Petits groupes

Michel Coste

3 octobre 2007

L'objectif est de faire la liste de tous les groupes (plus exactement, de toutes les classes d'isomorphisme de groupes) d'ordre < 16, et mettant en évidence les méthodes employées (Sylow, produit semi-direct, etc.)

1 Groupes d'ordre p premier

Rappelons que l'ordre d'un élément divise l'ordre du groupe, et que dans un groupe il y a un seul élément d'ordre 1 : l'élément neutre.

Un groupe de cardinal p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, puisqu'il contient un élément d'ordre p et que le sous-groupe engendré par cet élément, isomorphe à $\mathbb{Z}/p\mathbb{Z}$, contient tous les éléments du groupe.

Ceci règle le cas des ordres $2, 3, 5, 7, 11, 13$.

2 Groupes d'ordre p^2, p premier

Un groupe G d'ordre p^2 est forcément commutatif parce que

1. Le centre d'un p-groupe n'est pas réduit à l'identité. Rappelons qu'un p groupe est un groupe d'ordre une puissance de p, et que le centre d'un groupe G est

$$Z(G) = \{g \in G : \forall h \in G hg = gh\} = \{g \in G : \forall h \in G hgh^{-1} = g\} .$$

   Faisons agir un p-groupe G sur lui-même par conjugaison. Un élément de G est dans le centre si et seulement si son orbite est réduite à lui-même. Le cardinal d'une orbite divise l'ordre de G, et est donc ou bien 1, ou bien divisible par p. Comme la somme des cardinaux des orbites est l'ordre de G qui est divisible par p, p divise l'ordre du centre de G.
2. Si G est d'ordre p^2 et s'il n'était pas commutatif, son centre $Z(G)$ serait d'indice p d'après ce qui précède. Or il est impossible que le centre d'un groupe soit d'indice p. Sinon, soit x un élément de G qui n'est pas dans $Z(G)$. Le stabilisateur de x pour l'action de G sur lui-même par conjugaison est un sous groupe qui contient $Z(G)$ et x. Comme il contient strictement $Z(G)$, son indice divise strictement celui de $Z(G)$ et donc ce stabilisateur est G tout entier. Mais alors x est dans le centre de G, contradiction.

Ou bien G contient un élément d'ordre p^2, et alors il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.

Ou bien tous les éléments autres que l'identité sont d'ordre p. Alors G est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel, et donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.

On aurait pu aussi conclure en invoquant le théorème de structure des groupes abéliens de type fini.

Ceci règle la cas des ordres $4, 9$.

3 Groupes d'ordre pq, p et q premiers, $p < q$

Rappelons la partie des théorèmes de Sylow qui nous sera utile : le nombre de q-Sylow d'un groupe d'ordre $N = q^\alpha r$, avec $q \not| r$, est congru à 1 modulo q et divise r.

Pour un groupe G d'ordre $|G| = pq$ comme dans le titre de la section, le nombre de q-Sylow est congru à 1 modulo q et divise p. C'est donc forcément 1, et l'unique q-Sylow H de G est distingué. Ce q-Sylow H, qui est d'ordre q, est isomorphe à $\mathbb{Z}/q\mathbb{Z}$. Soit K un p-Sylow de G ; il est d'ordre p, et isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On a $H \cap K = \{1\}$ puisque les éléments de H autres que le neutre sont d'ordre q, tandis que ceux de K autre que le neutre sont d'ordre p. Par ailleurs $|G| = |H|\,|K|$. Donc G est le produit semi-direct de se sous-groupes H et K : $G = H \rtimes K$.

Ainsi G est isomorphe à un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, tordu par une action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$. Une telle action est donnée par un homomorphisme

$$\rho : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}\ .$$

Si ρ est l'homomorphisme trivial, on a G isomorphe au produit direct $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$. Si $p \nmid (q-1)$, c'est la seule possibilité. Ceci règle le cas de $15 = 3 \times 5$: tout groupe d'ordre 15 est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Si $(q-1) = pr$, alors on a des homomorphismes ρ non triviaux, tous injectifs d'image le sous-groupe de $\mathbb{Z}/(q-1)\mathbb{Z}$ engendré par $\overline{r}$. Les structures de produit semi-direct données par ces ρ sont toutes isomorphes entre elles (passer d'un tel ρ à un autre en composant avec un automorphisme de $\mathbb{Z}/p\mathbb{Z}$). Dans ce cas tout groupe d'ordre pq est isomorphe soit au produit direct $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$, soit au produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ tordu par une action non triviale.

Pour les ordres qui nous intéressent, seul se rencontre le cas $p = 2$ (le premier cas pour $p = 3$ est $21 = 3 \times 7$). Se donner une action non triviale de $\mathbb{Z}/2\mathbb{Z}$ sur un groupe G, c'est se donner un automorphisme d'ordre 2 de G (image par ρ de l'élément d'ordre 2 de $\mathbb{Z}/2\mathbb{Z}$). La seule action non triviale de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ est donnée par $\overline{m} \mapsto -\overline{m}$. Le produit semi-direct obtenu est isomorphe au groupe diédral D_q. En conclusion, tout groupe d'ordre $2q$ avec q premier impair est isomorphe soit à $\mathbb{Z}/2q\mathbb{Z}$, soit au groupe diédral D_q. Ceci règle le cas des ordres 6 et 10.

4 L'ordre 8

On peut régler le cas commutatif par le théorème de structure des groupes abéliens de type fini. On trouve, comme classe d'isomorphismes, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$. On peut ausi faire un raisonnement ad hoc. Soit G d'ordre 8.

Si G contient un élément d'ordre 8 il est isomorphe à $\mathbb{Z}/8\mathbb{Z}$

Si tous les éléments de G autres que le neutre sont d'ordre 2 alors G est commutatif ; en effet $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Donc G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

Reste le cas où G a un élément i d'ordre 4, et pas d'élément d'ordre 8 ; le sous-groupe cyclique engendré par i est d'indice 2, donc il est distingué et le quotient G/C est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. On a ainsi une suite exacte

$$1 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow G \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \ .$$

Cette suite exacte est scindée si et seulement s'il y a un élément d'ordre 2 dans $G \setminus C$ (qui sera image de l'élément non nul de $\mathbb{Z}/2\mathbb{Z}$ par le scindage). Dans ce cas, G est isomorphe au produit semi direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ tordu par une action $\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Il n'y a que deux actions de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/4\mathbb{Z}$: la triviale (auquel cas on récupère le produit direct $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), ou l'action par multiplication par -1 (auquel cas $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est isomorphe au groupe diédral D_4).

Il faut maintenant considérer le cas ou tous les éléments de $G \setminus C$ sont d'ordre 4. Soit j l'un d'entre eux ; j^2 est un élement de C d'ordre 2, donc $j^2 = i^2$. On a $ji \neq ij$, car sinon ij serait un élément d'ordre 2 dans $G \setminus C$. Donc G n'est pas commutatif, et son centre est forcément d'ordre 2 (on sait qu'il ne peut pas être d'indice 2. Comme i^2 est le seul élément de G d'ordre 2, on a $Z = \{1, i^2\}$; on note $i^2 = -1$. Les éléments de C sont $1, i, -1, -i$, ceux de $G \setminus C$ sont $j, ij, -j, -ij$. L'élément ji est dans $G \setminus C$ et est différent de $j, ij, -j = j(-1)$; donc $ji = -ij$. En résumé, G est engendré par i et j vérifiant $i^2 = j^2 = -1$ et $ji = -ij$; il est isomorphe au groupe $\mathbb{H}_8$ des quaternions.

Il y a 5 classes d'isomorphisme de groupes d'ordre 8 :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3, D_4, \mathbb{H}_8 \ .$$

5 L'ordre 12

Encore une fois le théorème de structure des groupes abéliens de type fini permet de faire la liste des classes d'isomorphisme de groupes commutatifs d'ordre 12 : $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Soit G un groupe d'ordre 12. Il a 1 ou 4 3-Sylow.

S'il y en a 1, appelons le H ; c'est un sous-groupe distingué de G, isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Choisissons un 2-Sylow K de G. On a $H \cap K = \{1\}$ et $|H|\,|K| = |G|$, donc $G = H \rtimes K$. Le groupe K peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Le groupe des automorphismes de $\mathbb{Z}/3\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

- Cas $K \simeq \mathbb{Z}/4\mathbb{Z}$. Il y a une seule action non triviale de $\mathbb{Z}/4\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$, correspondant à l'homomorphisme non trivial $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Le produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ correspondant est engendré par a, b avec $a^3 = b^4 = 1,\ ba = a^2b$.
- Cas $K \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Les homomorphismes non triviaux $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ viennent tous de la projection sur le premier facteur par composition avec un automorphisme de $(\mathbb{Z}/2\mathbb{Z})^2$ (on peut penser en termes d'espaces vectoriels sur $\mathbb{Z}/2\mathbb{Z}$). Il y a donc à isomorphisme près un seul produit semi-direct non commutatif $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$; on peut le présenter par générateurs a, b, c avec les relations $a^3 = b^2 = c^2$, $ba = ab$, $cb = bc$,

$ca = a^2c$. En posant $u = ab$, on a les générateurs u, c avec les relations $u^6 = c^2 = 1$, $cu = u^5c$. On reconnait sous cette présentation le groupe diédral D_6.

Supposons maintenant qu'il y a 4 3-Sylow (et forcément G n'est pas commutatif). L'intersection de deux 3 Sylow est réduite à $\{1\}$, donc la réunion de tous les 3-Sylow comporte, outre 1, 8 éléments d'ordre 3. Restent 3 éléments, qui forment avec 1 l'unique 2-Sylow ; appelons le K. C'est un sous-groupe distingué de G. Choisissons un 3-Sylow H. On a $K \cap H = \{1\}$ et $|K||H| = |G|$, donc $G = K \rtimes H$. On sait que H est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, et K est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $(\mathbb{Z}/2\mathbb{Z})^2$.

Considérons d'abord le cas $K \simeq \mathbb{Z}/4\mathbb{Z}$; son groupe d'automorphisme est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et il n'y a donc pas d'action non triviale de $\mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{Z}/4\mathbb{Z}$. Comme on ne veut pas du produit direct commutatif $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$, ce cas est impossible

Donc $K \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Son groupe d'automorphismes est $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) \simeq \mathcal{S}_3$. La donnée d'un homomorphisme non trivial $\mathbb{Z}/3\mathbb{Z} \to \mathcal{S}_3$ revient à celle d'un 3-cycle. Comme les 3-cycles sont tous conjugués dans $\mathcal{S}_3$, tous les produits semi-directs non triviaux $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ sont isomorphes.

Le cas où il y a 4 3-Sylow peut se traiter sans produit direct. Considérons l'action (transitive) de G sur l'ensemble de ses 3-Sylow par conjugaison ; cette action nous donne un homomorphisme $\varphi : G \to \mathcal{S}_4$. Le stabilisateur d'un 3-Sylow H contient H, et est d'ordre 3 (ordre de G divisé par le cardinal de l'orbite). C'est donc H. Le noyau de φ est l'intersection des stabilisateurs, et on a vu que l'intersection des 3-Sylow est réduite à $\{1\}$. Ainsi φ est injectif, G est isomorphe à son image dans $\mathcal{S}_4$ qui est un sous-groupe d'indice 2 de $\mathcal{S}_4$, donc distingué, donc égal à $\mathcal{A}_4$ (la signature est le seul homomorphisme non trivial $\mathcal{S}_4 \to \mathbb{Z}/2\mathbb{Z}$).

Si vous n'avez pas été convaincu(e) par l'identification de D_6 faite plus haut, on peut y revenir. D_6 n'est pas commutatif, donc isomorphe ni à $\mathbb{Z}/12\mathbb{Z}$, ni à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il a un élément d'ordre 6, donc il n'est pas isomorphe à $\mathcal{A}_4$. Il n'a pas d'élémenbt d'ordre 4, donc il n'est pas isomorphe à $cycl3 \rtimes \mathbb{Z}/4\mathbb{Z}$. Il ne reste bien comme possibilité que $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}^2$.

6 Un récapitulatif

ordre	classes d'isomorphisme
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, $D_3 \simeq \mathcal{S}_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, $\mathbb{H}_8$
9	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$, D_5
11	$\mathbb{Z}/11\mathbb{Z}$
12	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_6, $\mathcal{A}_4$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \simeq \langle a, b \mid a^3 = b^4 = 1,\ ba = a^2 b \rangle$
13	$\mathbb{Z}/13\mathbb{Z}$
14	$\mathbb{Z}/14\mathbb{Z}$, D_7
15	$\mathbb{Z}/15\mathbb{Z}$

Références

[Ar] M. Artin : Algebra. Prentice Hall, 1991.

[FG] S. Francinou, H. Gianella : Exercices de mathématiques pour l'agrégation, Algèbre 1. Masson, 1994

[Pe] D. Perrin : Cours d'algèbre.