103

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

Soit G un groupe.

I/ Conjugaison dans un groupe.

1) L'action par conjugaison.

Définition 1 : L'application $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$ définit une action de groupe de G sur lui-même, appelé action par conjugaison.

Définition 2 : L'orbite $\{ghg^{-1} / g \in G\}$ de $h \in G$ s'appelle sa classe de conjugaison et le stabilisateur de h s'appelle le centralisateur de h dans G et est noté $Z_G(h)$.

Exemple 3 : Dans S_3, les permutations $(1\,2\,3)$ et $(1\,3\,2)$ sont conjugués puisque $(1\,3\,2) = (1\,3)^{-1}(1\,2\,3)(2\,3)$

Définition 4 : Le centre d'un groupe G est le sous-groupe $Z(G) := \{h \in G \mid ghg^{-1} = h \ \forall g \in G\}$

Remarque 5 : Pour $h \in G$, on a $h \in Z(G) \Leftrightarrow G = Z_G(h)$

2) Exemple de classe de conjugaison

Proposition 6 : Si $\sigma \in S_n$, est un p-cycle, $\sigma = (a_1, \dots, a_p)$ et si $\tau \in S_n$ on a $\tau\sigma\tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$

Proposition 7 : Dans S_n, tous les p-cycles sont conjugués.

Proposition 8 : Les 3-cycles sont conjugués dans A_n.

Définition 9 : Soit $\mathbb{K}$ un corps. Deux matrices de $GL_n(\mathbb{K})$ sont semblables si elles sont conjuguées dans $GL_n(\mathbb{K})$.

Proposition 10 : $\forall A \in \mathcal{M}_n(\mathbb{C})$, A est semblable à A^T.

II/ Sous-groupes distingués et groupes quotients.

1) Sous-groupes distingués.

Définition 11 : Un sous-groupe H de G est dit distingué dans G si $\forall a \in G \ \forall h \in H$, $aha^{-1} \in H$. On note alors $H \triangleleft G$.

Exemple 12 : Le groupe $Z(G)$ est distingué dans G.

Remarque 13 : Si G est abélien, tout ses sous-groupes sont distingués.

Proposition 14 : Soit H un sous groupe de G. Il y a équivalence entre :

i) H est distingué

ii) $\forall g \in G$, $gH = Hg$.

Proposition 15 : Soit $\varphi : G \to H$ un morphisme de groupes. Alors $\ker(\varphi)$ est distingué dans G.

Exemple 16 : Le groupe $\{1, \sigma, \sigma^2\}$ où $\sigma = (a\,b\,c)$ est un sous groupe distingué de S_3.

2) Groupes quotients et théorèmes d'isomorphismes

Définition 17 : Soit H un sous-groupe de G. On définit la relation $\sim$ sur G par $x \sim y \Leftrightarrow xy^{-1} \in H$. L'ensemble des classes pour $\sim$ est noté G/H et est appelé le groupe quotient de G par H.

Définition 18: L'indice d'un sous groupe H de G est l'entier $[G:H] = |G/H|$.

Théorème 19: Soit H un sous groupe fini de G. Alors $|G| = [G:H] \times |H|$.

Proposition 20: Un sous-groupe H est distingué, si et seulement si H est le noyau d'un morphisme.

Théorème 21: Soit H un sous-groupe distingué de G. Alors G/H est muni d'une structure de groupe.

Exemple 22: $\forall n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe.

Remarque 23: La projection canonique $\pi : G \to G/H$ est un morphisme de groupe.

Théorème 24: (1er théorème d'isomorphisme) Soit $\varphi : G \to \Gamma$ un morphisme de groupes. Alors, il existe un isomorphisme

$$\bar{\varphi} : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi), \quad \bar{g} \mapsto \varphi(\bar{g})$$

De plus, si φ est surjectif, $\bar{\varphi}$ fournit un isomorphisme entre $G/\mathrm{Ker}(\varphi)$ et Γ.

Exemple 25: Un groupe cyclique fini G d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Théorème 26: (2ème Théorème d'isomorphisme) Soient K et H deux sous-groupes de G tels que H soit distingué dans G. Alors, il existe un isomorphisme $\frac{K}{H \cap K} \simeq \frac{HK}{H}$

Théorème 27: (3ème Théorème d'isomorphisme) Soit $K \subset H \subset G$ trois groupes tels que H et K soient distingués dans G. Alors, il existe un isomorphisme $G/H \simeq \frac{G/K}{H/K}$.

III / Groupes simples et p-groupes.

1) Les groupes simples

Définition 28: Un groupe est simple si ses seuls sous-groupes distingués sont $\{1\}$ et lui-même.

Exemple 29: $\mathbb{Z}/n\mathbb{Z}$ est simple $\iff$ n est premier.

Proposition 30 Les $\mathbb{Z}/p\mathbb{Z}$ où p premier sont les seuls groupes abéliens simples.

Lemme 31: Le groupe $\mathcal{A}_5$ est simple | D_1

Théorème 32: $\forall n \geq 5$, $\mathcal{A}_n$ est simple.

2) Les p-groupes et le théorème de Sylow.

Définition 33: Soit p un nombre premier. Un p-groupe est un groupe dont l'ordre est une puissance de p.

Proposition 34: Le centre d'un p-groupe est non trivial.

__Proposition 35__ : Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

__Définition 36__ : Soit G un groupe de cardinal n et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \nmid m$ on appelle p-sous groupe de Sylow de G un groupe de cardinal p^α.

__Exemple 37__ : Si $G = GL_n(\mathbb{F}_p)$ alors le sous-groupe $P = \{A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}$ est un p-sous groupe de Sylow de G.

__Théorème 38__ : (Sylow) Soit G un groupe fini et p un diviseur premier de $|G|$, alors G contient au moins un p-sous-groupe de Sylow.

__Lemme 39__ : Soit G un groupe d'ordre $n = p^\alpha m$ où $p \nmid m$ et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors, $\exists a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

__Théorème 40__ : (Sylow) Soit G un groupe, de cardinal $|G| = p^\alpha m$ où $p \nmid m$.

1) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$.

2) Les p-Sylow sont tous conjugués et leur nombre $k \mid n$.

3) On a $k \equiv 1\ [p]$ donc $k \mid m$.

__Application 41__ : Un groupe d'ordre 63 n'est pas simple.

Ulmer

Perrin.