Les groupes finis d'ordre 60 et 168

Michel CRETIN

1 Le groupe simple d'ordre 60

On considère un groupe *simple* G d'ordre $60 = 2^2 \cdot 3 \cdot 5$.

On désigne par n_p le nombre de p -groupes de Sylow de G . On a $1 < n_5 = 5k + 1 \mid 12$ de sorte que $n_5 = 6$; on désigne par Ω l'ensemble des 5-groupes de Sylow de G sur lequel G opère par conjugaison. Cette action est transitive.

Fixons $P, Q \in \Omega$ avec $P \neq Q$ on a $P, Q \simeq C_5$. Alors l'application :

$$\begin{aligned} u : P &\longrightarrow \Omega \setminus \{P\} \\ g &\longrightarrow gQg^{-1} \end{aligned}$$

est bijective : tout d'abord comme $P \neq Q$ on a bien $gQg^{-1} \in \Omega \setminus \{P\}$ pour tout $g \in P$. De plus supposons que $u(g) = u(g')$ avec $g, g' \in P$. On aurait alors $gg^{-1} \in N_G(Q)$. Or Q est l'unique 5-groupe de Sylow de $N_G(Q)$ de sorte que si l'on avait $gg^{-1} \neq e$, on aurait $gg^{-1} \in Q$ ce qui n'est pas possible car $P \cap Q = \{e\}$. Finalement $g = g'$ et u est injective.

Fixons un générateur α de $P : P = \langle \alpha \rangle$. On en déduit une application bijective :

$$\psi : P_1(\mathbb{F}_5) = \mathbb{F}_5 \cup \{\infty\} \longrightarrow \Omega$$

définie par $\psi(\infty) = P$ et $\psi(k) = \alpha^k Q \alpha^{-k}$ pour tout $k \in \mathbb{F}_5$ (en particulier $\psi(0) = Q$).

L'action de G dans Ω est canoniquement associée à un homomorphisme :

$$\varphi : G \longrightarrow \mathfrak{S}_\Omega$$

Cet homomorphisme est injectif et l'on a $\varphi(G) \subset \mathfrak{A}_\Omega \simeq \mathfrak{A}_6$.

En particulier tout élément $g \in G$ est d'ordre ≤ 6 .

De plus la bijection ψ permet de *transporter* l'action de G sur Ω en une action de G sur $P_1(\mathbb{F}_5)$; on a :

$$\psi(g.x) = g.\psi(x).g^{-1}$$

pour tout $x \in P_1(\mathbb{F}_5)$ et tout $g \in G$ et G s'identifie ainsi à un sous-groupe de $\mathfrak{A}_{P_1(\mathbb{F}_5)}$.

Alors α s'identifie à l'automorphisme $\alpha : x \longrightarrow x + 1$ de $P_1(\mathbb{F}_5)$; on a :

$$\psi(\alpha.\infty) = \alpha.P.\alpha^{-1} = P = \psi(\infty)$$

tandis que pour $k \in \mathbb{F}_5$ on a

$$\psi(\alpha.k) = \alpha(\alpha^k Q \alpha^{-k})\alpha^{-1} = \alpha^{k+1} Q \alpha^{-k-1} = \psi(k+1)$$

Ainsi α agissant sur $P_1(\mathbb{F}_5)$ a un point fixe ∞ et une orbite $P_1(\mathbb{F}_5) \setminus \{\infty\} = \mathbb{F}_5$ de sorte que α est le 5-cycle $(0, 1, 2, 3, 4)$.

Puisque $n_5 = 6$, $N_G(P)$ est d'ordre 10 donc est isomorphe à C_{10} ou à D_5 ; puisque les éléments de G sont d'ordre ≤ 6 on a $N_G(P) \simeq D_5$. Alors le groupe $M = N_G(P) \cap N_G(Q)$ est nécessairement d'ordre 2. Soit $M = \langle \beta \rangle = \{\text{id}, \beta\}$; on a alors

$$N_G(P) = P \rtimes M = \langle \alpha, \beta \rangle$$

avec α d'ordre 5, β d'ordre 2 et $\beta\alpha\beta^{-1} = \alpha^{-1}$. Alors β s'identifie à l'automorphisme $\beta : x \rightarrow -x$ de $P_1(\mathbb{F}_5)$; on a :

$$\psi(\beta.\infty) = \beta.P.\beta^{-1} = P = \psi(\infty)$$

tandis que pour $k \in \mathbb{F}_5$ on a

$$\psi(\beta.k) = \beta(\alpha^k Q \alpha^{-k})\beta^{-1} = (\beta\alpha^k\beta^{-1})(\beta Q \beta^{-1})(\beta\alpha^{-k}\beta^{-1}) = \alpha^{-k} Q \alpha^k = \psi(-k)$$

Notons que $Q = \langle -1 \rangle = \{1, -1\} \subset \mathbb{F}_5^*$ est le sous-groupe des carrés de $\mathbb{F}_5^*$. Posons $N = \mathbb{F}_5^* \setminus Q = \{2, 3\}$. Ainsi β agissant sur $P_1(\mathbb{F}_5)$ a deux points fixes 0 et ∞ et deux orbites Q et N de sorte que β est la permutation $(1, 4)(2, 3)$.

Puisque β est d'ordre 2 on a $N_G(M) = C_G(\beta)$. Or $C_G(\beta)$ est un sous-groupe de $C_{\mathfrak{A}_\Omega}(\beta)$ dont l'ordre est 2-primaire; or les 2-groupes de Sylow de G sont d'ordre 4 donc isomorphes à C_4 ou $C_2 \times C_2$ mais comme G s'identifie à un sous-groupe de $\mathfrak{A}_\Omega$, les 2-groupes de Sylow de G sont des groupes de Klein. On a donc :

$$N_G(M) = \langle \beta, \gamma \rangle$$

avec β et γ d'ordre 2 et $\beta\gamma = \gamma\beta$.

De plus $N_G(P)$ est un sous-groupe *maximal* de G car si H est un sous-groupe de G contenant $N_G(P)$, l'ordre de H est un multiple de 10 qui divise 60 donc H est égal à $N_G(P)$ et G . On a donc :

$$G = \langle \alpha, \beta, \gamma \rangle$$

Or G agit *transitivement* sur Ω et $P_1(\mathbb{F}_5)$; on a donc $G_\infty = N_G(P) = \langle \alpha, \beta \rangle$ de sorte que $\gamma(\infty) \neq \infty$. Mais $\beta\gamma(\infty) = \gamma\beta(\infty) = \gamma(\infty)$ de sorte que $\gamma(\infty)$ est un point fixe de β et finalement $\gamma(\infty) = 0$ de sorte que γ échange 0 et ∞ .

Or β est d'ordre 2, donc produit de deux transpositions de $P_1(\mathbb{F}_5)$ dont l'une est $(0, \infty)$ de sorte que γ a deux points fixes $a, b \in P_1(\mathbb{F}_5) \setminus \{0, \infty\} = \mathbb{F}_5^*$. Mais pour tout $k \in \mathbb{F}_5^*$ on a :

$$\beta\gamma(k) = \gamma\beta(k) = \gamma(-k) = -\gamma(k)$$

de sorte que si $\gamma(a) = a$ on a aussi $\gamma(-a) = -a$ par suite $\{a, b\}$ est égal à $N = \{2, 3\}$ ou $Q = \{1, 4\}$. Enfin remarquons que si $\gamma = (2, 3)(0, \infty)$ on a $\beta\gamma = (1, 4)(0, \infty)$ de sorte que quitte à remplacer γ par $\gamma\beta$ on peut supposer que $\gamma = (1, 4)(0, \infty)$ de sorte que γ est la permutation $x \rightarrow -\frac{1}{x}$ de $P_1(\mathbb{F}_5)$. Finalement on obtient :

$$G \simeq \text{PSL}_2(\mathbb{F}_5)$$

2 Le groupe simple d'ordre 168

On considère un groupe *simple* G d'ordre $168 = 2^3 \cdot 3 \cdot 7$.

On désigne par n_p le nombre de p -groupes de Sylow de G . On a $1 < n_7 = 7k + 1 \mid 24$ de sorte que $n_7 = 8$; on désigne par Ω l'ensemble des 7-groupes de Sylow de G sur lequel G opère par conjugaison. Cette action est transitive.

Fixons $P, Q \in \Omega$ avec $P \neq Q$ on a $P, Q \simeq C_7$. Alors l'application :

$$\begin{aligned} u : P &\longrightarrow \Omega \setminus \{P\} \\ g &\longrightarrow gQg^{-1} \end{aligned}$$

est bijective : tout d'abord comme $P \neq Q$ on a bien $gQg^{-1} \in \Omega \setminus \{P\}$ pour tout $g \in P$. De plus supposons que $u(g) = u(g')$ avec $g, g' \in P$. On aurait alors $gg^{-1} \in N_G(Q)$. Or Q est l'unique

7-groupe de Sylow de $N_G(Q)$ de sorte que si l'on avait $gg^{-1} \neq e$, on aurait $gg^{-1} \in Q$ ce qui n'est pas possible car $P \cap Q = \{e\}$. Finalement $g = g'$ et u est injective.

Fixons un générateur α de $P : P = \langle \alpha \rangle$. On en déduit une application bijective :

$$\psi : P_1(\mathbb{F}_7) = \mathbb{F}_7 \cup \{\infty\} \longrightarrow \Omega$$

définie par $\psi(\infty) = P$ et $\psi(k) = \alpha^k Q \alpha^{-k}$ pour tout $k \in \mathbb{F}_7$ (en particulier $\psi(0) = Q$).

L'action de G dans Ω est canoniquement associée à un homomorphisme :

$$\varphi : G \longrightarrow \mathfrak{S}_\Omega$$

Cet homomorphisme est injectif et l'on a $\varphi(G) \subset \mathfrak{A}_\Omega \simeq \mathfrak{A}_8$.

En particulier tout élément $g \in G$ est d'ordre ≤ 15 .

De plus la bijection ψ permet de transporter l'action de G sur Ω en une action de G sur $P_1(\mathbb{F}_7)$; on a :

$$\psi(g.x) = g.\psi(x).g^{-1}$$

pour tout $x \in P_1(\mathbb{F}_7)$ et tout $g \in G$ et G s'identifie ainsi à un sous-groupe de $\mathfrak{A}_{P_1(\mathbb{F}_7)}$.

Alors α s'identifie à l'automorphisme $\alpha : x \longrightarrow x + 1$ de $P_1(\mathbb{F}_7)$; on a :

$$\psi(\alpha.\infty) = \alpha.P.\alpha^{-1} = P = \psi(\infty)$$

tandis que pour $k \in \mathbb{F}_7$ on a

$$\psi(\alpha.k) = \alpha(\alpha^k Q \alpha^{-k})\alpha^{-1} = \alpha^{k+1} Q \alpha^{-k-1} = \psi(k+1)$$

Ainsi α agissant sur $P_1(\mathbb{F}_7)$ a un point fixe ∞ et une orbite $P_1(\mathbb{F}_7) \setminus \{\infty\} = \mathbb{F}_7$ de sorte que α est le 7-cycle $(0, 1, 2, 3, 4, 5, 6)$.

Puisque $n_7 = 8$, $N_G(P)$ est d'ordre 21 et n'est pas cyclique puisque les éléments de G sont d'ordre ≤ 15 . Alors le groupe $M = N_G(P) \cap N_G(Q)$ est d'ordre 1 ou 3. Mais si M était d'ordre 1 on aurait $\text{Card}(N_G(P).N_G(Q)) = 21^2 > 168$ et finalement M est d'ordre 3.

Soit $M = \langle \beta \rangle$; on a alors

$$N_G(P) = P \rtimes M = \langle \alpha, \beta \rangle$$

avec α d'ordre 7, β d'ordre 3 et $\beta\alpha\beta^{-1} = \alpha^r$ avec $r \not\equiv 0, 1 \pmod{7}$. On a donc $\beta\alpha^k\beta^{-1} = \alpha^{rk}$ et comme $\beta^3 = 1$ on a $\alpha = \alpha^{r^3}$ de sorte que $r^3 \equiv 1 \pmod{7}$. Ainsi on a $r = 2$ ou $r = 4$. Enfin si $r = 4$ on a $\beta\alpha\beta^{-1} = \alpha^4$ de sorte que $\beta^2\alpha\beta^{-2} = \alpha^2$. Quitte à remplacer le générateur β de M par le générateur β^2 on peut toujours supposer que l'on a :

$$\beta\alpha\beta^{-1} = \alpha^2$$

Alors β s'identifie à l'automorphisme $\beta : x \longrightarrow 2x$ de $P_1(\mathbb{F}_7)$; on a :

$$\psi(\beta.\infty) = \beta.P.\beta^{-1} = P = \psi(\infty)$$

tandis que pour $k \in \mathbb{F}_7$ on a

$$\psi(\beta.k) = \beta(\alpha^k Q \alpha^{-k})\beta^{-1} = (\beta\alpha^k\beta^{-1})(\beta Q \beta^{-1})(\beta\alpha^{-k}\beta^{-1}) = \alpha^{2k} Q \alpha^{-2k} = \psi(2k)$$

Notons que $Q = \langle 2 \rangle = \{1, 2, 4\} \subset \mathbb{F}_7^*$ est le sous-groupe des carrés de $\mathbb{F}_7^*$. Posons $N = \mathbb{F}_7^* \setminus Q = \{3, 5, 6\}$. Ainsi β agissant sur $P_1(\mathbb{F}_7)$ a deux points fixes 0 et ∞ et deux orbites Q et N de sorte que β est la permutation $(1, 2, 4)(3, 6, 5)$.

Notons que M est un 3-groupe de Sylow G . On a $1 < n_3 = 3k + 1 \mid 56$ de sorte que les valeurs possibles pour n_3 sont 4, 7 ou 28.

Soit n'_3 le nombre de 3-groupes de Sylow de $N_G(P)$; on a $n'_3 = 3k + 1|7$ de sorte que le valeurs possibles de n'_3 sont 1 ou 7 et comme $N_G(P)$ n'est pas abélien on a $n'_3 = 7$. Il en résulte donc que $n_3 = 28$.

Ainsi l'ordre de $N_G(M)$ est 6 et par suite $N_G(M)$ est isomorphe à C_6 ou à $\mathfrak{S}_3$.

Supposons que l'ensemble U des éléments d'ordre 6 de G soit non vide et considérons alors l'application $v \rightarrow \langle v^2 \rangle$ de U dans l'ensemble des 3-groupes de Sylow de G est surjective : comme $U \neq \emptyset$ soit $u \in U$. Pour tout 3-groupe de Sylow H de G il existe donc $g \in G$ tel que $H = g \langle u^2 \rangle g^{-1}$ de sorte $H = \langle (gug^{-1})^2 \rangle$ avec gug^{-1} d'ordre 6. On en déduit alors que l'application $v \rightarrow v^2$ de U dans l'ensemble des éléments d'ordre 3 de G est surjective : soit $w \in G$ un élément d'ordre 3 ; puisque $\langle w \rangle$ est un 3-groupe de Sylow on a $\langle w \rangle = \langle v^2 \rangle$ avec v d'ordre 6 de sorte que l'on a $w = v^2$ ou $w = v^4 = (v^5)^2$ et v^5 est d'ordre 6. Ainsi G qui possède 48 éléments d'ordre 7 ($n_7 = 8$) et 56 éléments d'ordre 3 ($n_3 = 28$) posséderait au moins 56 éléments d'ordre 6. Mais comme G possède au moins 2 2-groupes de Sylow le nombre d'éléments dépasserait 168. On a donc $U = \emptyset$ et finalement :

$$N_G(M) \simeq \mathfrak{S}_3$$

et par suite $N_G(M) = \langle \beta, \gamma \rangle$ avec β d'ordre 3, γ d'ordre 2 et $\gamma\beta\gamma^{-1} = \beta^{-1}$.

En fait $N_G(M)$ contient 3 éléments d'ordre 2 $\gamma, \gamma' = \beta\gamma\beta^{-1}$ et $\gamma'' = \beta^2\gamma\beta^{-2}$ qui vérifient tous la relation précédente.

De plus $N_G(P)$ est un sous-groupe *maximal* de G : si H est un sous-groupe strict de G contenant strictement $N_G(P)$, l'ordre de H est un multiple de 21 qui divise 168 donc est égal à 42, 84 donc est d'indice 2 ou 4. Comme G est simple H serait d'indice 4 ; mais l'homomorphisme

$$\begin{aligned} \phi_H : G &\longrightarrow \mathfrak{S}_{G/H} \\ g &\longrightarrow \phi_H(g) : \bar{x} \longrightarrow \overline{gx} \end{aligned}$$

étant injectif on aurait $168|4!$ (ce même argument montre d'ailleurs que les ordres *possibles* pour les sous-groupes de G sont 1,2,3,4,5,6,7,8,12,14,21,24).

On a donc ainsi :

$$G = \langle \alpha, \beta, \gamma \rangle$$

Or G agit *transitivement* sur Ω et $P_1(\mathbb{F}_7)$; on a donc $G_\infty = N_G(P) = \langle \alpha, \beta \rangle$ de sorte que $\gamma(\infty) \neq \infty$. Mais $\beta^{-1}\gamma(\infty) = \gamma\beta(\infty) = \gamma(\infty)$ de sorte que $\gamma(\infty)$ est un point fixe de β et finalement $\gamma(\infty) = 0$ de sorte que γ échange 0 et ∞ .

Ainsi γ est d'ordre 2, *échange les points fixes* 0 et ∞ de β et vérifie pour tout $k \in P_1(\mathbb{F}_7) \setminus \{0, \infty\} = \mathbb{F}_7^*$ la condition :

$$\beta^{-1}\gamma(k) = \gamma\beta(k) = \gamma(2k) = 4\gamma(k)$$

Si l'on avait $\gamma(1) \in Q$ on aurait $\gamma(Q) = Q$ donc γ contiendrait le 3-cycle (1,2,4). On a donc $\gamma(1) \in N$ de sorte que γ échange les orbites Q et N de β . Quitte à remplacer γ par l'un des deux autres éléments γ' ou γ'' d'ordre 2 de $N_G(P)$ on peut supposer que $\gamma(1) = 6$ de sorte que $\gamma(2) = 3$ et $\gamma(4) = 5$. On a donc $\gamma = (1,6)(2,3)(4,5)(0, \infty)$ de sorte que γ est la permutation $x \rightarrow -\frac{1}{x}$ de $P_1(\mathbb{F}_7)$. Finalement on obtient :

$$G \simeq \text{PSL}_2(\mathbb{F}_7)$$

Exemple : Un *plan projectif fini* est un ensemble fini X (les *points*) muni d'un ensemble $\mathcal{D} \subset \mathfrak{P}(P)$ de parties de X (les *droites*) vérifiant les conditions :

1. Pour $x, y \in P$ il existe un unique $D \in \mathcal{D}$ tel que $x, y \in D$.
2. Pour $D, D' \in \mathcal{D}$, on a $D \cap D' = \{x\}$ avec $x \in P$.

3. Il existe au moins 4 éléments de X ayant la propriété qu'il n'y en a pas 3 d'entre eux appartenant à un unique élément $D \in \mathcal{D}$.

Posons

$$X = \{1, 2, 3, 4, 5, 6, 7\}$$

et

$$\mathcal{D} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 3, 1\}\}$$

et considérons le groupe G des *collinéations* du *plan de Fano* $(X, \mathcal{D})$:

$$G = \{\sigma \in \mathfrak{S}_7 / D \in \mathcal{D} \Rightarrow \sigma(D) \in \mathcal{D}\}$$

On a $\pi = (1, 2, 3, 4, 5, 6, 7) \in G$ donc G est transitif; on a $\alpha = (2, 7, 6)(4, 3, 5) \in G$ et $\beta = (2, 4)(5, 6) \in G_1$ donc G est 2-transitif et donc primitif.

Soit $\sigma \in G_{1,2}$; on a $\sigma(4) = 4$; il en résulte que

$$G_{1,2} = \{e, (3, 5)(6, 7), (3, 6)(5, 7), (3, 7)(5, 6)\}$$

d'où

$$\text{Card}(G) = 7 \cdot 6 \cdot \text{Card}(G_{1,2}) = 168$$

Soit K un sous-groupe distingué de G ; puisque G est primitif, K est transitif donc contient un 7-cycle, donc un 7-groupe de Sylow de G et finalement tous les 7-groupes de Sylow de G , donc le nombre n_7 est égal à 1 ou 8. Ainsi il y a 6 ou 48 éléments d'ordre 7 dans K et dans G . Mais $(1, 7, 5, 3, 4, 2, 6) = \alpha\pi\alpha^{-1} \in G$ mais n'est pas dans le sous-groupe engendré par π , donc on a $n_7 = 8$ de sorte que $\text{Card}(K) \geq 49$ et finalement $K = G$. ainsi G est simple.

Appendice : Soit G un groupe opérant sur un ensemble X ; un *bloc* $B \subset X$ est une partie de X telle que pour tout $g \in G$ on ait $g(B) = B$ ou $g(B) \cap B = \emptyset$. Les blocs triviaux sont $\emptyset$, X et les parties à un élément $\{x\}$ avec $x \in X$. si tout bloc est trivial on dit que l'action de G sur X est *primitive*. D'autre part, pour $k \geq 1$, on désigne par $X^{(k)} \subset X^k$ l'ensemble des k -uples $(x_1, \dots, x_k)$ dont les composantes sont deux à deux distinctes. On dit que l'action de G sur X est *k-transitive* si l'action de G sur $X^{(k)}$ induite par l'action de G sur X est transitive.

Lemme 1 *Soit G agissant sur X ; si cette action est k -transitive avec $k \geq 2$, elle est primitive.*

▽ Soit B un bloc contenant au moins deux éléments x et y ; pour tout $z \in X$, $z \neq x$, il existe $g \in G$ tel que $g(x) = x$ et $g(y) = z$ de sorte que $g(B) = B$, donc $z \in B$ et $B = X$. Δ

Lemme 2 *Soit G agissant sur X ; on suppose cette action primitive; alors tout sous-groupe distingué K de G agit transitivement sur x*

▽ En effet les orbites de K forment un système de blocs. Δ

Michel CRETIN
Michel.Cretin@math.univ-lyon1.fr