103
Conjugaison dans un groupe. Exemples de sous groupes distingués et de groupes quotients. Applications.

Refs : [Perr] Perrin Algèbre [Gou1] Gourdon Algèbre. [Ulm] Ulmer Théorie des groupes.

Devts :
62 Isomorphismes exceptionnels
51 Théorème de Sylow
69 Table carac et ssgp dist)
70 Table $\mathfrak{S}_4$.

Cadre : On fixe $(G,\cdot)$ un groupe, $H \leqslant G$ un sous groupe, $\varphi : G \to G'$ un morphisme de groupes.

I. Actions par conjugaison.

1) Conjugaison, classes de conjugaison.

[Perr] 15.

Déf 1 : Soit $g \in G$, l'application $G \to G$ définie par $h \mapsto ghg^{-1}$ est un automorphisme (dit intérieur) noté γ_g. L'application $G \to \mathrm{Aut}(G)$ qui à g associe γ_g est un morphisme de groupes, qui munit donc G d'une action de G : l'action par conjugaison.

Not 2 : Les orbites sous cette actions sont les classes de conjugaison. Le stabilisateur de $a \in G$ est noté $C_G(a) = \{g \in G \mid ga = ag\}$.

Ex 3 : Dans le cas où G est abélien, l'action par conjugaison est triviale.

Prop 4 : L'ensemble $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ est un sous groupe de G : l'action de G sur ses sous groupes par conjugaison est bien définie. Le stabilisateur de H sous cette action sera noté $N_G(H)$ le normalisateur de H.

Déf 5 : Le noyau du morphisme $g \mapsto \gamma_g$ associé à l'action par conjugaison est le centre de G, donné par $Z(G) = \{g \in G \mid ghg^{-1} = h\ \forall h \in G\}$.

2) Deux exemples de classification

A) Groupe symétrique

[Perr] 15/16

Prop 6 : Si $\sigma \in \mathfrak{S}_n$ est un p-cycle, $\sigma = (i_1 \dots i_p)$ et $\tau \in \mathfrak{S}_n$. On a
$$\tau\sigma\tau^{-1} = (\tau(i_1) \dots \tau(i_p))$$
En particulier tous les p-cycles sont conjugués dans $\mathfrak{S}_n$.

Cor 7 : Si $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Cor 8 : Les classes de conjugaisons de $\mathfrak{S}_n$ sont caractérisées par le type dans la décomposition en produits de cycles à supports disjoints.

B) Matrices sur un corps

Fixons k un corps. L'action de $GL_n(k)$ sur lui même par conjugaison s'étend en une action sur $\mathcal{M}_n(k)$. Qui correspond au changement de base : Deux matrices A et B sont conjuguées si et seulement si elles représentent un même endomorphisme de k^n dans deux bases.
On peut chercher à raffiner ce résultat (le rendre plus pratiquable)

[Gou1] 290 - 292

Théo 9 : Soit E un k-espace vectoriel de dimension n et $f \in \mathcal{L}(E)$. Il existe une suite $F_1 \dots F_r$ de sous espaces de E, f-stables. Telle que :
- $E = F_1 \oplus \dots \oplus F_r$
- $\forall i \in [\![1, r]\!]$, $f_i := f_{|F_i}$ est cyclique
- Si P_i est le polynome minimal de f_i on a $P_i \mid P_{i+1}$ pour $i \leqslant r-1$.

La suite des P_i ne dépend que de f. On l'appelle la suite des invariants de similitudes de f.

Cor 10 : Deux matrices de $\mathcal{M}_n(k)$ sont conjuguées si et seulement si elles représentent dans la base canonique de k^n des endomorphismes ayant mêmes invariants de similitude.

Rq 11 : Dans le cas d'un corps algébriquement clos. Une autre classification est donnée par la réduite de Jordan.

[Perr] 147

Théo 12 : (Matrice orthogonale sur $\mathbb{R}$) Soit $M \in O_n(\mathbb{R})$. M est conjuguée à une unique matrice de la forme suivante (Fig 1). Avec $p+q+2r = n$, $\theta_i \in]0, 2\pi[$ formant une suite croissante (p,q dit ?)
+ utilité : diagonalisation

2) Sous-groupes distingués.

[Perr] 9-12.

Déf 13 : On dit que H est distingué (ou normal) dans G si $N_G(H) = G$. Autrement dit si $\forall g \in G$, $gHg^{-1} = H$. On notera alors $H \trianglelefteq G$.

Ex 14 : Les sous groupe $\{1\}$ et G sont toujours distingués. $Z(G)$ est toujours distingué dans G.

Rq 15 : Si G est abélien, tous ces sous groupes sont distingués.

Ex 16 : La réciproque est fausse : le groupe des quaternions ne possède que des groupes distingués, sans être abélien.

Ex 17 : $H \trianglelefteq K$ et $K \trianglelefteq G \not\Rightarrow H \trianglelefteq G$. Par exemple, en notant $H = \langle (12)(34) \rangle$, $K = \langle (12)(34), (13)(24), (14)(23) \rangle$ on a $H \trianglelefteq K$, $K \trianglelefteq \mathfrak{S}_4$ mais pas $H \trianglelefteq \mathfrak{S}_4$. En particulier il existe des sous-groupe non normaux

Prop 18 : Si $H' \trianglelefteq G'$, alors $\varphi^{-1}(H') \trianglelefteq G$, en particulier, $\mathrm{Ker}\,\varphi \trianglelefteq G$. Réciproquement, si φ est surjectif, et $H \trianglelefteq G$, alors $\varphi(H) \trianglelefteq G'$.

Ex 19 : On a $SO_n(\mathbb{R}) \trianglelefteq O_n(\mathbb{R})$, $SL_n(E) \trianglelefteq GL_n(E)$.

Prop 20 : Un sous groupe d'indice 2 est distingué.

II. Groupes quotients. Groupes produits.

1) Groupes quotients

[Ulm] 60, 63, 61

Def 21 : Le groupe G est naturellement muni de deux actions de H, respectivement à gauche et à droite. Les orbites sous ces actions sont les classes à droite (resp. à gauche) modulo H, on note $H \backslash G$ et G/H les classes à droite (resp. à gauche).

On cherche à munir G/H d'une loi de groupe, telle que la projection canonique $\pi : G \to G/H$ soit un morphisme de groupes. On doit poser $(g.H)(g'H) = gg'H$.

Théo 22 : On a équivalence entre.

- La loi ci-dessus est une loi de groupe
- $\forall g \in G,\ gH = Hg$
- $H \trianglelefteq G$
- $\exists\, \varphi : G \to G'$ un morphisme avec $H = \operatorname{Ker} \varphi$.
- La suite de morphismes $1 \to H \to G \to G/H \to 1$ est alors une suite exacte courte.

Théo 23 (Propriété universelle du quotient) Soient $H \trianglelefteq G$, $\pi : G \to G/H$ la projection canonique. Si $H \trianglelefteq \operatorname{Ker} \varphi$, alors $\exists!\, \bar{\varphi} : G/H \to G'$ tel que $\bar{\varphi}\pi = \varphi$:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "\varphi"'] & G/H \arrow[dl, "\bar{\varphi}"] \\ G' & \end{tikzcd}$$

Théo 24 : On a un isomorphisme $\bar{\varphi} : G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$ envoyant $g \operatorname{Ker}\varphi$ sur $\varphi(g)$: Tout morphisme induit une suite exacte courte $1 \to \operatorname{Ker}\varphi \to G \to \operatorname{Im}\varphi \to 1$.

Ex 25 : $k^* \simeq GL_n(k)/SL_n(k)$. $\mathbb{Z}/2\mathbb{Z} \simeq (\{\pm 1\}, \cdot) \simeq O_n(\mathbb{R})/SO_n(\mathbb{R})$.

Appl 26 : Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Prop 27 : La projection canonique π induit une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H.

Ex 28 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ où $d \mid n$.

Théo 29 : (3^e théorème d'isomorphie) Soient $K \leq H \leq G$ trois groupes. Avec $K \trianglelefteq G$, $H \trianglelefteq G$. Alors on a un isomorphisme $(G/K)/(H/K) \simeq (G/H)$. (Voir Fig 2).

2) Produits de groupes et suites exactes.

[Perr] 20-21

Def 30 : Soient N et H deux groupes. Le produit direct $N \times H$ est le produit cartésien de N et H, muni de la loi produit $(n, h).(n', h') = (nn', hh')$. On note ι_N, ι_H (resp π_N, π_H) les injections (resp projections) canoniques.

Prop 31 : On a $\pi_N \circ \iota_N = Id_N$ et $\pi_H \circ \iota_H = Id_H$. On a donc une suite exacte courte

$$1 \to N \xrightarrow{\iota_N} N \times H \xrightarrow{\pi_H} H \to 1 \qquad (\text{car } N \times \{1\} = \operatorname{Ker} \pi_H).$$

où ι_N et π_H sont scindés.

Prop 32 : Si $1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$ est une suite exacte courte, où p et i sont scindés, alors $G \simeq N \times H$.

Théo 33 (Restes Chinois) Si m et n sont premiers entre eux. Alors $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Rq 34 : Si N, G, H sont abéliens dans la prop 32. Il suffit d'avoir p scindé ou i scindé pour avoir le résultat. Ce qui est faux dans le cas général.

[Perr] 21-23

Def 35 : Soient N, H deux groupes, H agissant sur N par automorphismes. On définit sur $N \times H$ (produit cartésien) une loi de groupe par

$$(n, h)(n', h') := (n(h.n'), hh')$$

On note $N \rtimes H$ le groupe obtenu, c'est le produit semi-direct de N par H.

Rq 36 : Si $\varphi : H \to \operatorname{Aut}(N)$ est le morphisme structurel de l'action de H sur N, on pourra noter $N \rtimes_\varphi H$ pour mettre l'emphase sur l'action.

On a deux morphismes $N \to N \rtimes H$ et $N \rtimes H \to H$ d'où une suite exacte courte $1 \to N \to N \rtimes H \to H \to 1$. On a aussi $\bar{H} = \{(1, h) \mid h \in H\} \simeq H$ une copie de H dans $N \rtimes H$. Mais dans un produit semi-direct général, cette copie n'est pas distinguée.

Prop 34 : Si N, H et $N \rtimes H$ sont abéliens alors l'action de H sur N est triviale et $N \rtimes H = N \times H$

Théo 35 : Soient G, N, H trois groupes. Il y a équivalence entre

- $G \simeq N \rtimes H$
- Il existe une suite exacte courte $1 \to N \to G \xrightarrow{p} H \to 1$ où p est scindé.

Ex 36 : On a $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$. $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. $GL_n(k) \simeq SL_n(k) \rtimes \{\pm 1\}$.

III. Groupes et sous groupes remarquables.

→ classes de conjugaison

1) Groupes simples.

Def 37 : Un groupe G est dit simple s'il n'admet pas de sous-groupe distingué non trivial et $G \neq \{1\}$.

Ex 38 : $\mathbb{Z}/n\mathbb{Z}$ est simple si et seulement si n est premier, ce sont les seuls exemples de groupes abéliens simples.

[Perr] 99-107

Prop déf 39 Fixons k un corps. On a $Z(GL_n(k)) = \{\lambda I_n \mid \lambda \in k^*\}$ et $Z(SL_n(k)) = SL_n(k) \cap Z(GL_n(k))$. On définit alors $PSL_n(k) = SL_n(k)/Z(SL_n(k))$ et $PGL_n(k) = GL_n(k)/Z(GL_n(k))$.

Prop 40 : Le groupe $PGL_n(k)$ opère fidèlement sur l'ensemble $\mathbb{P}^{n-1}(k)$ des droites vectorielles de k^n.

Théo 41 : Le groupe $PSL_n(k)$ est simple sauf dans les deux cas suivants :

- $n = 2$ et $k = \mathbb{F}_2$
- $n = 2$ et $k = \mathbb{F}_3$.

Théo 42 : On a les isomorphismes de groupes suivants :

(a) $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) = \mathfrak{S}_3$

(b) $PGL_2(\mathbb{F}_3) = \mathfrak{S}_4$ et $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$

(c) $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$

(d) $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ et $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

DVP

[Perr] 28.

Théo 43 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Cor 44 : Le seul sous-groupe distingué non trivial de $\mathfrak{S}_n$ est $\mathfrak{A}_n$ pour $n \geq 5$.

2) p-groupes et théorèmes de Sylow.

Def 45 : Soit G un groupe fini, on dit que G est un p-groupe si son ordre est une puissance non triviale de p.

[Ulm] 67-70

Prop 46 : Soit G un p-groupe agissant sur X un ensemble non vide, on a $|X| \equiv |X^G| [p]$.

Co 47 : Le centre d'un p-groupe est non trivial.

Co 48 : Tout groupe d'ordre p^2 est abélien, isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^2$.

[Per] 18-20

Def 49 : Soit G un groupe fini de cardinal mp^α où $\alpha \geq 1$ et $p \wedge m$. On appelle p-sous groupe de Sylow (ou p-Sylow) de G tout sous groupe de G d'ordre p^α.

On fixe pour cette partie G un groupe d'ordre mp^α où $\alpha \geq 1$ et $p \wedge m$.

Prop 50 : Un sous groupe H de G est un p-Sylow si et seulement si c'est un p-groupe dont l'indice est premier à p.

Théo 51 (Sylow) En notant $Syl_p(G)$ l'ensemble des p-Sylow de G, on a

- $Syl_p(G) \neq \emptyset$.
- Pour $H \leq G$ un p groupe et $S \in Syl_p(G)$. H est inclus dans un conjugué de S. En particulier tous les éléments de $Syl_p(G)$ sont conjugués — DVP
- $|Syl_p(G)| \equiv 1 [p]$ et $|Syl_p(G)| \mid m$.

Co 52 Un p-sylow de G est distingué si et seulement si $|Syl_p(G)| = 1$.

Co 53 : Un groupe d'ordre $200m$ n'est pas simple.

Co 54 : Un groupe d'ordre pq, où $p<q$ sont premiers et $q \not\equiv 1 [p]$ est cyclique.

IV. Représentations linéaires et sous groupes distingués.

[Ulm] 143-150

Def 55. Soit G un groupe fini, une représentation (linéaire complexe) du groupe G est un morphisme $\rho : G \to GL(V)$ où V est un $\mathbb{C}$-espace vectoriel de dimension finie. La dimension de V est le degré de la représentation.
Une représentation ρ de G est dite fidèle si $\ker \rho = \{1\}$.

Ex 56 : Le morphisme trivial $G \to \mathbb{C}^*$ est la représentation triviale.
Si $\varphi : G \to \mathfrak{S}_n$ est un morphisme, et V un $\mathbb{C}$-espace vectoriel de base $(v_1 \dots v_n)$ en posant $g.v_i = v_{\varphi(g)(i)}$. On obtient une représentation par permutations de G.
En particulier, G agissant sur lui même par translation à gauche donne une rep dite régulière.

Prop def 57 Si $\rho_1 : G \to GL(V_1)$ et $\rho_2 : G \to GL(V_2)$ sont deux représentations. On définit des représentations en posant

$\rho_1 \oplus \rho_2 : G \to GL(V_1 \oplus V_2)$, $g.(v_1 \oplus v_2) = g v_1 \oplus g v_2$

$\rho_1 \otimes \rho_2 : G \to GL(V_1 \otimes V_2)$, $g.(v_1 \otimes v_2) = g.v_1 \otimes g.v_2$

[Ulm] 143-150

Def 58 : Soit $\rho_1 : G \to GL(V_1)$ et $\rho_2 : G \to GL(V_2)$ deux représentations de G.

- Un morphisme de représentations est une application linéaire $V_1 \to V_2$ telle que $\forall x \in V_1$, $g.\varphi(x) = \varphi(g.x)$.
  On notera $Hom_G(V_1, V_2)$ l'ensemble des tels morphismes.
- Une sous représentation est un sous espace vectoriel stable sous l'action de G.

Ex 59 : La représentation régulière admet la représentation triviale comme sous représentation.

Def 60 : Une représentation irréductible est une représentation sans sous représentation non triviale.

Théo 61 (Maschke) Toute représentation est somme directe de représentations irréductibles.

2) Caractères de groupes finis

On fixe $\rho : G \to GL(V)$ une représentation de G.

[Ulm] 150-160

Def 62 : On appelle caractère de ρ la fonction $\chi : G \to \mathbb{C}$, composition de ρ par la trace.

Prop 63 : Si ρ_1 et ρ_2 sont deux représentations, on a $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$ et $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \times \chi_{\rho_2}$.

Def 64 : Un caractère irréductible est le caractère d'une représentation irréductible.
Une fonction centrale sur G est une fonction $G \to \mathbb{C}$ constante sur les classes de conjugaison.

Théo 65 : • Les caractères sont des fonctions centrales.

- La formule $\langle \phi, \psi \rangle = |G|^{-1} \sum_{g \in G} \phi(g) \overline{\psi(g)}$ définit un produit scalaire hermitien sur les fonctions centrales. Les caractères irréductibles forment une base orthonormée pour ce produit.
- Il y a autant de caractères irréductibles que de classes de conjugaison de G.
- Deux représentations sont isomorphes si et seulement si elles ont même caractère.
- χ est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$.

On peut alors construire la table de caractères d'un groupe fini, qui regroupe les classes de conjugaison de G et ses caractères irréductibles.

Ex 66 : Table de caractères des groupes non abéliens d'ordre 8.

Prop 67 : Si $C_1 \dots C_m$ sont les classes de conjugaison de G. Et $\chi_1 \dots \chi_m$ ses caractères irréductibles, on a $\sum_{i} \chi_i(C_k) \overline{\chi_i(C_l)} = \delta_{k,l} \frac{|G|}{|C_k|}$.

Def 68 : Soit G un groupe et χ un caractère, on appelle noyau de χ l'ensemble $\{g \in G \mid \chi(g) = \chi(1)\}$. C'est aussi le noyau de ρ.

Prop 69 : Les sous groupes distingués de G sont les intersections de noyaux de caractères irréductibles de G — DVP

Appli 70 Table et sous groupes distingués de $\mathfrak{S}_4$. — DVP

Fig 1 $\begin{pmatrix} I_p & & & & 0 \\ & -I_q & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_r} \end{pmatrix}$ $R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix}$

Fig 2 :
$$\begin{tikzcd} K \arrow[r, hook] \arrow[d, equal] & H \arrow[r, two heads] \arrow[d] & H/K \arrow[d] \\ K \arrow[r] & G \arrow[r, two heads] \arrow[d, two heads] & G/K \arrow[d] \\ & G/H \arrow[r, phantom, "\simeq"] & (G/K)/(H/K) \end{tikzcd}$$

(lignes et colonnes exactes).