

149: groupes finis de petit cardinal

Pierre Lissy

March 3, 2010

Dans tout ce qui suit, G est un groupe de cardinal inférieur ou égal à 60. $\mathbb{Z}/n\mathbb{Z}$ sera noté Z_n . On confondra un groupe et sa classe d'isomorphisme. $A(i)$ = groupes abéliens de cardinal i . $NA(i)$ = ceux non abéliens.

1 Groupes abéliens

1.1 Classification des groupes abéliens finis

Théorème 1. *Tout groupe abélien est isomorphe à un produit direct de $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 2. *Soient $p_1, \dots, p_n$ des entiers premiers entre eux deux à deux. Alors en tant qu'anneaux, $\mathbb{Z}/p_1 p_2 \dots p_n \simeq \mathbb{Z}/p_1 \mathbb{Z} \times \mathbb{Z}/p_2 \mathbb{Z} \times \dots \times \mathbb{Z}/p_n \mathbb{Z}$. Inversément, si $\mathbb{Z}/p_1 p_2 \dots p_n \simeq \mathbb{Z}/p_1 \mathbb{Z} \times \mathbb{Z}/p_2 \mathbb{Z} \times \dots \times \mathbb{Z}/p_n \mathbb{Z}$ alors les nombres $p_1, \dots, p_n$ sont premiers entre eux deux à deux, et réciproquement.*

Corollaire 1. *On connaît exactement toutes les classes d'isomorphismes de groupes abéliens d'ordre n donné. Si on pose $n = \prod p_i^{\alpha_i}$, il y en a autant que de manière d'écrire $\sum \alpha_i$ comme somme d'entiers. Notamment, il y a 102 groupes finis abéliens de Cardinal inférieur à 60.*

Exemple 1. $A(2) = \{Z_2\}$, $A(3) = \{Z_3\}$, $A(4) = \{Z_2^2, Z_4\}$, $A(8) = \{Z_2^3, Z_2 \times Z_4, Z_2 \times Z_2 \times Z_2\}$, $A(10) = \{Z_2 \times Z_5\}$, $A(24) = \{Z_3 \times Z_8, Z_3 \times Z_2 \times Z_4, Z_3 \times Z_2^3\}$, $A(32) = \{Z_2^4, Z_2 \times Z_{16}, Z_4 \times Z_8, Z_2 \times Z_2 \times Z_8\}$, $A(48) = \{Z_3 \times Z_{16}, Z_2 \times Z_3 \times Z_8, Z_3 \times Z_4 \times Z_4, Z_2 \times Z_2 \times Z_3 \times Z_4\}$.

1.2 Sous-groupes

Remarque 1. 1. Un groupe abélien a un unique p -Sylow avec $p|n$.

2. Tous les sous-groupes d'un groupe abélien sont distingués

3. Z_n a un unique sous-groupe d'ordre d avec $d|n$: le groupe engendré par n/d .

Proposition 1. *Pour les groupes abéliens, il existe des sous-groupes de cardinal d avec d un diviseur de n : il suffit de prendre un certain produit $Z_{a_1} \times \dots \times Z_{a_i}$. Tout groupe abélien fini est isomorphe au produit direct de ses p -Sylow.*

Faux pour les groupes non abéliens, par exemple A_4 n'admet pas de sous-groupes d'ordre 6.

Corollaire 2. *Les seuls sous-groupes abéliens simples sont les Z_p avec p premiers. Il y en a donc 17 de petit cardinal: $Z_2, Z_3, Z_5, Z_7, Z_{11}, \dots, Z_{59}$.*

1.3 Automorphismes

Proposition 2. *Soient $p_1, \dots, p_n$ des entiers premiers entre eux deux à deux. Alors en tant que groupes, $(\mathbb{Z}/p_1 p_2 \dots p_n)^* \simeq \mathbb{Z}/p_1 \mathbb{Z}^* \times \mathbb{Z}/p_2 \mathbb{Z}^* \times \dots \times \mathbb{Z}/p_n \mathbb{Z}^*$*

Théorème 3. *$\text{Aut}(Z_n) \simeq Z_n^*$. Donc Si $n = \prod p_i^{\alpha_i}$ avec les p_i classés par ordre croissant*

1. Si $p_1 = 2, \alpha_1 \geq 2$, $\text{Aut}(Z_n) \simeq Z_2 \times Z_2^{\alpha_1 - 2} \times P_2^{\alpha_1 - 1}(p_2 - 1) \times \dots \times p_n^{\alpha_n}(p_n - 1)$.

2. Si $p_1 = 2, \alpha_1 = 1$, $Aut(Z_n) \simeq p_2^{\alpha_1-1}(p_2 - 1) \times \dots \times p_n^{\alpha_n}(p_n - 1)$.

3. Si $p_1 \geq 3$, $Aut(Z_n) \simeq p_2^{\alpha_1-1}(p_2 - 1) \times \dots \times p_n^{\alpha_n}(p_n - 1)$.

Exemple 2. $Aut(Z_2) = \{Z_1\}$, $Aut(Z_3) = \{Z_2\}$, $Aut(Z_4) = \{Z_2\}$, $Aut(Z_{10}) = \{Z_4\}$, $Aut(Z_{16}) = \{Z_2 \times Z_4\}$, $Aut(Z_{20}) = \{Z_2 \times Z_4\}$, $Aut(Z_{33}) = \{Z_2 \times Z_2 \times Z_3\}$.

Proposition 3. $Aut((Z_p)^n \simeq GL_n(F_p))$

Exemple 3. $Aut(V_4) \simeq GL_2(F_4) = S_3$, $Aut(Z_3^2) = GL_2(F_3)$ d'ordre 48.

Dans les autres cas, il faut faire au cas par cas.

Remarque 2. $Aut(Z_2 \times Z_4) = D_4$.

2 Cas non abélien

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.

Définition 1. Soit N et H deux groupes et φ une action de H sur N définie par automorphismes. 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 5. $N \rtimes_\varphi H$ 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 6. 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 Groupes d'ordre p et p^2

Proposition 4. Tout sous-groupe d'ordre p est abélien et même cyclique isomorphe à $\mathbb{Z}_p$.

Exemple 4. $NA(1) = NA(3) = \dots = NA(59)$.

Application 1. 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 5. valable pour 4, 9, 32, 49, 64..

2.3 Groupes d'ordre pq

Théorème 7. 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 6. 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.

2.4 Groupes d'ordre p^2q .

Théorème 8. 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 7. $NA(12)$, $NA(18)$, $NA(50)$, $NA(28)$, $NA(44)$, $NA(45)$

2.5 Groupes d'ordre p^3

Application 2. 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 8. Groupes d'ordre 27: les 3 abéliens et les produits semi-directs.

2.6 Autres cas

Proposition 5. 1. $NA(8) = D_4, H_8$

2. $NA(30) = \{D_{15}, Z_3 \rtimes D_5, Z_5 \rtimes D_3\}$

3. $NA(36) = \{Z_2 \rtimes_1 Z_2, Z_2 \rtimes_2 Z_2, Z_2 \rtimes_3 Z_2, Z_7 \rtimes_1 Z_6, Z_7 \rtimes_2 Z_6\}$

4. $NA(42) = \{Z_2^2 \rtimes Z_9, Z_2^2 \rtimes Z_3^2, Z_9 \rtimes Z_4, Z_9 \rtimes Z_2^2, Z_3^2 \rtimes_i Z_2^2, Z_3^2 \rtimes_i Z_4\}$ avec $i = 1, 2, 3$.

5. Le seul sous-groupe simple d'ordre 60 est A_5 .

6. Les cas suivants se déduisent de la même manière: . Il reste donc seulement les cas 16, 24, 32, 40, 48, 56, 60, un peu plus complexes.

Remarque 6. 1. $NA(i)$ contient uniquement des produits semi-directs de Z_n , sauf pour $i = 8, 16, 32, 40, 48, 56$

2. En fait, on montre qu'aucun groupe d'ordre strictement inférieur à 60 non abélien n'est simple (on a quasiment démontré ce résultat ici modulo les cas problématiques si-dessous et les autres cas pas faits du paragraphe précédent). A_5 est donc le premier groupe simple non abélien, et c'est le seul d'ordre 60. On rappelle que les seuls sous-groupes abéliens simples sont les Z_p .

2.7 Etude détaillée de petits groupes symétriques ou alternés

Proposition 6. 1. A_n est simple pour $n = 3$ et $n \geq 5$.

2. Le centre de S_n , A_n est trivial. $D(S_n) = D(A_n) = A_n$.

3. $\text{Int}(S_n) \simeq \text{Aut}(S_n) \simeq S_n$ sauf pour $n = 6$ ou on a un produit semi-direct $\text{Aut}(S_6) \simeq S_6 \rtimes 2$.

4. $S_n \simeq A_n \rtimes 2$.

5. La classe de conjugaison d'une permutation est l'ensemble des permutations du même type.

Proposition 7. S_3 du Ortisz.

Proposition 8. S_4 du Ortisz.

Proposition 9. A_4 du Ortisz.

2.8 Etude détaillée du groupe des quaternions

Tableau du Ortisz

References

[1] Perrin

[2] Combes

[3] Quéré

[4] Lelong-Ferrand Arnaudiès Algèbre