathrm{Vect}(1,1,\ldots,1), H = \{\sum_i x_i = 0\}, V$. En outre on a :

$$V = H \oplus D \Longleftrightarrow n \in k^\times$$

Définition 9.9: Module Semi-Simple

Un $k[G]$-module V est semi-simple s'il se décompose en somme directe de sous-modules irréductibles.

Proposition 9.7: Semi-Simplicité en Dimension Finie

Soit V un $k[G]$-module de dimension finie. Il y a équivalence entre :

1. V est semi-simple
2. V est somme de sous-modules irréductibles
3. Pour tout sous-module W de V, il existe une sous-module S de V vérifiant $V = W \oplus S$.
4. Tout sous-module de V est semi-simple.

Théorème 9.1: Groupe de Cardinal Inversible

On suppose G fini et $|G|$ dans $k^\times$. Alors tout $k[G]$-module de dimension finie est semi-simple.

Lemme 9.3.1. *Soient U et V deux $k[G]$-modules irréductibles.*

1. *Toute application $k[G]$-linéaire de U dans V est soit nulle soit un isomorphisme.*
2. *Si de plus k est algébriquement clos, et si U est de dimension finie, les applications $k[G]$-linéaires $U \to U$ sont les homothéties.*

Proposition 9.8: Décomposition en Modules Irréductibles

Soit V un $k[G]$-module semi-simple de dimension finie. On suppose donnée une décomposition $V = \bigoplus_{i \in I} V_i$ et pour tout i un $k[G]$-module irréductible de dimension finie S_i tels que :

1. $V_i \subseteq V$ est un sous-module isomorphe à $S_i^{\oplus n_i}$
2. $S_i \not\simeq S_{i'}$ si $i \neq i'$.

Alors, pour tout sous-module irréductible S de V, il existe un unique $i \in I$ tel que $S \simeq S_i$ et on a $S \subseteq V_i$.

9.4 Théorie des Caractères

Théorème 9.2: Classes de Conjugaison et Modules Irréductibles

Soit h le nombre de classes de conjugaison du groupe fini G.

1. A isomorphisme près, il existe h $\mathbb{C}[G]$-modules irréductibles.
2. Leurs dimensions n_i vérifient : $\sum_i n_i^2 = |G|$.

Définition 9.10: Caractère d'un Module

Soient V un $\mathbb{C}[G]-module$ de dimension finie et $\rho : G \to GL(V)$ le morphisme associé. Le caractère de V est la fonction $G \to \mathbb{C}$, $g \mapsto \mathrm{Tr}(\rho(g))$. On le note χ_V. En particulier $\chi_V(1) = \dim V$.

Définition 9.11: Fonctions Centrales

Une fonction est dite centrale si elle est constante sur les classes de conjugaison de G.

Proposition 9.9: Centralité des Caractères

Pour tout $\mathbb{C}[G]$-module V de dimension finie, χ_V est centrale sur G. De plus si $U \simeq V$, on a $\chi_U = \chi_V$.

Proposition 9.10: Somme de Caractères

Soient U, V des $\mathbb{C}[G]$-modules de dimension finie et $W = U \oplus V$. On a $\chi_W = \chi_U + \chi_V$.

Définition 9.12: Homomorphismes de Modules et $k[G]$-Modules

L'espace $Hom_k(U, V)$ des applications k-linéaires est muni d'une structure naturelle de $k[G]$-module en posant :

$$(g.\varphi)(x) = g.\varphi(g^{-1}.x)$$

On note $\mathrm{Hom}(U, V)$ ce module. Dans le cas $V = k$ on pose aussi $U^\vee = Hom(U, k)$ et on parle de représentation duale ou contragrédiente de U.

Proposition 9.11: Caractères et Morphismes

Soient U, V des $\mathbb{C}[G]$-modules de dimension finie.

1. Pour $W = Hom(U, V)$ on a $\chi_W(g) = \chi_U(g^{-1})\chi_V(g)$
2. En particulier : $\chi_{U^\vee}(g) = \chi_U(g^{-1})$

Proposition 9.12: Diagonalisabilité et Caractères

Soit $g \in G$ d'ordre d et V un $\mathbb{C}[G]$ module de dimension n. Alors $\rho_V(g)$ est diagonalisable et $\chi_V(g)$ est somme de n racines d-èmes de l'unité. De plus, $\chi_{V^\vee} = \overline{\chi_V}$.

Corollaire 9.1

Si χ, χ' sont des caractères, il en va de même de $\chi + \chi', \chi\chi', \overline{\chi}$.

Définition 9.13: Action d'un Module sur un Sous-Espace

Si V est un $\mathbb{C}[G]$-module, on pose :

$$V^G = \{v \in V \mid \forall g \in G, g.v = v\}$$

C'est le plus grand sev de V sur lequel G agit trivialement.

Lemme 9.4.1. *Si V est un $\mathbb{C}[G]$-module de dimension finie :*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$$

De manière équivalente, sur $L^2(G)$ muni du produit hermitien :

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{f'(g)}$$

on a : $\dim V^G = \langle \chi_V, 1 \rangle$

Théorème 9.3: Orthonormalité des Caractères

Soient U, V deux $\mathbb{C}[G]$-modules irréductibles. On a :

$$\langle \chi_U, \chi_V \rangle = \begin{cases} 1 & \text{si } U \simeq V \\ 0 & \text{sinon} \end{cases}$$

Corollaire 9.2: Décomposition en Caractères

Soit U un $\mathbb{C}[G]$-module de dimension finie. On suppose : $U \simeq \bigoplus_{i=1}^{r} S_i^{\oplus n_i}$ où les S_i sont des $\mathbb{C}[G]$-modules irréductibles deux à deux non isomorphes et les n_i sont des entiers positifs. Alors on a : $n_i = \langle \chi_U, \chi_{S_i} \rangle$ pour tout i.

Corollaire 9.3: Equivalence Caractère Module

Si U et V sont des $\mathbb{C}[G]$-modules de dimension finie on a :

$$U \simeq V \iff \chi_U = \chi_V$$

Définition 9.14: Caractère d'un Groupe

Un caractère de G est une fonction $\chi : G \to \mathbb{C}$ de la forme $\chi = \chi_V$ pour un certain V $\mathbb{C}[G]$-module de dimension finie. La fonction χ détermine uniquement V à isomorphisme près. On dit que χ est irréductible si V l'est. On note $CarG$ l'ensemble des caractères de G et $IrrG \subseteq CarG$ le sous-ensemble des caractères irréductibles.

Corollaire 9.4: Caractères Irréductibles

Soit $\chi \in CarG$. On a $\chi \in IrrG \iff \langle \chi, \chi \rangle = 1$.

Corollaire 9.5: Nombre de Modules Irréductibles

Tout $\mathbb{C}[G]$ module irréductible S apparaît dans la décomposition en irréductibles de la représentation régulière $\mathbb{C}G$ et ce avec une multiplicité $\dim S$. En particulier il n'y a qu'un nombre fini de $\mathbb{C}[G]$-modules irréductibles à isomorphisme près et leurs dimensions n_i vérifient $\sum_i n_i^2 = |G|$.

Définition 9.15: Espace des Fonctions Centrales

On note $L^2(G)_{cent}$ le sev de $L^2(G)$ des fonctions centrales.

Lemme 9.4.2. *$L^2(G)_{cent}$ a pour base les fonctions caractéristiques des classes de conjugaison de G. En particulier, $\dim L^2(G)_{cent} = h$.*

Théorème 9.4: Orthonormalité des Caractères

Les caractères irréductibles forment une base orthonormée de $L^2(G)_{cent}$.

Lemme 9.4.3. *Soient $f : G \to \mathbb{C}$ et $z \sum_{g \in G} f(g)g \in \mathbb{C}[G]$. Alors $z \in Z(\mathbb{C}[G]) \iff f centrale$.*

Définition 9.16: Translation et Homothétie

Soit S un $\mathbb{C}[G]$-module et $z \in Z(\mathbb{C}[G])$. L'application $m_z : v \in S \mapsto z.v \in S$ est $\mathbb{C}[G]$-linéaire. Supposons S irréductible. Par Lemme de Schur, m_z est une homothétie de rapport $\lambda_S(z)$.

Lemme 9.4.4. *Soient $f : G \to \mathbb{C}$ et $z \sum_{g \in G} f(g)g \in \mathbb{C}[G]$ et S un $\mathbb{C}[G]$-module simple. On a : $\lambda(z)_S(z) = \frac{|G|}{\dim S} \langle f, \chi_{S^\vee} \rangle$*

9.5 Tables de Caractères

Définition 9.17: Table de Caractères

On fixe dans la suite un groupe fini G. On note $C_1, \ldots, C_h$ les classes de conjugaison de G. On choisit $g_j \in C_j$ pour tout j. On note $\chi_1, \ldots, \chi_h$ les caractères irréductibles de G. Au dessus de la première ligne on mettra les cardinaux des classes de conjugaison et encore au dessus celle des $|G| \,/\, |C_j|$:

$$
\begin{array}{c|ccccc}
 & \frac{|G|}{|C_1|} & \cdots & \frac{|G|}{|C_j|} & \cdots & \frac{|G|}{|C_h|} \\
 & |C_1| & \cdots & |C_j| & \cdots & |C_h| \\
 & g_1 & \cdots & g_j & \cdots & g_h \\
\hline
1 = \chi_1 & 1 & \cdots & 1 & \cdots & 1 \\
\vdots & & & \vdots & & \\
\chi_i & & & \chi_i(g_j) & \cdots & \chi_i(g_h) \\
\vdots & & & \vdots & & \\
\chi_h & & & & &
\end{array}
$$

On complète la table avec les relations d'orthogonalité suivantes :

$$\sum_{j=1}^{h} |C_j| \, \chi_a(g_j)\overline{\chi_b(g_j)} = |G| \, \delta_{a,b} \text{ et } \sum_{i=1}^{h} \chi_i(g_a)\overline{\chi_i(g_b)} = \frac{|G|}{|C_a|}\delta_{a,b}$$

On donne dans la suite quelques exemples :
Etant donné un groupe, on donne sa table des caractères.

Proposition 9.13: Tables pour un Groupe Abélien

Si G est abélien, les caractères irréductibles sont de dimension 1 et l'ensemble des classes de conjugaison est G. On donne ici les tables pour $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

$$
\begin{array}{c|cc}
 & 2 & 2 \\
 & 1 & 1 \\
 & 1 & \tau \\
\hline
1 & 1 & 1 \\
\eta & 1 & -1
\end{array}
\qquad\qquad
\begin{array}{c|ccc}
 & 1 & \tau & \tau^2 \\
\hline
1 & 1 & 1 & 1 \\
\eta & 1 & j & j^2 \\
\eta^2 & 1 & j^2 & j
\end{array}
$$

Proposition 9.14: Groupe Symétrique S_3

Pour S_3, il y a 3 classes de conjugaisons. Il y a donc 3 caractères irréductibles à trouver :

#cent	6	2	3
#conj	1	3	2
	1	$(1\,2)$	$(1\,2\,3)$
1	1	1	1
ε	1	-1	1
χ_3	2	0	-1

Proposition 9.15: Morphismes de S_3 dans $GL_n(\mathbb{C})$

Pour tout morphisme de groupe $\rho : S_3 \to GL_n(\mathbb{C})$, il existe un unique décomposition $n = a + b + 2c$ avec $a, b, c \in \mathbb{N}$, telle que, quitte à conjuguer par une matrice $P \in GL_n(\mathbb{C})$, on ait :

$$\rho((1\,2)) = \begin{bmatrix} 1_a & 0 & 0 & 0 \\ 0 & -1_b & 0 & 0 \\ 0 & 0 & -1_c & 1_c \\ 0 & 0 & 0 & 1_c \end{bmatrix} \text{ et } \rho((1\,2\,3)) = \begin{bmatrix} 1_a & 0 & 0 & 0 \\ 0 & -1_b & 0 & 0 \\ 0 & 0 & 0 & -1_c \\ 0 & 0 & 1_c & -1_c \end{bmatrix}$$

Proposition 9.16: Groupe Symétrique S_4

On considère maintenant $G = S_4$. Puisque la droite $D = \text{Vect}(1, \ldots, 1)$ est stable sous l'action de S_4, on a un caractère irréductible $\chi_H = \chi_{\mathbb{C}^4} - 1$ de degré 3.

# cent	24	4	8	3	4
# conj	1	6	3	8	6
	1	$(1\,2)$	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,2\,3\,4)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_H	3	1	-1	0	-1
$\varepsilon\chi_H$	3	-1	-1	0	1

Pour χ_3, on observe que $\chi_3((1\,2)(3\,4)) = id$ puisque sa trace est 2 et est une somme de racines de l'unité. Si on note $\rho : S_3 \to GL_2(\mathbb{C})$ et si $u : S_4 \to S_3$ est le morphisme surjectif, $\chi_3 = \rho \circ u$.
On en déduit par ailleurs que $\varepsilon\chi_H$ est la représentation des isométries directes du cube, et χ_H la représentation des isométries du tétraèdre.

Proposition 9.17: Groupe Alterné A_5

On considère désormais $G = A_5$. On note dans la suite :

$$\varphi = \frac{1+\sqrt{5}}{2} \text{ et } \varphi' = \frac{1-\sqrt{5}}{2}$$

# cent	60	4	3	5	5
# conj	1	15	20	12	12
	1	$(1\,2)(3\,4)$	$(1\,2\,3)$	$(1\,2\,3\,4\,5)$	$(1\,2\,3\,5\,4)$
1	1	1	1	1	1
χ_2	3	-1	0	φ	φ'
χ_3	3	-1	0	φ'	φ
χ_H	4	0	1	-1	-1
$\chi_{H'}$	5	1	-1	0	0

On retrouve χ_H comme précédemment.
$\chi_{H'}$ vient de l'action exotique sur les pentagones mystiques, qu'on peut voir comme action sur les parties de $[\![1,5]\!]$ à deux éléments. On peut aussi faire comme pour χ_H en prenant l'action exotique vue sur $\mathbb{C}^6$
On trouve les coefficients de χ_2, χ_3 par des produits scalaires de colonnes et de lignes. On peut voir ce caractère comme la représentation de A_5 via une numérotation des 5 repères d'un dodécaèdre régulier. On compose par une permutation de ses repères, et selon si elle est dans A_5 ou dans $S_5 \setminus A_5$, on a χ_2 ou χ_3.

9.6 Propriété d'intégralité des caractères

Définition 9.18: Entier Algébrique

Un entier algébrique est un nombre complexe annulé par un polynôme unitaire à coefficients entiers. On note $\overline{\mathbb{Z}} \subset \mathbb{C}$ l'ensemble des entiers algébriques. En particulier, un entier algébrique est un nombre algébrique.

Proposition 9.18: Entier Algébrique Rationnel

Un entier algébrique rationnel est dans $\mathbb{Z}$, i.e. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$

Proposition 9.19: Anneau des Entiers Algébriques

$\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.

Proposition 9.20: Algébricité Sans Torsion

Soit R un anneau de groupe additif abélien de type fini sans torsion. Alors, si $x \in R$, il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(x) = 0$.

Proposition 9.21: Intégralité des Caractères

Pour tout χ de G, et tout $g \in G$, $\chi(g) \in \overline{\mathbb{Z}}$.

Proposition 9.22: Irréductibilité et Conjugaison

Pour tout $\chi \in Irr(G)$, de dimension $n = \chi(1)$ et tout $g \in G$, on a :

$$\frac{1}{n} |Conj(g)| \chi(g) \in \overline{Z}$$

Théorème 9.5: Dimension des Modules Irréductibles

Soit V un $\mathbb{C}[G]$-module irréductible de dimension finie. Alors $\dim V \mid |G|$.