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

On considère G un groupe noté multiplicativement et H un sous groupe de G.

1 Conjugaison dans un groupe

1.1 Notion de conjugaison

Proposition 1 (BER 130)**.** 1. Soit $g \in G$. L'application de G dans G définie par $Int_g : x \mapsto gxg^{-1}$ est un automorphisme de G.

2. De plus, l'application $g \mapsto Int_g$ est un morphisme de groupe de G dans $Aut(G)$.

Définition 2 (BER 130)**.** L'automorphisme précédent est appelé la conjugaison par g.

Notation 3 (BER 131)**.** Pour toute partie P de G et tout $g \in G$, on note gPg^{-1} l'image de P par Int_g, autrement dit $gPg^{-1} = \{gxg^{-1} | x \in P\}$

Proposition 4 (BER 131)**.** gPg^{-1} est fini si et seulement si P est fini. Dans ce cas, on a pour tout $g \in G$, $|gPg^{-1}| = |P|$.

Définition 5 (BER 131)**.** Deux éléments $x, x' \in G$ sont dits conjuguées dans G s'il existe $g \in G$ tel que $x' = gxg^{-1}$.

Définition 6 (BER 131)**.** On appelle classe de conjugaison de x dans G l'ensemble $Conj_G(x)$ des éléments de G conjugués à x, c'est-à-dire l'ensemble $Conj_G(x) = \{gxg^{-1} | g \in G\}$.

Proposition 7 (BER 132)**.** La relation "être conjugué dans G" est une relation d'équivalence. Les classes d'équivalences sont en faitles classes de conjugaison.

Exemple 8 (BER 132)**.** Si G est abélien, $Conj_G(x) = \{x\}$ pour tout $x \in G$.

1.2 Sous-groupe distingué

Définition 9 (BER 135)**.** On dit que H est distingué dans G si l'on a $ghg^{-1} \in H$ pour tout $h \in H$ et tout $g \in G$.

Exemple 10 (BER 136)**.** 1. Si G est abélien, tout sous-groupe de G est distingué.

2. $\{1\}$ et G sont toujours des sous-groupes distingués de G.

Proposition 11 (BER 139)**.** Soit $f : G \to G'$ un morphisme de groupes. Alors $Ker(f)$ est un sous-groupe distingué de G.

Remarque 12 (BER 139)**.** Pour démontrer qu'une partie H d'un groupe G est un sous-groupe distingué, on peut alors essayer de l'identifier au noyau d'un morphisme de groupes.

Exemple 13 (BER 139)**.** Soit E un $\mathbb{K}-$ev de dimension finie, où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. L'ensemble $SL(E)$ des automorphisme de E de déterminant 1 est un sous-groupe distingué de $GL(E)$ puisque c'est le noyau du morphisme déterminant $det : GL(E) \to \mathbb{K}^\times$.

Définition 14 (BER 140)**.** On dit qu'un groupe G est simple si $G \neq \{Id_G\}$ et si $\{1_G\}$ et G sont les seuls sous-groupes distingués de G.

Exemple 15 (BER 140)**.** $GL(E)$ n'est pas un groupe simple, puisque l'on a vu que $SL(E)$ est un sous-groupe distingué dans $GL(E)$.

2 Groupe Quotient

2.1 Prérequis

Notation 16 (BER 145)**.** Pour $a \in G$, on note $aH = \{ah | h \in H\}$ et $Ha = \{ha | h \in H\}$

Proposition 17 (BER 145)**.** La relation $\sim$ sur G définie par $x \sim y \iff x^{-1}y \in H$ est une relation d'équivalence. De plus, on a $\overline{x} = xH$ pour tout $x \in G$.
Ainsi, on associe à un sous-groupe H la relation d'équivalence précédentes.

Exemple 18 (BER 146)**.** Considérons le groupe $\mathbb{Z}$ et un de ses sous-groupe $n\mathbb{Z}$, où $n \in \mathbb{N}$. La relation d'équivalence associée à H est enfaite la relation de congruence modulo n.

Définition 19 (BER 145)**.** Un ensemble de la forme xH, $x \in G$ est appelé une classe à gauche modulo H. L'ensemble de ces classes à gauche est noté G/H.

Exemple 20 (BER 146)**.** Reprenons l'exemple précédent. La classe à gauche d'un élément $x \in \mathbb{Z}$ est l'ensemble $x + n\mathbb{Z}$.

Proposition 21 (BER 146)**.** Les classes à gauche de G modulo H sont les classe d'équivalence de la relation défini à la proposition 17 et forment alors une partition de G.

Définition 22 (BER 146)**.** Le nombre de classes à gauche modulo H, lorsqu'il est fini, est appelé l'indice de H dans G et est noté $[G : H]$. Si G/H est un infini, on pose $[G : H] = +\infty$.

Exemple 23 (BER 146)**.** L'ensemble quotient de notre est donc $\mathbb{Z}/n\mathbb{Z}$. Si $n > 0$, on a donc $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$. En revanche $[\mathbb{Z} : 0\mathbb{Z}] = +\infty$.

2.2 Autre vision des sous-groupe distingué

Ces notions permettent de donner une autre caractérisation des sous-groupes distingués

Proposition 24 (BER 147)**.** LASSE :

1. H est distingué dans G
2. $\forall x \in G, xH = Hx$
3. $\forall x \in G, xHx^{-1} = H$, où $xHx^{-1} := \{xhx^{-1} | h \in H\}$

Proposition 25 (BER 147)**.** Tout sous groupe d'indice 2 est distingué dans G.

Théorème 26 (BER 148)**.** [Lagrange] Supposons que G soit un groupe fini. Alors, on a

$$|G| = [G : H]|H|$$

En particulier, $|H|$ divise $|G|$.

Avoir en tête réciproque fausse car A_4 pas de sous groupe d'ordre 6

2.3 Groupe quotient

On suppose dans cette partie que H est un sous-groupe distingué de G.

Proposition 27 (BER 237)**.** La loi interne $(\overline{x}, \overline{y}) \in G/H \times G/H \mapsto \overline{xy} \in G/H$ est bien définie, de neutre $\overline{1_G}$, et induit sur G/H une structure de groupe. De plus, l'application $\pi : x \mapsto \overline{x}$ est un morphisme de groupes.

Définition 28 (BER 237)**.** [blabla : la proposition motive la définition et l'appellation suivante] Le groupe G/H est appelé le groupe quotient de G par H.

Proposition 29 (BER 237)**.** Pour tout $x \in G$, on a $\overline{x} = \overline{1_G} \iff x \; in H$.

Exemple 30 (BER 238)**.** Soit $n \leq 1$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

Proposition 31 (BER 238)**.** La projection canonique $\pi : G \to G/H$ est surjective, de noyau H.

Théorème 32 (BER 239)**.** Soit $f : G \to G'$ un morphisme de groupes tel que $H \subset Ker(f)$. Alors, il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $f = \overline{f} \circ \pi$ (cf annexe).

Théorème 33 (BER 241)**.** [théorème d'isomorphisme] Soient G, G' deux groupes et soit $f : G \to G'$ un morphisme de groupes. Alors le morphisme de groupes $\overline{f} : G/Ker(f) \to G'$ induit un isomorphisme de groupes $G/Ker(f) \simeq Im(f)$

Méthode 34 (BER 241)**.** Ce théorème nous permet d'identifier un groupe quotient G/H à un groupe connu. On essaye tout d'abord d'identifier H à un morphisme de groupe $f : G \to G'$, et on calcule ensuite l'image de f.

Exemple 35 (BER 241)**.** Cherchons à identifier $\mathbb{C}^\times/\mathbb{U}$. Pour cela remarquons que $\mathbb{U} = ker(f)$ où $f : z \mapsto |z|$ qui est un morphisme de groupes surjectif de $C^\times$ dans $\mathbb{R}_+^\times$. Le théorème précédent nous donne donc $C^\times/\mathbb{U} \simeq \mathbb{R}_+^\times$.

Exemple 36 (BER 241)**.** De même, en considérant le morphisme $f : \theta \in \mathbb{R} \mapsto e^{i\theta} \in \mathbb{U}$, on trouve que $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.

Remarque 37 (No ref)**.** Dans les exemples on a omis une vérification. Pour utiliser le théorème d'isomorphisme il faut que le sous groupe soit distingué. Cependant ici, cela ne pose pas de problème car $\mathbb{C}^\times$ et $\mathbb{R}$ sont des groupes commutatifs et tout leurs sous-groupe sont donc distingués.

2.4 Exemple du centralisateur et application

Définition 38 (BER 136)**.** Le centre d'un groupe est l'ensemble

$$Z(G) = \{z \in G | zg = gz, \forall g \in G\}$$

Remarque 39 (BER 136)**.** $Z(G) = G \iff G$ est abélien

Proposition 40 (BER 136)**.** $Z(G)$ est un sous-groupe distingué de G.

Application 41 (CAL 2)**.** [DEV 1] Soit G un groupe d'ordre n et $Z(G)$ son centre. On note p_G la probabilité que deux éléments h, g de G choisis indépendamment et de façon équiprobable commutent.

1. Si G est non abélien, $p \leq \frac{5}{8}$
2. Si k est le nombre de classe de conjugaison, alors $p = \frac{k}{n}$

3 L'exemple des permutations

Considérons E un ensemble à $n \leq 1$ éléments.

3.1 Prérequis essentielles

Définition 42 (BER 201)**.** L'ensemble des bijections de E sur lui-même est un groupe pour la composition des applications, appelé groupe des permutations de E ou groupe symétrique sur E, et est noté $\mathfrak{S}(E)$. Un élément de $\mathfrak{S}(E)$ est appelé une permutation.

Théorème 43 (BER 204)**.** [DEV bonus] Soit $\sigma \in \mathfrak{S}(E)$. Alors σ se décompose en produit de cycles à support disjoints, et cette décomposition est unique à l'ordre des facteurs près. Cette décomposition est donnée par : $\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega$ où Ω^* représente l'ensemble des σ-orbites non réduite à un singleton.

Corollaire 44 (BER 206)**.** $\mathfrak{S}(E)$ est engendré par les cycles.

Corollaire 45 (BER 207)**.** $\mathfrak{S}(E)$ est engendré par les transpositions.

3.2 Conjugaison dans $\mathfrak{S}(E)$

Définition 46 (BER 211)**.** Soit $n \geq 1$. Une partition de n est une suite d'entier $p = (p_k)_k$ décroissante, nulle à partir d'un certain rang, telle que $\sum_{k \geq 1} p_k = n$. On note $P(n)$ l'ensemble de ces partitions.

Définition 47 (BER 211)**.** Soit $\sigma \in \mathfrak{S}(E)$. Le type de σ est la partition de n dont les éléments non nuls sont les cardinaux des diverses $\sigma-$orbites, rangés par ordre décroissant. On la note p_σ

Exemple 48 (BER 211)**.** Si $\sigma = (13)(4765) \in \mathfrak{S}_9$, on a $p_\sigma = (4, 2, 1, 1)$.

Proposition 49 (BER 211)**.** Deux permutations de $\mathfrak{S}(E)$ sont conjuguées si et seulement si elles sont de même type.

Corollaire 50 (BER 212)**.** Notons C_E l'ensemble des classes de conjugaison de $\mathfrak{S}(E)$. L'application $\Phi : p \in \mathcal{P}(n) \mapsto Conj_{\mathfrak{S}(E)}(\sigma_p) \in C_E$ est une bijection de l'ensemble des partitions de n sur l'ensemble des classes de conjugaison de $\mathfrak{S}(E)$.

Méthode 51 (BER 212)**.** Pour trouver toutes les classes de conjugaison de $\mathfrak{S}(E)$, il suffit donc de décomposer n en somme d'entiers strictement positifs décroissants de toutes les façons possibles.

Exemple 52 (BER 212)**.** $\mathfrak{S}_4$ possède cinq classes de conjugaison distinctes représentées par (1234), (123), $(12)(34)$, (12), Id

3.3 Le groupe alternée et simplicité

Définition 53 (ROM 46)**.** On définit la signature de σ par l'élément $\epsilon(\sigma) = (-1)^r$, où r est le nombre de transposition dans la décomposistion en transposition de σ.

Proposition 54 (un peu ROM 47, BER 213)**.** La signature est un morphisme.

Définition 55 (BER 215, ROM 49)**.** Le groupe alterné, noté $\mathfrak{A}(E)$, est l'ensemble des permutations de $\mathfrak{S}(E)$ de signature 1.

Proposition 56 (BER 215)**.** $\mathfrak{A}(E)$ est un sous groupe distingué de $\mathfrak{S}(E)$ comme noyau du morphisme signature. On a donc $[\mathfrak{S}(E) : \mathcal{A}(E)] = 2$.

Corollaire 57 (BER 140)**.** $\mathfrak{S}(E)$ n'est donc pas simple pour $n \geq 3$.

Lemme 58 (BER 216)**.** Soit E un ensemble à n éléments. Si $n \geq 3$, le groupe alterné $\mathfrak{A}(E)$ est engendré par chacune des familles suivantes :

1. les produits de deux transpositions
2. les 3-cycles.

Théorème 59 (BER 217, ROM 50)**.** [DEV 2] Soit E un ensemble à $n \geq 3$ éléments. Montrer que le groupe alterné $\mathfrak{A}(E)$ est simple si et seulement si $n \neq 4$.