

103: Exemples et applications des notions de sous-groupes distingués et de groupes quotients.

Pierre Lissy

March 4, 2010

1 Définitions et premières propriétés

1.1 Sous-groupe distingué

Définition 1. Un sous-groupe est dit distingué ssi il est stable par automorphismes intérieur, ie $g^{-1}Hg \subset H$ pour tout g . Il est dit caractéristique ssi il est stable par tout automorphisme du groupe. Un sous-groupe caractéristique est distingué.

Exemple 1. Le sous-groupe formé des doubles permutations dans S_4 est distingué. Le groupe spécial linéaire est distingué dans $GL(E)$.

En général un sous-groupe n'est pas distingué.

Exemple 2. Le groupe engendré par un p – cycle n'est jamais distingué. Le groupe engendré par I dans le groupe des quaternions n'est pas distingué.

Définition-proposition 1. On appelle centre d'un groupe l'ensemble des éléments qui commutent avec tous les autres, noté $Z(G)$. C'est un sous-groupe caractéristique de G .

Exemple 3. 1. Le centre des endomorphismes (ou des matrices) sont les homothéties.

2. Le centre de S_n (resp A_n) est trivial

3. Le centre du groupe diédral D_n avec n pair est $\{Id, -Id\}$, avec n impair il est trivial

4. Le centre du groupe des quaternions est $\{1, -1\}$.

Définition-proposition 2. On appelle groupe dérivé (ou groupe des commutateurs) le sous-groupe engendré par les commutateurs, noté $D(G)$. C'est un sous-groupe caractéristique de G , et c'est même le plus petit groupe tel que $G/D(G)$ est abélien.

Exemple 4. 1. Le groupe dérivé d'un groupe com est trivial

2. Le groupe dérivé de S_3 est le groupe du 3-cycle.

3. Le centre du groupe diédral est le groupe engendré par le carré de la rotation élémentaire cf [1]

4. Le groupe dérivé des quaternions est $\{1, -1\}$.

1.2 premières propriétés

Proposition 1. Si H est distingué, et K sous-groupe, alors KH et HK sont des sous-groupes. De plus, si K est distingué alors HK aussi.

Définition-proposition 3. Normalisateur d'un sous-groupe = stabilisateur de H pour la relation de conjugaison. C'est un sous-groupe de G , le plus grand sous-groupe dans lequel H est distingué. Si K est un sous-groupe de H distingué il est donc inclus dans $N_G(H)$. Si K est un sous-groupe de N_H , alors KH est un groupe de H est distingué dans KH .

1.3 Critères de distinction

Proposition 2. *Le noyau d'un morphisme est toujours distingué.*

Proposition 3. *Un sous-groupe d'ordre 2 est toujours distingué.*

Exemple 5. A_n est distingué dans S_n . Le groupe des rotations de D_n est distingué dans D_n .

Proposition 4. *Un sous-groupe caractéristique d'un sous-groupe distingué dans G est lui-même distingué.*

Un sous-groupe distingué d'un sous-groupe distingué n'est pas forcément distingué.

Exemple 6. *Le groupe des doubles transpositions, et un de ses sous-groupes d'ordre 2 distincts.*

Remarque 1. *Dans un groupe abélien, tout sous-groupe est évidemment distingué.*

1.4 Groupe quotient

Rappel: on peut parler du quotient d'un groupe par un sous-groupe, c'est l'ensemble des classes d'équivalences pour la relation d'équivalence $xy^{-1} \in H$. On les prendra ici à droite mais ça serait pareil à gauche

Théorème 1. *Les propositions suivantes sont équivalentes:*

1. *La relation d'équivalence est compatible avec la loi de composition*
2. $xH = Hx$ pour tout x
3. H est distingué

Dans ce cas, le quotient G/H est un groupe et la surjection canonique est un morphisme de groupe.

Proposition 5. *Suite exacte: une suite de morphismes telle que le noyau de l'un et l'image du suivant. Alors Celui du milieu est isomorphe au quotient et celui de gauche s'injecte distinctement.*

Proposition 6. *Si on considère un morphisme de groupe f de G sur G' . Si H est un sous-groupe de G contenu dans le noyau de f on peut factoriser f de manière unique sur G/H en $\bar{f}$, ie $f \circ j = \bar{f}$ où j est la surjection canonique. Le noyau de $\bar{f}$ est $j(Ker(f))$ et l'image de $\bar{f}$ est égale à celle de f . Ce morphisme est un isomorphisme de $Im(f)$ sur $G/Ker(f)$.*

Application 1. *On a les isomorphismes suivants:*

1. $[2]$ H distingué dans G , K sous-groupe de G ; Alors $K/(H \cap K) \simeq HK/H$.
2. $[2]$ H distingué dans G , K sous-groupe distingué de G , $H \subset K$; Alors $G/K \simeq (G/H)/(K/H)$.
3. $[3]$ U et V , et u et v distingués. Alors $u(U \cap v)$ est distingué

Remarque 2. *Notamment si G' est un groupe abélien, on peut toujours factoriser par le groupe dérivé de G .*

Proposition 7. *Suite exacte: une suite de morphismes telle que le noyau de l'un et l'image du suivant. Alors celui du milieu est isomorphe au quotient et celui de gauche s'injecte distinctement.*

1.5 Groupes simples

Définition 2. *Un groupe est simple ssi ses seuls sous-groupes distingués sont lui même et le neutre.*

Exemple 7. *Les $\mathbb{Z}/p\mathbb{Z}$ avec p sont simples. Ce sont les seuls groupes abéliens finis simples.*

Proposition 8. *Toute morphisme de groupe d'un groupe simple vers un autre est soit injectif soit trivial*

Théorème 2. Les groupe A_n est simple

On a déjà vu que A_4 n'était pas simple.

Corollaire 1. les sous-groupes distingués de S_n sont lui-même, le neutre et A_n .

Corollaire 2. $D(S_n) = D(A_n) = A_n$.

Lemme 1. $PSL(2, \mathbb{F}_2) \simeq \mathcal{S}_3$,
 $PSL(2, \mathbb{F}_3) \simeq \mathcal{A}_4$.

Théorème 3. Le groupe $PSL_n(k)$ est simple sauf dans les deux cas précédents.

2 Produits directs, semi-direct et applications à la classification des groupes finis

2.1 Rappels théoriques

Théorème 4 (Sylow). Si $|G| = p^\alpha * m$, avec p premier et $\text{pgcd}(p, m) = 1$.

1. Il existe un sous-groupe d'ordre p^α , appelé sous-groupe d'ordre de Sylow
2. Deux sous-groupes d'ordre p^α sont conjugués (donc leur nombre divise n)
3. Le nombre de p -Sylow est un diviseur de m , congru à 1 modulo p
4. Tout p -sous-groupe est inclus dans un p -Sylow.

Proposition 9. Soit H et K deux groupes. On pose le groupe produit direct muni de $(h, k)(h', k') = (hh', kk')$. Les projections canoniques sont des morphismes surjectifs, les injections sont des isomorphismes, les deux sous-groupes sont distingués

Théorème 5. Si on a deux sous-groupes distingués H et K d'un groupe G tel que $HK = G$ et d'intersection triviale, alors G est isomorphe au produit semi-direct $H \times K$.

Définition 3. Soit N et H deux groupes et φ une action de H sur N définie par automorphismes de groupes (ie tombe dans $\text{Aut}(N)$!!!!!!). La loi suivante sur $N \times H$: $(n, h)(n', h') = (n\varphi(h)n', hh')$ définit une loi de groupe $N \times H$ appelé produit semi-direct de N par H noté $N \rtimes_\varphi H$.

Remarque 3. N est un sous-groupe distingué de $N \rtimes_\varphi H$ au contraire de H qui n'en est pas un en général. On a même:

Théorème 6. $N \rtimes_\varphi H$ abélien $\Leftrightarrow \varphi$ trivial $\Leftrightarrow H$ distingué.

Remarque 4. Si N est distingué dans G et que H est un sous-groupe de G alors NH est un groupe.

Théorème 7. Soit G un groupe, H et N , avec N distingué dans G , $NH = G$ et $N \cap H = 1$. Alors G s'écrit comme produit semi-direct

Remarque 5. Il existe des groupes qui ne sont pas décomposables en produits semi-directs de la forme $\mathbb{Z}/\mathbb{Z}$, par exemple parmi les 5 groupes d'ordre 8, on en a trois abéliens, le diédral D_4 et le groupe des quaternions H_8 pas décomposable.

2.2 Dévissage des groupes diédraux, symétriques, alternés

Théorème 8. Le groupe S_n est isomorphe à un produit semi-direct $A_n \rtimes \mathbb{Z}_2$, la section étant n'importe quelle transposition (on envoie sur sa signature), cela donne les mêmes produits.

Théorème 9. Le groupe diédral $\mathbb{D}_n$ est isomorphe à un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}_2$.

Application 2. Les sous-groupes d'ordre 8 sont les sous-groupes abéliens, le groupe diédral et le groupe des quaternions

2.3 Groupes d'ordre p et p^2

Proposition 10. *Tout sous-groupe d'ordre p est abélien et même cyclique isomorphe à Z_p .*

Exemple 8. $NA(1) = NA(3) = \dots = NA(59)$.

Application 3. *Tout sous-groupe d'ordre p^2 est commutatif et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$.*

Exemple 9. *valable pour 4, 9, 32, 49, 64.*

2.4 Groupes d'ordre pq

Théorème 10. *Tout sous-groupe d'ordre pq est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ si p et $q-1$ sont premiers entre eux, si p divise $q-1$ alors on a deux classes d'isomorphie, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et au produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$*

Exemple 10. *Sous-groupes d'ordre 6: S_3 et $\mathbb{Z}/3\mathbb{Z}$. Sous-groupes d'ordre 15, 33, 51, 35: seulement ceux abéliens. Sous-groupes d'ordre 10, 14, 21, 22, 26, 34, 38, 58: l'abélien et le produit semi-direct.*

2.5 Groupes d'ordre p^2q .

Théorème 11. *Soient p et q premiers distincts. On s'intéresse aux groupes d'ordre p^2q .*

Par souci de clarté, on appelle C_1 la condition : p divise $q-1$, C_2 la condition p^2 divise $q-1$, C_3 la condition q divise $p-1$, C_4 la condition q divise $p+1$. C_2 implique trivialement C_1 .

1. *Si $q = 2$, on a 3 produits semi-directs non isomorphes $Z_{p^2} \rtimes Z_2$, $Z_p^2 \rtimes_1 Z_2$, $Z_p^2 \rtimes_2 Z_2$. On se place dorénavant dans le cas $q \geq 3$.*
2. *Aucune des conditions vérifiées: pas de sous-groupes non abéliens*
3. *C_1 mais aucune des autres: deux produits semi-directs $Z_{p^2} \rtimes Z_q$, $Z_p^2 \rtimes Z_q$.*
4. *C_2 mais pas les autres: $Z_q \rtimes Z_p^2$, $Z_q \rtimes_1 Z_{p^2}$, $Z_q \rtimes_2 Z_{p^2}$*
5. *C_2 et C_3 : 4 produits $Z_q \rtimes Z_{p^2}$, $Z_q \rtimes_1 Z_p^2$, $Z_q \rtimes_2 Z_p^2$, $Z_{p^2} \rtimes Z_q$.*
6. *C_2 et C_4 : 4 produits $Z_q \rtimes Z_{p^2}$, $Z_q \rtimes_1 Z_p^2$, $Z_q \rtimes_2 Z_p^2$, $Z_p^2 \rtimes Z_q$.*
7. *C_3 mais pas les autres: un seul $Z_{p^2} \rtimes q$*
8. *C_4 mais pas les autres: un seul $Z_p^2 \rtimes q$*

Exemple 11. $NA(12)$, $NA(18)$, $NA(50)$, $NA(28)$, $NA(44)$, $NA(45)$

2.6 Groupes d'ordre p^3

Application 4. p impair premier. *Tout groupe d'ordre p^3 est isomorphe soit à $\mathbb{Z}/p^3\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}^2 \times \mathbb{Z}/\mathbb{Z}^2$ ou $\mathbb{Z}/p^3\mathbb{Z}$ ou au produit semi-direct $\mathbb{Z}/p\mathbb{Z}^2 \rtimes \mathbb{Z}/\mathbb{Z}^2$ ou au produit semi-direct $\mathbb{Z}/p\mathbb{Z}^2 \rtimes \mathbb{Z}/\mathbb{Z}$.*

Exemple 12. *Groupes d'ordre 27: les 3 abéliens et les produits semi-directs.*

3 Applications à la théorie de Galois

3.1 Groupes résolubles

Définition 4. *Soit G un groupe. On considère une chaîne de sous-groupes $G_0 \supset G_1 \dots \supset G_m$ telle que G_{i+1} soit distingué dans G_i . Cette suite est appelé suite de composition de G vers G_m . Si G_m est réduit au neutre, on parle seulement de suite de composition. La suite est normale ssi les G_i sont distingués dans G . Elle est abélienne (resp monogène, cyclique) ssi les quotients G_i/G_{i+1} sont abéliens (mon, cyc).*

Proposition 11. *L'image réciproque d'une suite de composition de G vers G_m reste une suite de composition de $f^{-1}(G)$ vers $f^{-1}(G_m)$, qui garde les mêmes props.*

Définition 5. *Un groupe est résoluble ssi il admet une suite de composition abélienne.*

Exemple 13. *Le groupe des matrices triangulaires supérieures est un groupe résoluble. Un p -groupe est résoluble.*

Proposition 12. *Une suite de composition abélienne admet un raffinement cyclique. Donc un sous-groupe résoluble admet une suite de composition cyclique.*

Proposition 13. *G un groupe et H un sous-groupe distingué. Il est résoluble ssi H et G/H le sont.*

Proposition 14. *On considère deux suites de composition $G = G_1 \supset G_2 \supset \dots \supset G_r = e$, $G = H_1 \supset H_2 \supset \dots \supset H_s = e$. Elles sont dites équivalentes ssi $r = s$ et si les suites de quotients sont les mêmes à permutation des indices et isomorphisme près.*

Théorème 12 (Schreier). *Deux suites de composition admettent des raisonnements équivalents.*

Proposition 15 (Jordan-Hölder). *On considère une suite de composition tel que chaque groupe G_i/G_{i+1} soit simple et non trivial. Alors toute suite de composition avec les mêmes propriétés lui est équivalente.*

3.2 Correspondance de Galois

Définition 6. *Une extension finie L d'un corps K est dite galoisienne ssi elle est séparable (ie tout élément de l'extension est tel que le polynôme minimal n'a que des racines simples) et normale (ie tout morphisme invariant K et est automorphisme). Le groupe des automorphismes de L laissant invariant K est appelée le groupe de Galois de K sur k , noté $\text{Gal}(K/k)$.*

Lemme 2 (élément primitif). *Toute extension finie séparable d'un corps est monogène.*

Lemme 3. *Tout polynôme irréductible à coefficients dans K ayant au moins une racine dans L a toutes ses racines dans L (ie. que tout polynôme irréductible de $K[X]$ ayant une racine dans L se décompose en facteurs linéaire dans $L[x]$).*

Théorème 13 (Correspondance de Galois).

3.3 Résolubilité par radicaux

Définition 7. *Une extension finie F de k est dite radicale (ou résoluble par radicaux) ssi elle est séparable et s'il existe une extension finie E de k contenant F et une tour $k = E_0 \subset E_1 \subset \dots \subset E_m = E$, telle que chaque extension E_{i+1}/E_i soit des trois types suivants:*

1. *Obtenue par adjonction d'une racine de l'unité*
2. *Obtenue par adjonction d'une racine d'un polynôme $X^n - a$ avec $a \in E_i$ et n premier à la caractéristique*
3. *Obtenue par adjonction d'une racine d'un polynôme $X^p - X - a$ avec $a \in E_i$ et $p > 0$ la caractéristique.*

Définition 8. *Une extension finie et séparable F de k est dite résoluble ssi le groupe de Galois de la plus petite extension galoisienne K de k contenant E est un groupe résoluble.*

Théorème 14. *Une extension est résoluble ssi elle est résoluble par radicaux.*

Définition 9. *Un polynôme est dit résoluble par radicaux ssi il existe une extension radicale contenant $\text{Dec}_K(P)$.*

Corollaire 3. *Un polynôme est résoluble par radicaux ssi le groupe de Galois $\text{Gal}(\text{Dec}_K(P), K)$ est résoluble.*

Application 5. *L'équation de degré générale 2,3,4 est résoluble par radicaux, contrairement à l'équation générale de degré supérieure ou égale à 5 ne l'est pas.*

References

- [1] Ortisz
- [2] Combes
- [3] Lang