Fiche résumée du cours d'algèbre 1

1 Groupes

1.1 Généralités/Rappels

1.1.1 *Définition* ***(Groupe)***

Un groupe est un magma associatif unifère, dont tous les élements sont inversibles.

1.1.2 *Proposition*

Soit $(G,.)$ un groupe, et soit un sous-ensemble de G. Il existe un plus petit sous groupe H de G contenant E, on dit que H est le sous groupe engendré par E, noté $< E >$.

1.1.3 *Définition* ***(Morphisme de groupe)***

Un morphisme de groupe est une application qui respecte la structure de groupe. (En particulier, l'image de 1_G est $1_{G'}$

1.1.4 *Proposition*

Soit $f : G \to G'$ morphisme de groupe. Soit H un sous groupe de G, alors $f(H)$ est un sous groupe de G', et, si H' est un sous groupe de G', $f^{-1}(H')$ est un sous groupe de G. En particuler, $Im(f)$ et $Ker(f)$ sont des sous groupes de G' et G respectivement.

1.2 Sous groupes distingués et sous groupes quotients

1.2.1 *Proposition*

Soit G un groupe et H un sous groupe de G. Les relations $x \underset{d}{\sim} y \Leftrightarrow x^{-1}.y \in H$ et $x \underset{g}{\sim} y \Leftrightarrow x.y^{-1} \in H$ sont des relations d'équivalence. 'Reflexives, symétriques, et transitives).On note G/H et $H\backslash G$ les ensembles quotients formés par les classes d'équivalence. Leurs éléments sont respectivement les $a.H$ et $H.a$, $a \in G$.

1.2.2 *Corollaire* ***(Théorème de Lagrange)***

Soit G un groupe fini, H un sous groupe, alors, on a $|H|$ qui divise $|G|$. On a en fait $|G|=|H|.|G/H|$

Lemme : Soit G un groupe, E un ensemble et $\Pi : G \to E$ application surjective. Il existe au plus une loi de groupe sur E telle que Π soit un morphisme de groupe.

1.2.3 *Théorème* ***(sous groupe distingué)***

Soit G un groupe, H un sous groupe. On note $\begin{array}{ccccc} \Pi & : & G & \to & G/H \\ & & g & \mapsto & g.H \end{array}$ la surjection canonique.

Les propositions suivantes sont équivalentes :

i) Il existe une (unique) structure de groupe "naturel" sur G/H telle que Π soit un morphisme de groupe.

ii) $\forall g \in G$, on a $g.H.g^{-1} = H$

iii) $\forall g \in G$, on a $g.H. = H.g$, de sorte que $G/H = H\backslash G$

iv) Il existe un morphisme de groupe $\varphi : G \in G'$, où G' est un groupe quelconque, tel que $H = Ker(\varphi)$

On dit alors que H est **distingué** (ou normal, ou invariant) dans G, et que G/H est le groupe quotient du groupe H. Un groupe G est dit simple si ses seuls sous groupes distingués sont $\{1\}$ et$G$

1.2.4 *Théorème* ***(de factorisation)***

Soit $f : G \to G'$ un morphisme de groupes. Il existe un unique morphisme de groupe $\widetilde{f} : G/Ker(f) \to G'$, tel que $f = \widetilde{f} \circ \Pi$, où $\Pi : G \to G/Ker(f)$ est la surjection canonique. De plus, on a un isomorphisme de groupe induit par $\widetilde{f} : G/Ker(f) \to Im(f)$

1.2.5 *Définition* ***(Groupe caractéristique, groupe dérivé)***

Si H est stable par tout automorphisme de G, on dit que H est caractéristique. (En particulier, caractéristique $\Rightarrow$ Stable par tout automorphisme intérieur $\Leftrightarrow$ distingué)

Soit G un groupe et $(x, y) \in G^2$. On appelle commutateur de x et y l'élement $[x; y] = xyx^{-1}y^{-1}$. ($[x; y] = 1 \Leftrightarrow x$ et y commutent). le sous groupe de G engendré par les commutateurs est apellé sous groupe dérivé, noté $D(G)$.

1.2.6 *Proposition*

Le sous groupe $D(G)$ est caractéristique, donc distingué. Le groupe quotient $G/D(G)$ est abélien. De plus, pour tout sous groupe H distingué dans G $(H \triangleleft G)$, tel que G/H est abélien, on a$D(G) \subset H$ On dit que $G^{ab} = G/D(G)$ est l'abélianisé de G (ou le plus grand quotient abélien de G)

1.2.7 *Définition* ***(Chaine exacte, courte)***

Une suite $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 ... \to G_n \xrightarrow{f_n} G_{n+1}$ de morphismes de groupe est dite exacte si $\forall i \in \{1..n\}, Im(f_i) = Ker(f_{i+1})$

Une suite exacte est dite courte si elle est de la forme

$$1 \to H \xrightarrow{i} G \xrightarrow{\Pi} N \to 1$$

Dans cette situation, H est isomorphe à $i(H) \triangleleft G$, et N est isomorphe à G/H. On dit alors que G est une extension de N par H.

1.3 Groupes opérant sur un ensemble

1.3.1 *Définition* ***(Groupe opérant sur un ensemble)***

Soit G un groupe, et X un ensemble. On dit que G opère ou agit sur X si on a une application $\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g.x \end{array}$ telle que :

i) $\forall x \in X, 1_G.x = x$

ii) $\forall g,g' \in G, \forall x \in X, (g.g').x = g.(g'.x)$

De manière équivalente, une action $G \to X$ est la donnée d'un morphisme de groupe $\varphi : G \to (S(X), \circ)$, où $S(x)$ est le groupe des bijections $X \to X$, avec $\varphi(g) : x \mapsto g.x$.

1.3.2 *Définition* ***(Orbite, stabilisateur)***

Soit G un groupe opérant sur un ensemble X, soit $x \in X$, on définit l'orbite de x par $O(x) = \{g.x, g \in G\}$. Les orbites forment une partition de X. Lorsqu'il n'y en a qu'une seule, on dit que G agit **transitivement** sur X. Soit Ω l'ensemble des orbites de G dans X. Un système de représentants des orbites est la donnée, pour tout $\omega \in \Omega$ d'un élément de ω, $x_\omega \in \omega$.

On définit le stabilisateur de x (sous l'action de G) par :

$$stab_G(x) = \{g \in G \mid g.x = x\}$$

On remarque que $stab_G(x)$ est un sous groupe de G.

1.3.3 *Proposition*

Soit G un groupe qui agit sur X, $x \in X$. L'application $\begin{array}{ccc} G/stab_G(x) & \to & O(x) \\ g.stab_G(x) & \mapsto & g.x \end{array}$ est bien définie et est une bijection. En particulier, si G est fini, $|O(x)|=|G/stab_G(x)|$ divise $|G|$

1.3.4 *Définition* ***(Action fidèle, action libre)***

On dit que l'action de G est fidèle si le seul élément qui stabilise tous les x de X est 1_G, ie $\bigcap\limits_{x \in X} stab_G(x) = \{1_G\}$, ou encore $G \to S(X)$ injective.

On dit que l'action de G est libre si $\forall x \in X$, $stab_G(x) = \{1_G\}$.

1.3.5 *Proposition*

L'opération $G \to G$ par translation à gauche est libre. Si G est un groupe fini de cardinal n, on obtient un morphisme injectif $G \to S_n$. Donc, tout groupe fini d'ordre n est un sous groupe de S_n.

1.3.6 *Corollaire* ***(Equation aux classes)***

Soit G un groupe opérant sur un ensemble X. Si $R = \{x_\omega, \omega \in \Omega\}$ est un système de representants des orbites, et si X est de cardinal fini, alors :

$$|X| = \sum_{x \in R} |G/stab_G(x)|$$

1.4 Théorèmes de Sylow, p-groupes

1.4.1 *Définition* ***(p-groupes, p-Sylow)***

Soit p un nombre premier, on appelle p-groupe un groupe fini de cardinal p^k, $k \in \mathbb{N}$

Soit G un groupe fini de cardinal $|G| = p^\alpha.r$, avec p premier et $p \wedge r = 1$. Un p sous groupe de Sylow est un sous groupe de G d'ordre p^α.

1.4.2 *Proposition*

Soit G un p-groupe, de cardinal p^n, $n \geq 1$

i) le centre Z de G est non trivial

ii) Si G est de cardinal p ou p^2, alors G est abélien.

1.4.3 *Théorème* ***(1er théorème de Sylow)***

$\forall p$ premier divisant $|G|$, $\exists$ un p-sous groupe de G de Sylow dans G

1.4.4 *Lemme 1*

Soit G un groupe d'ordre n, alors G est isomorphe à un sous groupe de $GL_n(\frac{\mathbb{Z}}{n\mathbb{Z}})$

1.4.5 *Lemme 2*

Soit H un sous-groupe de G et S un p-Sylow de G. Il existe $a \in G$ tel que $a.S.a^{-1} \cap H$ est un p-Sylow de H. Le théorème 1 en est une conséquence.

1.4.6 *Théorème* ***(2nd théorème de Sylow)***

Soit G un groupe fini de cardinal $|G| = p^\alpha.m$, avec $m \wedge p = 1$.

i) Si $H \subset G$ est un p-sous groupe, il existe un p-Sylow de G qui contient H

ii) Les p-sylow de G sont conjugués.

iii) Soit k le nombre de p-Sylow, alors $k \mid m$ et $k \equiv 1\,[p]$

1.5 Produit semi-direct de groupes

1.5.1 *Proposition/Def* ***(Produit semi direct de groupes)***

Soient H et N deux groupes tels que N agit dans H. On a donc un morphisme de groupes $\varphi : N \to Aut(H)$, où $n.h = \varphi(n)(h)$. On peut définir dans cette situation une loi de groupe sur le produit $H \times N$ par

$$(h, n) \times (h', n') = (h(n.h'), nn') = (h\varphi(n)(h'), nn')$$

Ce groupe est le **produit semi direct** de H par N relativement à φ. On le note $H \rtimes_\varphi N$, ou $H \rtimes N$.

1.5.2 *Proposition*

On suppose que N agit dans H par automorphisme, et on pose $G = H \rtimes N$.

i) On a une suite exacte courte de la forme :

$$(*) : 1 \to H \xrightarrow{i} G \xrightarrow{\Pi} N \to 1$$

avec $i(h) = (1, h)$ et $\Pi(h, n) = n$. i est un isomorphisme de H vers le sous groupe distingué $\underline{H} = i(H)$

ii) La suite exacte $(*)$ est **scindée** : il existe un morphisme de groupes$S : N \to G$ tel que $\Pi \circ S = Id_N$. On dit que S est une section de Π. Le morphisme S est injectif et définit un isomorphisme de N vers le sous groupe $\underline{N} = S(N)$ de G.

iii) On a : $\underline{H} \lhd G$, $\underline{H} \cap N = \{1_G\} = \{(1, 1)\}$, $\underline{H}.\underline{N} = \{\underline{h}.\underline{n} \mid \underline{h} \in \underline{H} \text{ et } \underline{n} \in \underline{N}\} = G$. On a de plus $N \lhd G$

Si on identifie H à $\underline{H}$, et N à $\underline{N}$, l'opération $\underline{N} \to \underline{H}$ est donnée par

$$\underline{n}.\underline{h} = \underline{n}.\underline{h}.\underline{n}^{-1}$$

1.5.3 Proposition

i) **Caractérisation interne** : Soit G un groupe contenant deux sous groupes H,N, avec $H \lhd G$, $H \cap N = \{1\}$, et $H.N = G$. Alors, g est un produit semi direct de ces deux sous groupes. $G = H \rtimes N$, où l'opération de N dans H est $n.h = nhn^{-1}$. de plus, si $N \rtimes G$, le produit est direct.

ii) **Caractérisation externe** : Soit $1 \to H \xrightarrow{i} G \xrightarrow{\Pi} N \to 1$ une suite exacte scindée admettant une section $S : N \to G, \Pi \circ S = Id_N$.Alors N est isomorphe au sous groupe $S(N)$ de G et $G = i(H) \rtimes S(N) \simeq H \rtimes N$ pour l'opération

$$"n.h = nhn^{-1}" \Leftrightarrow S(n).i(H) = S(n).i(h).S(n)^{-1}$$

1.6 Structure de groupe de $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$

Lemme : Soit $n \in \mathbb{N}$ et $s \in \mathbb{Z}$, les propriétés suivantes sont équivalentes :

i) $s \wedge n = 1$

ii) $\overline{s}$ engendre $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$

iii) $\overline{s} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$

1.6.1 Définition ***(Fonction caractéristique d'Euler)***

La fonction caractéristique d'Euler est définie par :

$$\varphi(n) = card((\frac{\mathbb{Z}}{n\mathbb{Z}})^*) = card\{s \in \{1..n\} \mid s \wedge n = 1\}$$

1.6.2 Proposition

i) Pour p premier et $n \in \mathbb{N}^*$, $\varphi(p^n) = p^{n-1}(p - 1)$

ii) $Aut(\frac{\mathbb{Z}}{n\mathbb{Z}}, +) \simeq (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$

iii) On a un isomorphisme de groupes $\frac{\mathbb{Z}}{n\mathbb{Z}} \to \prod \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}$, où $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition de n en facteurs premiers. On en déduit un isomorphisme de groupes(pour la multiplication)

$$(\frac{\mathbb{Z}}{n\mathbb{Z}})^* \simeq \prod (\frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}})^*$$

Finalement,

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

Si $n \wedge m = 1$, alors $\varphi(nm) = \varphi(n).\varphi(m)$

1.6.3 Théorème

Soit p un nombre premier. Alors, le groupe $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$ est cyclique, donc isomorphe à $\frac{\mathbb{Z}}{p-1\mathbb{Z}}$, ie $\exists a \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ tel que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^* = \{1, a, a^2...a^{p-1}\}$

1.6.4 Théorème (bis)

Soit $\mathbb{K}$ un corps commutatif, soit $g \subset \mathbb{K}$ un sous groupe fini sur $\mathbb{K}^*$, alors G est cyclique.

1.6.5 *Lemme 1*

Un polynôme $P(X)$ à coefficients dans un corps commutatif $\mathbb{K}$ de degré d a au plus d racines dans $\mathbb{K}$

1.6.6 *Lemme 2*

$\forall n \in \mathbb{N}$, on a $n = \sum_{d|n} \varphi(d)$

1.6.7 *Généralisation*

i) Soit $p > 2$ un nombre premier et $\alpha \in \mathbb{N}^*$. Alors, $\frac{\mathbb{Z}}{p^\alpha \mathbb{Z}}$ est cyclique d'ordre $p^{\alpha-1}(p-1)$

ii) $(\frac{\mathbb{Z}}{4\mathbb{Z}})^* \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$ et, pour $\alpha \geq 3$, $(\frac{\mathbb{Z}}{2^\alpha \mathbb{Z}})^* \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}}$ n'est pas cyclique.

Lemme :

i) $\overline{1} + \overline{p}$ est d'ordre $p^{\alpha-1}$ dans $(\frac{\mathbb{Z}}{p^\alpha \mathbb{Z}})^*$

ii) $\forall k \in \mathbb{N}^*$, $(1+p)^{p^k} = 1 + \lambda_k . p^{k+1}$, avec $\lambda_k \wedge p = 1$

1.7 Les groupes S_n et A_n

1.7.1 *Proposition* ***(rappels)***

i) Deux cycles à support disjoints commutent

ii) toute permutation σ de S_n a une écriture unique (à l'ordre près) comme produit de cycles à supports disjoints. Cette décomposition correspond aux orbites de l'action de $< \sigma >$ sur $\{1..n\}$

iii) On définit le support d'une permutation σ par $supp(\sigma) = \{a \in \{1..n\} \mid \sigma(a) \neq a\}$

iv) Soit $(a_1..a_k)$ un cycle, il est décomposable en produit de transposition (non unique). En particulier, $(a_1..a_k) = (a_1 a_2)(a_2 a_3)..(a_{k-1} a_k)$. On en déduit notamment que S_n est généré par les transpositons.

v) Soit $\sigma \in S_n$, avec $\sigma = \tau_1..\tau_r = \tau'_1..\tau'_s$, où les τ_i et les τ'_i sont des transpositions. Alors $s \equiv r\ [2]$

vi) L'application

$$\begin{array}{rccc} \varepsilon & : & S_n & \to & \{-1,1\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \\ & & \sigma & \mapsto & (-1)^r \end{array}$$

est bien définie et est un morphisme de groupe.

1.7.2 *Définition* ***(Groupe alterné)***

On note $A_n = Ker(\varepsilon)$ le groupe alterné, ou groupe des permutations paires.

1.7.3 *Remarques importantes*

S_n agit sur S_n par conjuguaison : soit $(a_1..a_k)$ un k cycle, $\sigma \in S_n$, on a $\sigma(a_1..a_k)\sigma^{-1} = (\sigma(a_1), \sigma(a_2)..\sigma(a_k))$. Cette opération est transitive, et pour tout k-cycle $(b_1..b_k)$, il existe un autre k-cycle $(a_1..a_k)$ et une permutation σ tels que $\sigma.(a_1..a_k) = \sigma(a_1..a_k)\sigma^{-1} = (b_1..b_k)$

1.7.4 *Définition* ***(Type d'une permutation)***

On définit le type de $\sigma \in S_n$ par $type(\sigma) = (e_n(\sigma), ...e_2(\sigma))$, où $e_i(\sigma)$ est le nombre de i-cycles apparaissant dans la décomposition de σ. Alors, σ opère transitivement sur l'ensemble des permutations d'un type donné.

1.7.5 *Théorème*

$\forall n \in \mathbb{N}, n \neq 4$, le groupe A_n est simple. Pour n=4, le sous groupe engendré par les doubles transpositions, V_4, est d'ordre 4 et est distingué dans A_4, de même que dans S_4.V_4 est une union de classes de conjuguaison sous S_4.

1.7.6 *Corollaire 1*

Soit $n \geq 5$. et H un sous groupe distingué de S_n. Alors, $H = \{1\}$, ou $H = A_n$, ou $H = S_n$.

1.7.7 *Corollaire 2*

Soit $n \geq 5$, $D(S_n) = A_n$, et $D(A_n) = A_n$.

1.7.8 *Lemme 1*

Pour $n \geq 3$, les 3-cycles engendrent A_n.

1.7.9 *Lemme 2*

Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n.

1.7.10 *Corollaire 3*

Pour $n \geq 5$, un sous groupe $H \triangleleft A_n$ qui contient un trois cycle est égal à A_n.

Lemme : On suppose $n \geq 5$ et $H \triangleleft A_n$, $H \neq \{1\}$. il existe alors un élément ρ dans H, $\rho \neq 1$, tel que $|supp(p)| \leq 5$.

1.8 Groupes résolubles, groupes nilpotents

1.8.1 *Définition* ***(Groupe résoluble)***

Soit g un groupe. On dit que G est **résoluble** s'il existe une suite finie de sous groupes de G

$$\{1\} = G_0 \subsetneq G_1 ... \subsetneq G_n = G$$

tels que, $\forall i \in \{1..n-1\}$, $G_i \triangleleft G_{i+1}$, et G_{i+1}/G_i est abélien.

1.8.2 *Proposition*

Soit g un groupe, on pose $D^0(G) = G$, et $\forall n \in \mathbb{N}, D^{n+1}(G) = D(D^n(G))$. Alors

$$G \text{ résoluble} \Leftrightarrow \exists n \in \mathbb{N}^*, D^n(G) = \{1\}$$

1.8.3 *Corollaire*

Un sous groupe et un quotient d'un groupe résoluble sont résolubles.Une extension d'un groupe résoluble par un groupe résoluble est résoluble. Pour $(1, H, G, N, 1)$ une suite exacte courte, G est résoluble si H et N le sont.

1.8.4 *Définition* ***(Groupe nilpotent)***

Un groupe G est nilpotent s'il existe une suite finie de sous groupes de G

$$\{1\} = G_0 \subsetneq G_1 ... \subsetneq G_n = G$$

tels que, $\forall i \in \{1..n-1\}$, $G_i \triangleleft G$, et G_i/G_{i-1} contenu dans le centre de G/G_{i-1}.

2 Représentation linéaire des groupes finis

2.1 Représentation linéaire, définition et premières propriétés

2.1.1 *Définition* ***(représentation inéaire)***

Soit g un groupe fini. une **repésentation linéaire** de G dans un $\mathbb{C}$-evddf V est un morphisme de groupe $G \xrightarrow{\rho} \mathcal{GL}(V)$. On note (V, ρ), ou V si ρ est clair, une telle représentation.

On suppose que G agit sur un en ensemble fini Y. soit un $\mathbb{C}$-evddf V, de base $(e_x)_{x \in X}$ indexée par X. Pour tout $g \in G$, on définit $\rho(g)$ par $\rho(g).e_x = e_{g.x}$. Alors, (V, ρ) est une rep. linéaire de G, appellée représentation linéaire de permutation associée à l'action de G sur X. Lorsque X=G, elle est dite régulière, et ρ est notée ρ^{reg}.

2.1.2 *Définition* ***(Morphisme de représentation)***

Soient (V_1, ρ_1), et (V_2, ρ_2) deux représentations linéaires de G. Un **morphisme de représentations** est une application linéaire $\varphi : V_1 \to V_2$ telle

que $\forall g \in G$, le diagramme suivant commute :

$$\begin{array}{ccccc} & V_1 & \xrightarrow{\varphi} & V_2 & \\ \rho_1(g) & \downarrow & & \downarrow & \rho_2(g) \\ & V_1 & \xrightarrow{\varphi} & V_2 & \end{array}$$

ie $\varphi \circ \rho_1(g) = \rho_2(g) \circ \varphi$.

2.1.3 Définition ***(Sous représentation)***

Soit (V, ρ) une représentation. Une sous représentation de G est un ssev W de V qui est stable par $\rho(g)$, et ce $\forall g \in G$. Alors, $(W, \rho' g \mapsto \rho(g)_{/W})$ est une représentation de G.

Lemme : Soit $W \subset V$ une sous representation de G, il existe une sous representation W' de (V, ρ) telle que

$$V = W \oplus W'$$

Remarque : Soit (V, ρ) une representation de G, il existe un produit scalaire hermitien que V qui est G invariant, ie

$$(x \mid y) = (\rho(g)(x) \mid \rho(g)(y)) \quad \forall x, y \in V$$

2.1.4 Définition ***(Représentation irréductible)***

Soit $\rho : G \to GL(V)$ une représentation linéaire de G. On dit que ρ est **irréductible (ou simple)** si les seules sous représentations de G sont $\{0\}$ et V.

2.1.5 Proposition

Toute représentation linéaire de G est somme directe de représentations irréductibles.

2.1.6 Lemme ***(de Schur)***

Soit $\varphi : (V, \rho_1) \to (W, \rho_2)$ un morphisme de représentations. **On suppose V et W irréductibles**.

i) Soit φ est un isomorphisme, soit $\varphi = \widetilde{0}$

ii) Si $V = W$ et $\rho_1 = \rho_2$, alors $\varphi = \lambda Id$ avec $\lambda \in \mathbb{C}$

2.1.7 Proposition

Pour toute représentation (V, ρ) de G, il existe une unique décomposition (à l'ordre des facteurs près)

$$V = V_1^{\oplus a_1} \oplus V_2^{\oplus a_2} ... \oplus V_k^{\oplus a_k}$$

où les V_i sont des sous représentations irréductibles, deux à deux non isomorphes. La notation $W^{\oplus a}$ désigne un espace vectoriel somme directe de a espaces vectoriels isomorphes à W. Si W est muni de $\rho : G \to GL(V)$, alors $W^{\oplus a}$ est muni de la représentation $\rho^{\oplus a}$ définie par $\rho^{\oplus a}(g)(e_1 + ... + e_a) = \rho(g)(e_1) + ...\rho(g)(e_a)$ Les composantes $V_k^{\oplus a_k}$ sont appellées **composantes isotypiques** de (V, ρ). On dit qu'une représentation est **isotypique** si elle ne comprend qu'une seule composante isotypique.

2.2 La théorie des caractères

2.2.1 Définition ***(Fonction centrale, caractère)***

Une fonction $f : G \to \mathbb{C}$ est dite **centrale (ou fonction de classe)** si elle vérifie :

$$\forall h, g \in G, \quad f(ghg^{-1}) = f(h) \Leftrightarrow \forall h, g \in G, \quad f(gh) = f(hg)$$

On note $\mathscr{C}(G)$ l'espace des fonctions centrales sur G. C'est un $\mathbb{C}$-espace vectorielde dimension h, où h est le nombre de classes de conjuguaison de G (i.e. le nombre d'orbites de G agissant dans G par conjuguaison).

Le **caractère** de (V, ρ) est la fonction centrale $\chi_\rho G \to \mathbb{R}$ définie par $\chi_\rho(g) = Tr(\rho(g))$

2.2.2 Théorème

Soient (V, ρ) et (V', ρ') deux représentations irréductibles de G. Alors, $(\chi_\rho \mid \chi_{\rho'}) = \begin{cases} 1 \text{ si } V \simeq V' \\ 0 \text{ si } V \not\simeq V' \end{cases}$

2.2.3 *lemme*

On note $\varphi = \frac{1}{|G|}\sum_{g\in G}\rho(g) \in End(V)$, et $V^G = \{v \in V, f(g).v = v, \forall g \in G\}$. On a alors φ qui est un projecteur de V sur V^G

2.2.4 *Définition ($\widetilde{\rho}$, représentation duale)*

Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations de G. On définit la représentation $\widetilde{\rho}$ sur $Hom(V_1, V_2)$, ensemble des morphisùes de V_1 dans V_2, par

$$\widetilde{\rho}(\varphi)(v) = \rho_2(g)(\varphi(\rho_1(g)^{-1}(v)))$$

La **représentation duale (ou contragédiente)** est $\rho^* = Hom(V_1, \mathbf{1}_G)$. Par conséquent, on a :

$$\rho^*(\varphi)(v) = \varphi(\rho(g)^{-1}(v)) \quad \forall \varphi \in Hom(V, \mathbb{C}) = V^\times$$

Lemme : Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations de G.Le caractère χ de la représentation $Hom(V_1, \mathbf{1}_G)$ est $\overline{\chi}_{\rho_1}.\chi_{\rho_2}$. En particulier, le caractère χ_{ρ^*} de la représentation (V^*, ρ^*) contragédiente de (V, ρ) est $\chi_{\rho^*} = \overline{\chi}_\rho$ On note $Hom_G(V_1, V_2)$ l'ensemble des morphismes de représentation de (V_1, ρ_1) dans (V_2, ρ_2)

2.2.5 *Corollaire 1*

Les caractères des représentations irréductibles de G forment un système orthonormal dans l'espace des fonctions centrales sur G. En particulier, le nombre de représentations irréductibles à isomorphisme près est fini est inférieur à $dim(\mathscr{C}(G))$ =nombre de classes de conjuguaison de G

2.2.6 *Corollaire 2*

Une représentation de G est déterminée par son caractère (Le caractère χ_ρ de ρ caractérise ρ)

2.2.7 *Proposition*

Soit R la représentation régulière de G. ($V_R = \bigoplus_{g\in G}\mathbb{C}e_g$, et $\rho(g)(e'_g) = e_{gg'}$). On a

$$\begin{cases} \chi_R(g) = 0 \text{ si } g \neq 1_G \\ \chi_R(g) = |G| \text{ si } g = 1_G \end{cases}$$

De plus, toute représentation irréductible V_i de G intervient dans la représentation régulière avec la multiplicité $a_i = dim(V_i)$. On a donc

$$V_R = V = V_1^{\oplus dim(V_1)} \oplus V_2^{\oplus dim(V_2)} ... \oplus V_k^{\oplus dim(V_k)}$$

2.2.8 *Corollaire*

$$|G| = Dim(V_R) = \sum_{i=1}^{k}(Dim(V_i)^2$$

2.2.9 *Théorème 2*

Le nombre de représentations irréductibles de G est égal au nombre de classes de conjuguaison de G. Les caractères des représentations irréductibles forment une base orthonormale de $\mathscr{C}(G)$.

Lemme : Soit (V, ρ) une représentation de G. Soit ,$\alpha : G \to \mathbb{C}$ une fonction sur G. On pose $\varphi_{\alpha/v} = \sum_{g\in G}\alpha(g)\varphi(g) \in End(V)$. Si α est une fonction centrale, on a alors $\varphi_{\alpha/v}$ qui est un morphisme de représentations.

2.2.10 *Proposition*

les propriétés suivantes sont équivalentes :

i) G est abélien

ii) Toutes les représentations irréductibles de G sont de dimension 1

2.2.11 *Définition ($\widehat{G}$)*

On définit G dual, $\widehat{G} = \text{Hom}(G, \mathbb{C}^*)$, ensemble des caractères/représentations irréductibles, de $G \to \mathbb{C}^*$. On a un isomorphisme

canonique

$$\begin{array}{ccccccc} G & \to & & & \widehat{\widehat{G}} & & \\ g & \mapsto & \varphi_g & : & \widehat{G} & \to & \mathbb{C}^* \\ & & & & \chi & \mapsto & \chi(g) \end{array}$$

2.2.12 Proposition

Soit G un groupe, D(G) son groupe dérivé, et $\Pi : G \to G^{ab}$. Pour χ un caractère de G^{ab}, on obtient un caractère $\chi \circ \Pi$ de G.Par ailleurs, on obtient ainsi toutes les représentations de G.

2.2.13 Définition ***(représentation standard)***

Pour $n \in \mathbb{N}$, la représentation de permutation de S_n correspond à l'action de S_n sur $\{1, .., n\}$, l'espace V_n de cette représentation est $V_n = \bigoplus_{i=1}^{n} \mathbb{C}e_i$, avec $\forall \sigma \in S_n$, $\rho_n(\sigma)(e_i) = e_{\sigma(i)}$. L'espace $\mathbb{C}(e_1 + .. + e_n)$ est isomorphe à la représentation triviale. Soit H l'hyperplan d'équation $\sum_{i=1}^{n} x_i = 0$. Alors H est stable par $\rho(g), \forall g \in G$. On dit que$(H, \rho_{n/H})$, est la représentation standard de S_n, notée ρ^{stand}, de caractère $\chi_{stand} = \chi_{\rho_n} - \mathbf{1}$.

2.2.14 Proposition ***(Orthogonalité des colonnes)***

Soit $s \in G$, et c(s) le cardinal de la classe de conjuguaison de s. Soient $\chi_1..\chi_r$ les caractères des représentation irréductibles de G.

a) $\sum_{i=1}^{h} \chi_i(s)\overline{\chi_i(s)} = \frac{|G|}{c(s)}$

b) Si $t \in G$ n'est pas conjugué à s, on a $\sum_{i=1}^{h} \chi_i(s)\overline{\chi_i(t)} = 0$

3 Produit tensoriel d'espaces vectoriels et de représentations

Définition ***(Produit tensoriel)***

Soient V_1 et V_2 deux $\mathbb{C}$-espace vectoriel de dimension finie. On appelle produit tensoriel de V_1 et V_2 un $\mathbb{C}$-espace vectorielW, muni d'une application bininéaire $b : V_1 \times V_2 \to W$, telle que, si $(e_1..e_n)$ est une base de V_1, $(f_1..f_n)$ est une base de V_2, alors les $(b(e_i, f_j))_{i,j}$ sont une base de W. En particulier, $dim(W) = dim(V_1)dim(V_2)$

Proposition

Un tel espace existe et est unique dans le sens suivant : soient $(W_1, b_1(.,.))$, $(W_2, b_2(.,.))$ deux produits tensoriels de V_1 et V_2, alors il existe un unique isomorphisme linéaire $U : W_1 \to W_2$ tel que $b_2(x, y) = U \circ b_1(x, y)$. On note $W = V_1 \otimes V_2$ et $\begin{array}{ccccc} b & : & V_1 \times V_2 & \to & W \\ & & (x, y & \mapsto & x \otimes y \end{array}$ l'application bilinéaire $b(x, y) = x \otimes y$

On a la propriété universelle suivante : soit E un espace vectoriel, et $b_E : V_1 \times V_2 \to E$ une application bilinéaire, alors, il existe un unique morphisme (linéaire) $U : V_1 \otimes V_2 \to E$ tel que $b_E(x, y) = U(x \otimes y)$

Lemmme

Soient $u_1 \in \mathrm{End}(V_1)$, et $u_2 \in \mathrm{End}(V_2)$. il existe un unique endomorphisme $u \in \mathrm{End}(V_1 \otimes V_2)$ tel que $\forall (x_1, x_2) \in V_1 \times V_2$, $u(x_1 \otimes x_2) = u_1(x_1) \otimes u_2(x_2)$. On note alors $u = u_1 \otimes u_2$.

Définition ***(Produit tensoriel de représentations)***

Soient (V_1, ρ_1), (V_2, ρ_2), deux représentations de G. On définit une représentation $\rho = \rho_1 \otimes \rho_2$ sur $V_1 \otimes V_2$ par $\rho(g) = \rho_1(g) \otimes \rho_2(g)$. Cette représentation n'est pas nécessairement irréductible, même si V_1 et V_2 le sont. Enfin, on a la formule $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1}\chi_{\rho_2}$

Lemme

Soient V_1 et V_2 deux espace vectorielsur $\mathbb{C}$, $V_1^* = \mathrm{Hom}(V, \mathbb{C})$ le dual. Il existe un isomorphisme canonique :

$$\begin{array}{rccccc} \psi & : & V_1^* \otimes V_2 & \to & \mathrm{Hom}(V_1, V_2) & \\ & & e^* \otimes f & \mapsto & \psi(e^* \otimes f) = & \begin{array}{rccc} \varphi_{e^*,f} & : & V_1 & \to & V_2 \\ & & x & \mapsto & \varphi_{e^*,f}(x) = e^*(x)f \end{array} \end{array}$$

Proposition

Soient (V_1, ρ_1), (V_2, ρ_2) deux représentations de G. Soit (V_1^*, ρ_1^*) la représentation contragédiente de (V_1, ρ_1). Alors, $\psi : V_1^* \otimes V_2 \to \mathrm{Hom}(V_1, V_2)$ est un isomorphisme de représentations.

Proposition ***(Produit tensoriel externe)***

Soient G_1, G_2 deux groupes et soient (V_1, ρ_1), (V_2, ρ_2) deux représentations de G_1 et G_2. On définit le produit tensoriel externe $(V_1 \boxtimes V_2, \rho)$, comme la représentation de $G_1 \times G_2$ sur $V_1 \otimes V_2$ telle que :

$$\rho(g_1, g_2)(v_1 \otimes v_2) = \rho_1(g_1)(v_1) \otimes \rho_2(g_2)(v_2)$$

De plus, si V_1, V_2 sont irréductibles, alors $V_1 \otimes V_2$ est une représentation irréductible de $G_1 \times G_2$. par ailleurs, on obtient ainsi toutes les représentations irréductibles de $G_1 \times G_2$.

3.0.15 Définition ***(Produits symétriques et alternés)***

Soit V un $\mathbb{C}$-espace vectoriel, posons $W = V \otimes V$. on dispose d'un automorphisme $\begin{array}{rccc} \theta & : & W & \to & W \\ & & x \otimes y & \mapsto & y \otimes x \end{array}$ On a alors $\theta^2 = 1$, et une décomposition $V \otimes V \simeq \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$, encore notée $V \otimes V \simeq \mathrm{S}^2(V) \oplus \Lambda^2(V)$, où l'on a défini

$$\mathrm{Sym}^2(V) = \{z \in V \otimes V, \theta(z) = z\}, \text{ et } \mathrm{Alt}^2(V) = \{z \in V \otimes V, \theta(z) = -z\}$$

3.0.16 Proposition

On note $\chi_{Sym^2}(V)$, ou $\chi_{Sym^2}(\rho)$ le caractère de $(Sym^2(V), Sym^2(\rho))$, alors

$$\chi_{Sym^2}(V)(g) = \frac{\chi_\rho(g)^2 + \chi_\rho(g^2)}{2}, \text{ et } \chi_{Alt^2}(V)(g) = \frac{\chi_\rho(g)^2 - \chi_\rho(g^2)}{2}$$

3.0.17 lemme

Soient E_1, E_2, E_3 trois $\mathbb{C}$-espace vectoriel de dimension finie, il existe un unique isomorphisme $\begin{array}{ccc} E_1 \otimes (E_2 \otimes E_3) & \to & (E_1 \otimes E_2) \otimes E_3 \\ x \otimes (y \otimes z) & \mapsto & (x \otimes y) \otimes z \end{array}$

3.0.18 Proposition ***(Traduction de la propriété universelle pour un r-produit tensoriel :)***

Pour toute application r-linéaire $\psi : E^r \to F$, il existe une unique application $U : \overset{r}{\underset{i=1}{\otimes}} E = T^r(E) \to F$ tel que $\psi(x_1..x_r) = U(x_1 \otimes .. \otimes x_r)$

3.0.19 Définition ***(Application symétrique, alternée)***

On dit qu'une application r-linéaire ψ est **symétrique** (resp. **alternée**) si $\forall \sigma \in S_n$, $\forall (x_1..x_r) \in E^r$

$$\psi(x_{\sigma(1)}..x_{\sigma(r)}) = \psi(x_1..x_r)$$

$$(\text{resp. } \psi(x_{\sigma(1)}..x_{\sigma(r)}) = \varepsilon(\sigma)\psi(x_1..x_r))$$

On définit également

$$W_r = < (x_{\sigma(1)} \otimes .. \otimes x_{\sigma(r)}) - (x_1 \otimes .. \otimes x_r) >_{\sigma \in S_r, x_1..x_r \in E}$$

3.0.20 Proposition

On a la propriété universelle suivante : Soit $\psi : E^r \to F$ une application r-linéaire symétrique, alors, il existe une unique application linéaire

$\overline{U} : S^r(E) \to F$ (ou $S^r(E) = T^r(E)/W_r(E)$) telle que l'on aie une factorisation :

$$\begin{array}{ccccc} E^r & \stackrel{\psi}{\to} & F & & \\ & \searrow & \uparrow U & \nwarrow \overline{U} & \\ & & T^r(E) & \to & S^r(E) \end{array}$$

3.0.21 Proposition

Si E est un $\mathbb{C}$-espace vectoriel normé de dimension finien de base $(e_1..e_n)$, alors $\Lambda^r(E) = 0$ si $r > n$, et, pour $r \leq n$, $\Lambda^r(E)$ a pour base les $e_{i_1} \wedge e_{i_2} ... \wedge e_{i_r}$, avec $i_1 < i_2 < .. < i_r$. En particulier, $\Lambda^n(E) = \mathbb{C}(e_1 \wedge ... \wedge e_n)$, et $dim(\Lambda^r(E)) = \binom{n}{k}$

4 *Anneaux, Modèles*

On considère ici des anneaux unitaires commutatifs.

4.1 Definitions, premières propriétés

4.1.1 Définition ***(Idéal)***

Soit A un anneau. Une partie I de A est un **idéal** si :

i) $(I, +)$ est un sous groupe de A

ii) Si $x \in I$, $a \in A$, alors $a.x \in I$

4.1.2 Proposition

Soit A un anneau , I un idéal de A. Alors, le quotient $(A/I, +)$ muni de la multiplication $\overline{a}\overline{b} = \overline{ab}$ est un anneau, appellé **quotient de A par I** dont l'élément unité est $1 + I = \overline{1}$, et $\begin{array}{rccc} \Pi & : & A & \to & A/I \\ & & a & \mapsto & \overline{a = a + I} \end{array}$ est un morphisme d'anneaux

4.1.3 Théorème ***(De factorisation)***

Soit $f : A \to B$ un morphisme d'anneaux, il existe un unique morphisme d'anneaux $\widetilde{f} : A/Ker(f) \to B$ tel que $f = \widetilde{f} \circ \Pi$. De plus, $\widetilde{f}$ est injective, et induit un isomorphisme d'anneaux de $A/Ker(f)$ dans $Im(f)$

4.1.4 Définition ***(Anneau intègre)***

Un anneau A est dit intègre si $A \neq \{0\}$, et si $\forall a, b \in A$, $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

4.1.5 Théorème ***(Corps des fractions d'un anneau intègre)***

Soit A un anneau intègre, il existe un corps $\mathbb{K}$ et un homéomorphisme injectif $i : A \to \mathbb{K}$ universel tel que, $\forall \mathbb{K}'$, $\forall j : A \to \mathbb{K}'$ morphisme injectif, il existe un unique morphisme de corps $f : \mathbb{K} \to \mathbb{K}'$ tel que $j = f \circ i$. Le couple $(\mathbb{K}, i)$ est unique à isomorphisme unique près. On dit que $\mathbb{K}$ est le **corps des fractions** de A, noté Frac(A)

4.1.6 Définition ***(Idéal premier)***

Un idéal I de A est dit **premier** si le quotient A/I est intègre, c'est à dire si il est différent de A, et si

$$\forall a, b \in A \quad ab \in I \Rightarrow a \in I \text{ ou } b \in I$$

4.1.7 Définition ***(Idéal maximal)***

Un idéal I de A est dit maximal s'il est différent de A, et si le seul idéal qui le contient strictement est A lui même.

4.1.8 Proposition

I est maximal dans A $\Leftrightarrow$ A/I est un corps. En particulier, tout idéal maximal est premier.

4.1.9 *Définition* ***(Topologie de Zariski)***

Soit A un anneau, on pose spec(A) l'ensemble des idéaux premiers de A. On définit une topologie sur spec(A) définie par ses fermés : ce sont les

$$V_I = \{P \in spec(A), I \subset P\}$$

Les ouverts sont donc les

$$D_I = \{P \in spec(A), I \not\subseteq P\}$$

4.1.10 *Proposition*

Les $D(aA)$, $a \in A$ forment une base d'ouverts de spec(A)

4.1.11 *Proposition*

spec(A), muni de la topologie de Zariski, est quasicompact (ie. non séparé)

4.1.12 *Définition* ***(Radical)***

On appelle **radical de A** l'idéal premier $R(A) = \bigcap_{P \in spec(A)} P$. Dans un anneau intègre, $R(A) = \{0\}$.

4.2 Divisibilité dans les anneaux intègres

4.2.1 *Définition* ***(Divisibilité)***

Soient $a, b \in A$, on dit que a divise b s'il existe $c \in A$ tel que $b = ac$. Une définition équivalente est que $(b) \subset (a)$. En particulier, si $u \in A^*$, on a $(u) = A$, car $u \mid a \quad \forall a \in A$

4.2.2 *Proposition*

Soient $a, b \in A$

i) $a \mid b$ et $b \mid a$

ii) $(a) = (b)$

iii) $\exists u \in A^* \quad a = ub$

On dit alos que a et b sont associés.

4.2.3 *Définition* ***(Element irréductible)***

Un élément $p \in A$ est dit **irréductible** s'il n'est pas dans A^*, et si ses seuls diviseurs lui sont associés.

4.2.4 *Définition* ***(Anneau principal, idéal principal)***

Un idéal de A est dit **principal** s'il est de la forme $aA = (a)$ $a \in A$. Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.

4.2.5 *Définition* ***(Eléments premiers entre eux)***

On dit que a et b sont premiers entre eux si leurs seuls diviseurs communs sont les éléments de A^*

4.2.6 *Théorème* ***(Bézout)***

Soit A un anneau principal. deux éléments a et b de A sont premiers entre eux si et seulement si il existe $u, v \in A$ tels que $au + bv = 1$, ie si $aA + bA = (a, b) = A$

4.2.7 *Définition* ***(Anneau factoriel)***

Un anneau est dit **factoriel** s'il vérifie les trois propriétés suivantes :

i) A est intègre

ii) Tout élément non nul $a \in A$ s'écrit sous la forme $a = up_i..p_r$, $u \in A^*$, $r \in \mathbb{N}$ et les p_i irreductibles.

iii) **Point clé : Unicité** si $a = up_1..p_r = vq_1..q_s$, alors $r = s$, et il existe $\sigma \in S_n$, telle que $\forall i p_i$ et $q_{\sigma(i)}$ soient associés.

Lemme : Soit A un anneau factoriel, $a = u_a \Pi p^{v_p(a)}$, et $b = u_b \Pi p^{v_p(b)}$. Alors,

$$a \mid b \Leftrightarrow \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$$

4.2.8 Proposition

Soit A un anneau intègre, tel que tout élément non nul soit produit d'irréductibles. Alors, les propriétés suivantes sont équivalentes : :

i) A est factoriel

ii) $\forall p \in A$, p irréductible, l'idéal $(p) = pA$ est premier

iii) (Lemme de Gauss pour les anneaux factoriels) Si $a \mid bc$ avec $a \wedge b = 1$, alors $a \mid c$

4.2.9 Définition ***(PGCD, PPCM)***

Soit A un anneau factoriel, $a = u_a \Pi p^{u_p(a)}$, $b = u_b \Pi p^{u_p(b)}$. On peut alors définir :

$$PGCD(a,b) = \prod_{p \in \mathcal{P}} p^{min(v_p(a), v_p(b))} \text{ et } PPCM(a,b) = \prod_{p \in \mathcal{P}} p^{min(v_p(a), v_p(b))}$$

4.3 Anneaux noetheriens

4.3.1 Proposition

Soit A un anneau intègre, les propriétés suivantes sont équivalentes : :

i) Tout idéal de A est engendré par un nombre fini d'éléments

ii) Tout suite croissante d'idéaux de A est stationnaire

iii) Toute famille non vide d'idéaux de A a un élément maximal (pour l'inclusion)

Si ces conditions sont vérifiées, on dit que A est **noetherien**

Remarque : Les idéaux de A/I sont les J/I, avec J idéal de A et $I \subset I$

4.3.2 Proposition

Soit A un anneau intègre noetherien. Alors, tout élément non nul $x \in A - \{0\}$ s'écrit sous la forme $x = u.p_1...p_n$, avec $u \in A^*$, et les p_i irréductibles dans A, n un entier.

4.3.3 Corollaire

A principal $\Rightarrow$ A factoriel

4.3.4 Corollaire

Soit $\mathbb{K}$ un corps, soit $P(X) \in \mathbb{K}[X]$ irréductible, alors $L := \frac{\mathbb{K}[X]}{P(X)\mathbb{K}[X]}$ est un corps.

4.3.5 Théorème

Soit A un anneau noetherien, alors A[X] est noetherien

4.3.6 Corollaire

Si A est noetherien, alors $\forall n \in \mathbb{N}$, $A[X_1, X_2...X_n]$ est noetherien.

4.3.7 Définition ***(Type fini)***

Soit A un anneau, une **A algèbre de type fini** si on a un morphisme d'anneaux $f : A \to B$, et $x_1...x_n \in B$ tel que le morphisme

$$\begin{array}{rccc} \widetilde{f} & : & A[X_1..X_n] & \to & B \\ & & \Sigma a_i X_i & \mapsto & \Sigma a_i x_i \end{array}$$

soit surjectif.

4.4 Anneaux euclidiens, factoriels, principaux.

4.4.1 *Définition* ***(Anneau euclidien)***

Un anneau intègre A est dit **euclidien** si $\exists v : A - \{0\} \to \mathbb{N}$ tel que $\forall a, b \in A - \{0\}$, $\exists (q, r) \in A^2 \quad a = bq + r = 0 \quad v(r) < v(b)$

4.4.2 *Corollaire*

Soit A noetherien, tout anneau B qui est une A algèbre de type fini est noetherien

4.4.3 *Théorème*

A euclidien $\Rightarrow$ A principal

4.4.4 *Définition* ***(Contenu d'un polynome)***

Soit A un anneau factoriel. Le contenu $c(P)$ d'un polynome $P \in A[X]$ est le PGCD des coefficients de P. On dit que P est primitif si $c(P) \in A^*$. On remarque que $\forall P \in A[X]$, $P = c(P)Q$, avec Q primitif.

4.4.5 *Proposition*

$\forall P, Q \in A[X]$, $c(PQ) = c(P)c(Q)$

4.4.6 *Théorème*

Soit A un anneau factoriel, de corps des fractions $\mathbb{K} = Frac(A)$. Les irréductibles de $A[X]$ sont :

i) Les polynomes $P = p$ de degré 0, avec $p \in A$, et p irréductibles dans A.

ii) Les polynomes primitifs de $A[X]$ de degré strictement positif, irréductibles dans $\mathbb{K}[X]$

4.4.7 *Théorème*

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

4.4.8 *Théorème* ***(Critère d'Eisenstein)***

Soit A un anneau factoriel, $P(X) \in A[X]$ un polynome non constant de $A[X]$. Soit P un irréductible de A, $P(X) = \sum_{k=0}^{n} a_k X^k$. On suppose :

i) p ne divise pas a_n

ii) $p \mid a_k$, $\forall k \in \{0, ..., n-1\}$

iii) $p^2 \nmid a_0$

Alors $P(X)$ est irréductible dans $\mathbb{K}[X]$, $\mathbb{K} = Frac(A)$

4.4.9 *Définition* ***(Polynomes cyclotomiques)***

Soit p un nombre premier, on définit le **p-ième polynome cyclotomique** $\varphi_p(X) = \frac{X^p - 1}{X - 1} = \prod_{k=1}^{p-1} (X - e^{\frac{2i\pi k}{p}})$

4.4.10 *Proposition*

$\varphi_p(X)$ est irréductible pour tout p premier.

4.4.11 *Proposition*

Soit A un anneau factoriel, $\mathbb{K}$ le corps des fractions de A. Soit $P(X) \in A[X]$ primitif, p un irréductible de A, et

$$\begin{array}{ccc} A[X] & \to & \frac{A}{(p)}[X] \\ Q & \mapsto & \overline{Q} \end{array}$$

On suppose que :

$$\begin{cases} deg\, P = deg\, \overline{P} \\ \overline{P} \text{ irréductible dans } Frac(B)[X], B = \frac{A}{(p)} \end{cases}$$

Alors P est irréductible.

4.5 Modules sur les anneaux

4.5.1 *Définition* ***(A-module)***

Soit A un anneau (commutatif non nul). Un **A-module** $(M,+,.)$ est un ensemble M muni d'une loi interne $+$, et d'une loi externe $\begin{array}{rccc} . & : & A\to M & \to & M \\ & & (a,m) & \mapsto & a.m \end{array}$ telle que, $\forall \alpha,\beta \in A^2\ \forall \in m,m' \in M^2$:

i) $(M,+)$ est un groupe abélien

ii) $\alpha(m+m') = \alpha m + \alpha m'$

iii) $(\alpha+\beta)m = \alpha m + \beta m$

iv) $(\alpha\beta)m = \alpha(\beta m)$

v) $1.m = m$

Si A est un corps, un A-module est juste un A-espace vectoriel. Un **sous module** $N \subset M$ est un sous groupe $(N,+)$ de $(M,+)$ stable par multiplication par les éléments $a \in A$

4.5.2 *Définition* ***(Module engendré)***

Soit M un module de A, et S une partie de M. Soit $E = \{N$ sous module contenant $E\}$ On définit le sous module engendré par M, $< S >$, par :

$$< S >= \bigcap_{N\in E} N = \{\sum_{s\in S} \alpha_s.s, (\alpha_s)_{s\in S} \text{ une famille presque nulle d'éléments de S}\}$$

4.5.3 *Définition* ***(Morphisme de A-modules)***

Un **morphisme de A-modules** est une application $f : M \to M'$ telle que :

i) $\forall m_1,m_2 \in M,\ f(m_1+m_2) = f(m_1)+f(m_2)$

ii) $\forall a \in A,\ \forall m \in M,\ f(a.m) = a.f(m)$

Alors, $Ker(f) = f^{-1}(\{0\})$ et $Im(f) = f(M)$ sont des sous modules de M et M' respectivement. On a également la notion d'isomorphisme entre A-modules.

4.5.4 *Théorème/Definition* ***(Passage au quotient)***

Soit N un sous module d'un A-module M le groupe quotient $\frac{M}{N}$, muni de la loi externe $\alpha.\overline{m} = \overline{\alpha.m}$, est un module, appellé module quotient de M par N. Si $f : M \to M'$ est un morphisme de A modules, il existe un unique morphisme de A-modules $\widetilde{f} : \frac{M}{Ker\, f} \to M'$ tel que $f = \widetilde{f} \circ \Pi$, où Π est la surjection canonique. de plus, $\widetilde{f}$ est injective, et on a un isomorphisme de A-modules $\widetilde{f} : \frac{M}{Ker\, f} \to Im(f)$

4.5.5 *Définition* ***(Sommes directes internes et externes)***

Soit $(M_i)_{i\in I}$ une famille de A-modules.

i) La **somme directe externe** $\bigoplus_{i\in I} M_i$ est le sous A-module de $\prod_{i\in I} M_i$ constitué des $(m_i)_{i\in I}$ presque nulles. Si I est fini, $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$

ii) Soit $(M_i)_{i\in I}$ une famille de sous modules d'un A-module M. La somme directe interne, notée $\sum_{i\in I} M_i$ est le sous module engendré par les M_i $\sum_{i\in I} M_i = \{\sum_{i\in I} m_i\ (m_i)_{i\in I}$ famille presque nulle $\}$. Par ailleurs, si la condition $\sum_{i\in I} m_i = 0 \Leftrightarrow m_i = 0 \forall i \in I$ est vérifiée, on dit que la somme est directe. Dans ce cas, $\sum_{i\in I} M_i \simeq \bigoplus_{i\in I} M_i$

4.5.6 *Définition* ***(Module de type fini)***

Un A-module M est dit de type fini si il existe une partie finie S de M qui engendre M. Si $S = \{s_1...s_r\} \subset M$, on a un morphisme surjectif de A-modules $\begin{array}{ccc} A^r & \to & M \\ (a_1...a_r) & \mapsto & \sum_{i=1}^{r} a_i s_i \end{array}$

On dit que M est un A-module **libre** s'il admet une base $(x_i)_{i\in I}$, i.e si tout $x \in M$ s'écrit de manière unique $x = \sum_{i\in I} a_i x_i$. Un A-module est **sans torsion** si il est "intègre"

Remarque : Un quotient de modules de type fini est de type fini.

4.5.7 *Proposition*

Un module libre M sur un anneau intègre A est sans torsion.

4.5.8 *Théorème*

Soit M un A module sur un anneau A. Si M est de type fini, et si M est libre, alors M admet une base finie $(m_1...m_r)$, ie $M = \overset{r}{\underset{i=1}{\oplus}} A.m_i$. De plus, toutes les bases de M sont de cardinal r.

4.5.9 *Lemme*

Soit A un anneau (non nul). On suppose qu'il existe une surjection de A modules $f : A^r \to A^s$, alors $r \geq s$

4.5.10 *Théorème*

Soit A un anneau noétherien, M un A-module de type fini. alors, tout sous module de M est de type fini.

Lemme : Soit $0 \to L_1 \to L \overset{\Pi}{\to} L_2 \to 0$ une suite exacte de A-modules. On suppose que L_1 et L_2 sont de type fini, alors L est de type fini.

4.6 Modules de type fini sur un anneau principal

4.6.1 *Théorème*

Soit A un anneau principal, alors tout sous module N de A^r est librede rang $m \leq n$

4.6.2 *Théorème* ***(Base adaptée)***

Soit A un anneau principal, M un A-module de rang n. Soit $N \subset M$ un sous A-module. Alors, il existe $e_1...e_n \in M$, et $d_1...d_n \in A$, avec $m \leq n$, tels que $d_i \mid d_{i+1} \forall i \in \{1...m-1\}$, et $(d_1e_1, ..., d_ne_n)$ soit une base de N.

Lemme 1 : $\exists f_1 \in Hom(M, A)$ morphisme de A-modules $M \to A$ tel que :

i) $f_1(N)$ est maximal parmi les $f(N)$, $f \in Hom(M, A)$

ii) En particulier, on a $f_1(N) = d_1A$, $\exists e_1 \in M$ tel que $f_1(e_1) = 1$ et tel que $u_1 = d_1e_1 \in N$

Lemme 2 : Avec les notations précédentes :

i) $M = Ae_1 \oplus Ker\, f_1$, et $N = Au_1 \oplus (Ker\, f_1 \cap N)$

ii) $\forall f \in Hom(M, A)$, $f(N) \subset d_1A$

4.6.3 *Corollaire*

Soit M un module de type fini sur A principal, Alors, il existe $d_1...d_s \in A$, avec $d_i \neq 0$, $d_i \notin A^*$, $d_1 \mid d_2... \mid d_s$ tel que

$$M = A^m \oplus (\overset{s}{\underset{i=1}{\oplus}} \frac{A}{d_iA})$$

avec $m \in \mathbb{N}$. Si $s = 0$, on convient que $M \simeq A^m$

4.6.4 *Définition* ***(module p-primaire)***

Un A module est dit p-primaire s'il est de la forme $\overset{s}{\underset{i=1}{\oplus}} \frac{A}{p^{u_i}A}$, $u_1..u_s \in \mathbb{N}$

4.6.5 *Théorème*

Soit M un A-module de type fini sur A anneau principal. Si $M \simeq A^m \oplus \overset{s}{\underset{i=1}{\oplus}} \frac{A}{d_iA} \simeq A^{m'} \oplus \overset{s'}{\underset{j=1}{\oplus}} \frac{A}{d'_jA}$, avec $m, m', s, s' \in \mathbb{N}$, $d_1 \mid d_2... \mid d_s$ $d'_1 \mid d'_2... \mid d'_{s'}$, avec $d_1, d'1 \notin A^*$, alors $m = m'$, $s = s'$, et $\forall i \in \{1..s\}$, et d_1 et d'_1 sont associés.

Lemme :

i) Soit $d = \cup \underset{p \in P}{\Pi} p^{v_p(d)}$ la décomposition de $d \in A$ en facteurs irréductibles, alors :

$$\frac{A}{dA} = \underset{p \in P}{\oplus} \frac{A}{p^{v_p(d)}A}$$

ii) Soit M un A-module de torsion, alors $M = \bigoplus_{p \in P} M_p$, avec M_p p-primaires. De plus, $\forall k$ assez grand, $M_p \simeq \frac{M}{p^k M}$

Lemme : Soit $\alpha \in \mathbb{N}$, et $M_\alpha = \frac{A}{p^\alpha A}$. Alors, si l'on pose $\mathbb{K} = \frac{A}{pA}$

$$p^n \frac{M_\alpha}{p^{n+1} M_\alpha} = \begin{cases} 0 \text{ si } n \geq \alpha \\ \mathbb{K} \text{ si } n < \alpha \end{cases}$$

4.6.6 Corollaire

$$dim_{\mathbb{K}} \left(\frac{p^n M_p}{p^{n+1} M_p} \right) = |\{i \in \{1...S_p\}, n < v_p(d_i)\}|$$

4.7 Interprétation externe d'algèbre linéaire

4.7.1 Définition ***(Ensemble des matrices)***

Soit A un anneau, $M_{p,q}(A)$ l'ensemble des matrices é p lignes et q colonnes é coefficients dans A.

4.7.2 Définition ***(Matrices équivalentes)***

Deux matrices B et C dans $M_{p,q}(A)$ sont équivalentes si il existe $M \in GL_p(A)$ et $V \in GL_q(A)$ telles que $C = UBV \Leftrightarrow$ il existe une base B de A^p et une base B de A^q telles que $Mat_{B,B'}(u) = C$, oé u est le morphisme de A^p dans A^q de matrice B dans les bases canoniques de A^p et A^q respectivement.

4.7.3 Théorème

Soit A un anneau principal

i) Toute matrice $B \in M_{p,q}(A)$ est équivalente é une matrice de la forme $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$, avec $D = diag(d_1...d_r)$, $d_1 \mid d_2... \mid d_r$

ii) Deux matrices de la forme $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix}$, avec $D = diag(d_1...d_r)$, $d_1 \mid d_2... \mid d_r$, et , avec $D' = diag(d'_1...d'_{r'})$, $d'_1 \mid d'_2... \mid d'_{r'}$ sont équivalentes si et seulement si $r = r'$ et $d_i \sim d'_i$ (associés) $\forall i$

4.8 Théorie élémentaire des corps

4.8.1 Définition ***(Diverses définitions)***

les corps $(\mathbb{K}, +, .)$ ici considérés sont commutatifs et ont au moins deux éléments $\{0, 1\}$, avec $0 \neq 1$. On appelle cartactéristique de $\mathbb{K}$, notée $car(\mathbb{K})$, le générateur positif du noyau du morphisme d'anneau $\begin{array}{ccc} \varphi : \mathbb{Z} & \to & \mathbb{K} \\ n & \mapsto & n-1 \end{array}$.

- Soit $car(\mathbb{K}) = 0$, φ est injective, $\mathbb{K}$ contient $\mathbb{Z}$, donc $\mathbb{Q} = Frac(\mathbb{Z})$, car $\mathbb{K}$ est un corps.
- Sinon, $\varphi(\mathbb{Z})$ est un sous anneau de intègre de $\mathbb{K}$, donc $car(\mathbb{K}).\mathbb{Z}$ est un idéal premier, et est donc monogéne (cf sous anneaux de $\mathbb{Z}$) de la forme $p.\mathbb{Z}$, avec p premier, donc $car(\mathbb{K}) = p$ est premier, $Im(\varphi)$ est isomorphe é $\frac{\mathbb{Z}}{p\mathbb{Z}}$, donc $\mathbb{K}$ contient le corps fini é p éléments.

4.8.2 Définition ***(Extension)***

Soit $\mathbb{K}$ un corps, une extension de $\mathbb{K}$ est un corps $\mathbb{L}$ contenant $\mathbb{K}$. Dans cette situation, $\mathbb{L}$ est un $\mathbb{K}$ espace vectoriel, via $\begin{array}{ccc} \mathbb{K} \times \mathbb{L} & \to & \mathbb{L} \\ (k, l) & \mapsto & k.l \end{array}$. Un corps de caractéristique 0 est un $\mathbb{Q}$ espace vectoriel, et un corps de caractéristique p est un $\frac{\mathbb{Z}}{p\mathbb{Z}}$ espace vectoriel.

Remarque : Tout morphisme de corps est injectif; en effet, soit $\varphi : \mathbb{K} \to \mathbb{L}$ un morphisme de corps, $Ker(\varphi)$ est un idéal, donc $Ker(\varphi) = \{0\}$ou $\mathbb{K}$. mais $\varphi(1_{\mathbb{K}}) = 1_{\mathbb{L}}$, donc $Ker(\varphi) = \{0\}$. On peut donc identifier $\mathbb{K}$ é un sous corps de $\mathbb{L}$.

4.8.3 Définition ***(Extension finie)***

Quand une extension $_{|\mathbb{K}}$ est de dimension finie comme $\mathbb{K}$-espace vectoriel, on dit que $_{|\mathbb{K}}$ est finie de degré d. On note $[\mathbb{L} : \mathbb{K}] = dim_{\mathbb{K}-ev}(\mathbb{L})$

4.8.4 *Théorème* ***(Base téléscopique)***

Soit $\mathbb{L}$ une extension de $\mathbb{K}$, et M une extension de $\mathbb{L}$. Si $\mathbb{L}|\,\mathbb{K}$, et si $M|\,\mathbb{L}$ est fini, alors $M|\,\mathbb{K}$ est fini, et $[M:\mathbb{K}] = [M:\mathbb{L}][\mathbb{L}:\mathbb{K}]$

4.8.5 *Définition* ***(Nombre transcendant)***

On dit que α est transcendant sur $\mathbb{K}$ si $\begin{array}{cccc}\varphi & : & \mathbb{K}[T] & \to & \mathbb{L} \\ & & P(T) & \mapsto & P(\alpha)\end{array}$ est injectif. Dans ce cas, $\mathbb{K}[\alpha] \simeq \mathbb{K}[T]$, et $\mathbb{K}(\alpha) = \mathbb{K}(T)$. Si φ n'est pas injectif, on note $\Pi_\alpha(X)$ le générateur unitaire de $Ker(\varphi)$. On dit alors que α est algébrique sur $\mathbb{K}$ de polynome minimal $\Pi_\alpha(X)$

4.8.6 *Proposition*

Soit $_{|\mathbb{K}}$ une extension de corps, et $\alpha \in \mathbb{L}$. les propriétés suivantes sont équivalentes :

i) α est algébrique sur $\mathbb{K}$

ii) $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$

iii) $\mathbb{K}[\alpha]$ est un $\mathbb{K}$-espace vectoriel de dimension finie

Dans ce cas, $[\mathbb{K}[\alpha] : \mathbb{K}] = deg(\Pi_\alpha(X))$, et on dit que α est de degré $[\mathbb{K}[\alpha] : \mathbb{K}]$ sur $\mathbb{K}$

4.8.7 *Définition* ***()***

Une extension de corps $_{|\mathbb{K}}$ est algébrique si tout $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$. On dit qu'un corps $\mathbb{K}$ est algébriquement clos si toute extension algébrique de $\mathbb{K}$ est égale à $\mathbb{K}$, ce qui équivaut à ce que tout polynôme de $\mathbb{K}[X]$ soit scindé, ou encore que les irréductibles de $\mathbb{K}[X]$ soie nt de degré 1.

4.8.8 *Théorème*

Soit $_{|\mathbb{K}}$ une extension de corps. Soit M l'ensemble des éléments de $\mathbb{L}$ qui sont algébriques sur $\mathbb{K}$

i) M est un sous corps de $\mathbb{L}$

ii) Tout élément de $\mathbb{L}$ algébrique sur M est algébrique sur $\mathbb{K}$

iii) Si $\mathbb{L}$ est algébriquement clos, M est algébriquement clos.

4.9 Corps de rupture, corps de décomposition

4.9.1 *Définition* ***(corps de rupture)***

Soit $\mathbb{K}$ un corps, $P(X) \in \mathbb{K}[X]$ un polynome irréductible. On dit qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture de $P(X)$ si $\exists \alpha \in \mathbb{L}$ tel que $P(\alpha) = 0$ et $\mathbb{L} = \mathbb{K}[\alpha]$

4.9.2 *Définition* ***($\mathbb{K}$-isomorphisme)***

Soient $\mathbb{L}_1$, $\mathbb{L}_2$ deux extensions de $\mathbb{K}$, un $\mathbb{K}$-isomorphisme de $\mathbb{L}_1$ sur $\mathbb{L}_2$ est un isomorphisme de corps $\mathbb{K}$-linéaire

4.9.3 *Théorème*

Pour tout polynôme irréductible $P(X) \in \mathbb{K}[X]$ il existe un corps de rupture, unique à $\mathbb{K}$-isomorphisme près.

4.9.4 *Définition* ***(Corps de décomposition)***

Soit $\mathbb{K}$ un corps et $P(X)$ un polynome de $\mathbb{K}[X]$. Un corps de décomposition de $P(X)$ est une extension de $\mathbb{K}$ finie, $\mathbb{L}$ telle que :

i) P est scindé sur $\mathbb{L}$: $P(X) = a\prod_{i=1}^{n}(X - \alpha_i)$, avec $a \in \mathbb{L}$, $\alpha_i \in \mathbb{N}$

ii) $\mathbb{L} = \mathbb{K}[\alpha_1 ... \alpha_n]$

4.9.5 *Théorème*

$\forall P \in \mathbb{K}[X]$, il existe un unique corps de décomposition à isomorphisme près.

4.10 Corps finis

Un corps $\mathbb{K}$ de cardinal fini est appellé corps fini. Il est de caractéristique $p > 0$, donc $\mathbb{K}$ est un espace vectoriel normé de dimension finiesur $\mathbb{F}_p$ donc $|\mathbb{K}| = p^n$, où $n = dim_{|\mathbb{F}_p}(\mathbb{K})$

4.10.1 Théorème

Soit p un nombre premier, n un entier non nul. Il existe à $\mathbb{F}_p$ isomorphisme près un unique corps de cardinal $p^n = q$. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Lemme : Un polynôme $P(X)$ a toutes ses racines distinctes si et seulemetn si $P \wedge P' = 1$

4.10.2 Théorème ***(De l'élément primitif)***

$\exists \alpha \in \mathbb{F}_p^n$ tel que $\mathbb{F}_{p^n} = F_p[\alpha]$

4.10.3 Définition ***(Automorphisme de Frobenius)***

$q = p^n$ l'application $\begin{array}{rccc} \varphi & : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & & x & \mapsto & x^p \end{array}$ est un morphisme de corps. φ est un automorphisme $\mathbb{F}_p$-linéaire de $\mathbb{F}_q$. On dit que φ est l'automorphisme de Frobenius et on note $Aut_{\mathbb{F}_p}(\mathbb{F}_q)$ l'ensemble des automorphismes de $\mathbb{F}_q$ $\mathbb{F}_q$-linéaires.

4.10.4 Proposition

$Aut_{\mathbb{F}_p}(\mathbb{F}_q)$ est cyclique d'ordre n généré par φ

4.10.5 Proposition

Il existe une bijection entre l'ensemble des sous corps de $\mathbb{F}_q$ et l'ensemble des sous groupes de $Aut_{\mathbb{F}_p}(\mathbb{F}_q)$ donné par

$$\begin{array}{ccc} \{H \text{ ss gpe de } Aut(\mathbb{F}_q)\} & \to & \text{ss corps de } \mathbb{F}_q \\ H & \mapsto & \mathbb{F}_q^H = \{x \in \mathbb{F}_q, h.x = x \forall h \in H\} \end{array}$$

4.10.6 Proposition

Soit $\mathbb{K}$ un corps fini de caractéristique p, $\mathbb{K} = \mathbb{F}_p^n$. Soit r un entier premier à p, et $l = r \wedge q - 1$. On note $\psi_r(x)$ le morphisme de groupe $\mathbb{K}^* \to \mathbb{K}^*$ tel que $\psi_r(x) = x^r$

i) Le noyau de ψ_r est l'unique sous groupe d'ordre d de $\mathbb{K}^*$, soit $\mathbb{K}^{*r} = Im_{\psi_r}$, alors $\mathbb{K}^{*r}$ est l'unique sous groupe de $\mathbb{K}^*$ d'ordre $\frac{q-1}{d}$.

$$x \in \mathbb{K}^{*r} \Leftrightarrow x^{\frac{q-1}{d}} = 1$$

ii) Si $p \neq 2$, $\mathbb{K}^{*r}$ est d'indice 2 dans $\mathbb{K}^*$

$$x \in \mathbb{K}^{*r} \Leftrightarrow x^{\frac{q-1}{d}} = 1$$

$$(-1) \in \mathbb{K}^* \Leftrightarrow q \equiv 1[4]$$

5 Groupes et géométrie

5.1 Générateurs et centre de GL(E), SL(E)

5.1.1 Proposition

Soit H un hyperplan de E, $u \neq Id$ tel que $u_{|H} = Id_H$. les propriétés suivantes sont équivalentes :

i) $Det(u) = \lambda \neq 1$

ii) u est diagonalisable et admet une valeur propre différente de 1

iii) $Im(u - Id) \nsubseteq H$

iv) Il existe une base B de E telle que $Mat_B(u) = \begin{pmatrix} 1 & & (0) & \\ & \ddots & & (0) \\ (0) & & 1 & \\ & (0) & & \lambda \end{pmatrix}$

On dit que u est une **dilatation**, d'hyperplan H et de droite $D = Im(u - \lambda Id)$

5.1.2 Proposition

Soit H un hyperplan de E, $u \neq Id$ tel que $u_{|H} = Id_H$. les propriétés suivantes sont équivalentes :

i) $Det(u) = 1$

ii) u n'est pas diagonalisable

iii) $\exists a \neq 0$, $a \in H$, $u(x) = x + f(x).a$

iv) Il existe une base B de E telle que $Mat_B(u) = \begin{pmatrix} 1 & & (0) & \\ & \ddots & & \\ (0) & & 1 & 1 \\ & (0) & & 1 \end{pmatrix}$

On dit que u est une **transvection**, d'hyperplan H et de droite $D = Im(u - Id)$

Lemme : Soit $f \in E^*$ et $a \in Ker(f)$, $a \neq 0$. Posons $\tau(a, f) = x + f(x).a$. Alors, $\tau(a, f)^{-1} = \tau(-a, f)$, et $\forall u \in GL(E)$, on a $u\tau(a, f)u^{-1} = \tau(u(a), f \circ u^{-1})$.

5.1.3 Corollaire 1

Le centre de $GL(E)$ est $Z = \{\lambda Id, \lambda \in \mathbb{K}^*\}$, et le centre de $SL(E)$ est $Z \cap SL(E) = \{\lambda Id, \lambda \in \mathbb{K}^*, \lambda^n = 1\}$

5.1.4 Théorème

Les transvections engendrent $SL(E)$ et les transvections et les dilatations engendrent $GL(E)$

Lemme : Soient x,y non colinéaires, alors il existe une transvection qui transforme x en y.

5.2 Conjuguaisons et commutateurs

5.2.1 Proposition

i) Deux dilatations de GL(E) sont conjuguées dans GL(E) si et seulement si elles ont le même déterminant

ii) Deux transvections de SL(E) sont conjuguées par un élément de GL(E). Si $n \geq 3$, alors elles sont conjuguées dans SL(E)

5.2.2 Théorème

i) $D(GL_n(\mathbb{K}) = SL_n(\mathbb{K})$, sauf si $n = 2$, $\mathbb{K} = F_2$

ii) $D(SL_n(\mathbb{K}) = SL_n(\mathbb{K})$, sauf si $n = 2$, $\mathbb{K} = F_2$ ou $\mathbb{K} = F_3$

5.2.3 Théorème

PSL_n est simple, saduf dans deux cas exceptionnels, $PSL_2(F_2) \simeq S_3$, et $PSL_2(F_3) \simeq A_4$

5.3 Cas $n = 2$

On pose $G = SL_2(F)$, on note $B = \{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, a \in F^*, b \in F\}$

$A = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, a \in F\}$

$C = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in F\}$

$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $U^- = \{\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}, b \in F\}$

5.3.1 Proposition

$B = AU = UA$, et $U \lhd B$, et $G = B \sqcup BwB$ (décomposition de Bruhat)

5.3.2 Corollaire

B est un sous groupe maximal de $SL_2(F)$ **Lemme :**$SL_2(F)$ est engendré par U et U^-

5.3.3 Théorème

Si $|F|\geq 4$, alors $PSL_2(F)$ est simple. **Lemme :**Soit Z le centre de $SL_2(F)$, alors $Z = \underset{g\in SL_2(F)}{\cap} gBg^{-1}$

5.3.4 Proposition

Soit $H \subset SL_2(F)$ un sous groupe distingué. Alors, soit $H \subset Z$, soit $H = SL_2(F)$

Isomorphismes exceptionnels

On suppose que $\mathbb{K}$ est un corps quelconque de caractéristique $p > 0$, donc $|\mathbb{K}|= q = p^k$, où $k \in \mathbb{N}^*$

5.3.5 Proposition

i) $|GL_n(\mathbb{K})|= (q^n - 1)(q^n - q)...(q^n - q^{n-1})$

ii) $|SL_n(\mathbb{K})|=|PGL_n(\mathbb{K})|= \frac{GL_n(\mathbb{K})}{|\mathbb{K}^*|} = (q^n - 1)(q^n - q)...(q^n - q^{n-2})q^{n-1}$

iii) $|PSL_n(\mathbb{K})|= \frac{SL_n(\mathbb{K})}{d}$, où $d = n \wedge q - 1$

5.3.6 Proposition

Soit F_q le corps à q éléments, on a les isomorphismes dits exceptionnels suivants :

i) $GL_2(F_2) = SL_2(F_2) = PGL_2(F_2) = PSL_2(F_2) \simeq S_3$

ii) $PGL_2(F_3) \simeq S_4$, $PSL_2(F_3) \simeq A_4$

iii) $PGL_2(F_4) = PSL_2(F_4) \simeq A_5$

iv) $PGL_2(F_5) \simeq S_5$, $PSL_2(F_5) \simeq A_5$