7. Applications dans la théorie des groupes

L'équation de classe est très simple et s'applique dans beaucoup de situations. Il y a beaucoup d'applications dans la topologie algébrique, la géométrie différentielle, la théorie de la représentation et dans d'autres sujets. Maintenant nous allons tirer des conséquences non-triviales dans la théorie des groupes finis soi-même.

Premièrement on va donner une condition suffisante pour qu'un sous-groupe soit normal, une généralisation du fait que si l'index d'un sous groupe est $(G : H) = 2$ alors $H \lhd G$. La preuve utilise l'action de G (et donc de H) sur G/H.

Proposition 7.1. *Soit $H < G$ tel que $p := (G : H)$ est le plus petit diviseur premier de $O(G)$. Alors $H \lhd G$.*

Preuve. Le groupe G agit sur $X := G/H$ par multiplication à gauche, alors son sous-groupe H agit aussi sur G/H par restriction et le plus petit diviseur premier de $O(H) \geq p$. Le translaté gH est un point fixe pour cette H-opération si et seulement si $hgH = gH$ pour chaque $h \in H$, donc si et seulement si $g^{-1}hg \in H$ ou $g \in N_G(H)$ (le normalisateur de H). Donc

$$|X^H| = |N_G H/H| = (N_G H : H) \geq 1$$

et

$$|X| - |X^H| = (G : H) - (N_G H : H) < p.$$

Par Lemme 6.1 on obtient que $X = X^H$, donc $N_G H = G$ et $H \lhd G$. □

Exercice 7.1. Soient $H < G$, $O(H) = m$, $O(G) = mk$ tel que le plus petit diviseur premier de m est $\geq k$. Montrer que $H \lhd G$.

Par exemple, si $O(G) = 140$ et $O(H) = 35$ donc $H \lhd G$.

Exercice 7.2. Soit G un groupe d'ordre 245 et X un G-ensemble d'ordre 244 et de 49 orbites. Montrer l'existence d'un point fixe.

7.1. **Action par conjugaison.** La deuxième application de l'équation de classe utilise l'action d'un groupe sur soi-même par conjugaison :

$$g \odot x := gxg^{-1},$$

pour $g \in G$ et $x \in X := G$.

Vérification : On a $\mathbf{1} \odot x = x$ et

$$g_1 \odot (g_2 \odot x) = g_1(g_2 \odot x)g_1^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = (g_1 g_2) \odot x,$$

et donc $(g, x) \mapsto g \odot x$ est vraiment une G-opération sur G.

Les G-orbites pour cette opération sont appelées *classes de conjugaison.* L'élément $x \in G$ est un point fixe pour cette action si et seulement si $gx = xg$ pour chaque g si et seulement si x est dans le centre $Z(G)$ de G. Le stabilisateur de $x \in X = G$ est appelé le *centralisateur* de x

$$\mathrm{Stab}(x) = \{g \in G; gx = xg\}.$$

Exemple 7.1. Soit $G = \mathbf{U}(n)$ le groupe des matrices unitaires. Dans le cours de l'algèbre linéaire on démontre que pour chaque $u \in G$ il existe un $v \in G$ tel que $v^{-1}uv = \Lambda$, où Λ est une matrice diagonale. En fait, on peut prendre pour la i-ème colonne de v un vecteur propre de u avec valeur propre Λ_{ii}. Si $f(t)$ est un polynôme unitaire de degré n dont tous les zéros sont de valeur absolue 1, alors il existe une seule classe de conjugaison dans G ayant $f(t)$ comme polynôme caractéristique. Donc il y a une bijection entre les classes de conjugaison de G et les polynômes unitaire de degré n dont chaque zéro est de valeur absolue 1.

On va utiliser l'action par conjugaison dans la preuve de la proposition suivante.

Proposition 7.2. *Soit P un groupe fini d'ordre p^r, où p est un nombre premier et $r > 0$. Alors le centre $Z(P)$ de P a au moins p éléments.*

L'ordre de $Z(P)$ n'est pas p^{r-1}, car sinon P n'est pas abélien et $P/Z(P)$ est cyclique. Mais, si P n'est pas abélien, alors $P/Z(P)$ n'est pas cyclique.

Preuve. Considérons l'action de P sur soi-même par conjugaison. Les points fixes forment le centre, donc $|P| - |Z(P)|$ est divisible par p, par Lemme 6.2. Donc p divise $|Z(P)|$. Mais le neutre est dans le centre, donc ils existent encore au moins $p-1$ autres éléments dans $Z(P)$.

Supposons que $P/Z(P)$ est cyclique de générateur $vZ(P)$, pour un $v \in P$. Donc pour chaque $x, y \in P$ ils existent $i, j \in \mathbb{Z}$ et $c_1, c_2 \in Z(P)$ tels que

$$x = v^i c_1 \text{ et } y = v^j c_2.$$

Donc

$$xy = v^i c_1 v^j c_2 = v^i v^j c_1 c_2 = v^{i+j} c_2 c_1 = v^j v^i c_2 c_1 = v^j c_2 v^i c_1 = yx,$$

parce que c_1 et c_2 commutent avec tous les éléments du groupe. Alors P est abélien et $P = Z(P)$.

Supposons que $|Z(P)| = p^{r-1}$, donc P n'est pas abélien. Le groupe quotient $P/Z(P)$ est cyclique d'ordre p, donc P est abélien. Contradiction. □

Exercice 7.3. Montrer qu'un group d'ordre p^2 est abélien, isomorphe à C_{p^2} ou à $C_p \times C_p$.

Exemple 7.2. Groupes d'ordre p^3 ne sont pas nécessairement abélien. Par exemple le groupe D_4 (isomorphe à $U(3, \mathbb{F}_2)$) d'ordre 8. Un autre exemple est le groupe des quaternions de Hamilton : $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ avec le centre $\{1, -1\}$ et les multiplications

$$i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik.$$

Q (six éléments d'ordre 4) n'est pas isomorphe à D_4 (seulement deux éléments d'ordre 4).

Exercice 7.4. Montrer qu'un groupe d'ordre p^s est résoluble.

7.2. **Théorème de Cauchy.** La troisième application est le théorème de Cauchy qui dit que pour chaque diviseur premier de l'ordre du groupe il existe un élément de tel ordre. Ce résultat est très utile. La preuve utilise aussi des actions.

Théorème 7.1 (Cauchy)**.** [16] *Soit G un groupe fini et soit p un diviseur premier de $|G|$. Alors le groupe contient au moins un élément d'ordre p.*

[16] Augustin-Louis Cauchy, mathématicien français, 1789-1857.

Soit n_p le nombre d'éléments de G d'ordre p et soit N_p le nombre de sous-groupes de G d'ordre p. Alors $n_p + 1$ et $N_p - 1$ sont divisible par p et $n_p = N_p(p-1)$, donc n_p est divisible par $p-1$.

Preuve. Dans cette preuve ce n'est pas G qui agit, mais un groupe cyclique $P =< \sigma >$ d'ordre p. Définissons sur l'ensemble

$$Y := \{(g_1, g_2, \ldots, g_p) \in G^p;\ g_1 g_2 \ldots g_p = \mathbf{1}_G\}.$$

une P-action par

$$\sigma \bullet (g_1, g_2, \ldots, g_p) := (g_2, g_3, \ldots, g_p, g_1),$$

la permutation cyclique des coefficients. Donc en effet σ^p agit trivialement, et si $g_1 g_2 \ldots g_p = \mathbf{1}$, alors

$$g_2 g_3 \ldots g_p g_1 = g_1^{-1} g_1 g_2 \ldots g_p g_1 = \mathbf{1}.$$

On va identifier les points fixes. On a que $(g_1, g_2, \ldots, g_p) \in Y^P$ si et seulement si

$$(g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

donc $g_1 = g_2 = g_3 = \ldots = g_p$, disons g, et $g_1 g_2 \ldots g_p = gg \ldots g = g^p = \mathbf{1}$. Donc

$$Y^P = \{(g, g, \ldots, g \in G^p); g^p = 1\}.$$

Si $g^p = 1$ alors $O(g) = p$ ou $O(g) = 1$ (c.-à-d. $g = \mathbf{1}_G$), parce que p est premier. D'où

$$|Y^P| = |\{g \in G;\ g^p = \mathbf{1}\}| = 1 + n_p.$$

L'application

$$\pi : Y \longrightarrow G^{p-1} :\ (g_1, g_2, \ldots, g_p) \mapsto (g_1, g_2, \ldots, g_{p-1})$$

est une bijection, parce que $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$. Donc

$$|Y| = O(G)^{p-1}.$$

Par l'équation de classe (ou par Lemme 6.2) on obtient que

$$|Y| - |Y^P| = O(G)^{p-1} - (1 + n_p)$$

est divisible par p. Par l'hypothèse p divise $O(G)$, donc $n_p + 1$ est divisible par p. En particulier, $n_p > 0$ et il existe un élément d'ordre p.

L'intersection de deux sous-groupes différents d'ordre p est $\{\mathbf{1}\}$, chaque groupe d'ordre p contient exactement $p-1$ éléments d'ordre p et chaque élément x d'ordre p est dans un unique sous-groupe d'ordre p (le sous-groupe $< x >$). Donc $n_p = N_p(p-1)$ et $pN_p - N_p + 1$ est divisible par p, donc $N_p - 1$ est divisible par p. □

Nous allons maintenant donner une preuve alternative (aussi utilisant des actions) pour l'existence d'un élément d'ordre p. Nous allons utiliser l'exercice suivant.

Exercice 7.5. Soit G un groupe et $n \in \mathbb{Z}_{>0}$ un entier avec la propriété suivante. Pour chaque sous-groupe $H < G$ tel que $H \neq G$ on a que n divise l'index $(G : H)$. Montrer que pour chaque G-ensemble fini X on a que

$$|X| \equiv |X^G| \mod n.$$

Preuve alternative de l'existence d'un élément d'ordre p, si p divise $O(G)$. Nous allons utiliser une preuve par induction sur $O(G)$. Si $O(G) = p$, alors G est cyclique d'ordre p et donc il existe en effet un élément d'ordre p. Supposons en suite le résultat soit vrai pour les groupes d'ordre $< O(G)$.

Supposons alors que p est un diviseur premier de l'ordre de G. Supposons qu'il existe un sous-groupe $H < G$ tel que $H \neq G$ et p divise $O(H)$. Par l'hypothèse d'induction il existe un $h \in H$ tel que $O(h) = p$, mais $h \in G$ donc on a trouvé G un élément d'ordre p dans G. Donc la preuve serait complète.

Supposons, par contre, que pour chaque sous-groupe $H < G$ tel que $H \neq G$ on a que p ne divise pas $O(H)$. En conséquence, pour chaque sous-groupe propre H on a que p divise l'index $(G : H)$. Cela implique que pour chaque G-action et chaque orbite Orb telle que $|\,\mathrm{Orb}\,| > 1$ on a p divise $|\,\mathrm{Orb}\,|$. Considérons maintenant l'action de G sur soi-même par conjugaison. L'équation de classe nous donne

$$O(G) = O(Z(G)) + \sum_{C,|C|>1} |C|,$$

où la somme est sur les classes de conjugaison d'ordre > 1, et donc cette somme est divisible par p. On obtient que $O(Z(G))$ est aussi divisible par p, et il suit que $Z(G) = G$ et donc G est abélien (car, par hypothse, G est le seul sous-groupe de G dont l'ordre est divisible par p).

Ainsi on peut supposer, en plus, que G est un groupe abélien. Soit maintenant $g \in G$ non-trivial. Si $O(g) = np$ alors $O(g^n) = p$ et on est prêt. Supposons alors que p ne divise pas $O(g) =: n$, et donc aussi que $H :=< g >\neq G$. Le groupe G est abélien, donc $H \lhd G$ et G/H est un groupe d'ordre $O(G)/n < O(G)$ et encore divisible par p. Par l'hypothèse d'induction on conclut qu'il existe un $k \in G$ tel que le translaté kH est d'ordre p dans le groupe quotient G/H, c-à-d, $kH \neq H$ et $k^pH = H$.

Parce que p et n sont relativement premier, il existe des entiers $a, b \in \mathbb{Z}$ tel que $1 = an + bp$. On a que $k^nH \neq H$, car sinon on aurait $k^nH = H$ et $kH = k^{an+bp}H = (k^nH)^a(k^pH)^b = H$, mais $kH \neq H$.

$k^pH = H$ implique qu'il existe un r tel que $k^p = g^r$ et donc $k^{np} = g^{rn} = 1$, car $n = O(g)$. Mais $k^nH \neq H$ implique que $k^n \notin H$, donc $k^n \neq 1$. On conclut que $O(k)$ divise np mais ne divise pas n, alors est de la forme $O(k) = mp$. Il suit que k^m est de l'ordre p et donc G contient un élément d'ordre p. □

Exercice 7.6. Si $7|O(G)$ et n_7 dénote le nombre d'éléments d'ordre 7, alors $n_7 \equiv 6 \mod 42$.

Calculer le nombre d'éléments d'ordre 7 dans Alt_7 et vérifier que c'est 6 modulo 42.

Exercice 7.7. Soit P un groupe d'ordre p^s et $t \leq s$. Utiliser le théorème de Cauchy et Proposition 7.2 pour montrer que P contient un sous-groupe d'ordre p^t.

Exercice 7.8. Considérons le groupe $G = \mathrm{GL}(3, \mathbb{F}_2)$. Montrer que $O(G) = 168$.

Posons

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ g_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};\ g_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix};\ g_4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix};$$

$$g_7 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} ; \; g_7^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Montrer que $O(g_i) = i$.

Si $C_G(x) = \{g \in G; gxg^{-1} = x\}$ est le centralisateur de $x \in G$, montrer que

$$C_G(g_1) = G; C_G(g_3) =< g_3 >; C_G(g_4) =< g_4 >; C_G(g_7) =< g_7 >=< g_7^{-1} >= C_G(g_7^{-1})$$

et

$$C_G(g_2) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} ; \; a, b, c \in \mathbb{F}_2 \}.$$

Posons n_i pour le nombre d'éléments de G d'ordre i. Montrer que

$$n_1 = 1, n_2 = 21, n_3 = 56, n_4 = 42, n_7 = 48$$

et $n_i = 0$ si $i \notin \{1, 2, 3, 4, 7\}$.

Montrer que les polynómes caractéristiques de g_7 et g_7^{-1} sont différents, et montrer qu'il y a deux classes de conjugaison d'éléments d'ordre 7, et six classes de conjugaison en total.

7.3. **Produits semi-direct.** [17] Les actions peuvent aussi être utiles pour construire ou décomposer des groupes. Si un groupe G opère sur un autre groupe N par des automorphismes on peut construire un produit semi-direct. Plus précisément, soit G et N deux groupes et

$$\phi : \; G \longrightarrow \operatorname{Aut} N$$

un homomorphisme de groupes (comparez avec le théorème de Cayley généralisé). Nous définissons le *produit semi-direct*

$$N \rtimes_\phi G$$

de N et G. L'ensemble de ce groupe est le produit cartésien $N \times G$ et l'opération interne est définie par

$$(n_1, g_1) \circ (n_2, g_2) := (n_1 \cdot [\phi(g_1)](n_2), g_1 g_2) \in N \times G.$$

Lemme 7.1. *$N \rtimes_\phi G$ est un groupe.*

Preuve. On a que $\phi : \; G \longrightarrow \operatorname{Aut} N$ est un homomorphisme de groupes. Alors pour $g_1, g_2 \in G$ et $n_1, n_2 \in N$ on a

$$[\phi(g_1)](n_1 n_2) = [\phi(g_1)](n_1) \cdot [\phi(g_1)](n_2) \tag{3}$$

(parce que $\phi(g_1)$ est un automorphisme de N) et

$$[\phi(g_1 g_2)](n_1) = [\phi(g_1) \circ \phi(g_2)](n_1) = [\phi(g_1)]([\phi(g_2)](n_1)) \tag{4}$$

(parce que ϕ est un homomorphisme et l'opération interne de $\operatorname{Aut} N$ est la composition d'applications).

[17] Ne fait pas partie de la matière examen

Vérifions maintenant l'associativité.

$$\begin{aligned}
&((n_1, g_1) \circ (n_2, g_2)) \circ (n_3, g_3) = \\
&= (n_1 \cdot [\phi(g_1)](n_2), g_1 g_2) \circ (n_3, g_3) \\
&= (n_1 \cdot [\phi(g_1)](n_2) \cdot [\phi(g_1 g_2)](n_3), g_1 g_2 g_3) \\
&= (n_1 \cdot [\phi(g_1)](n_2) \cdot [\phi(g_1)]([\phi(g_2)](n_3)), g_1 g_2 g_3) \text{ par (4)} \\
&= (n_1 \cdot [\phi(g_1)](n_2 \cdot [\phi(g_2)](n_3)), g_1 g_2 g_3) \text{ par (3)} \\
&= (n_1, g_1) \circ (n_2 \cdot [\phi(g_2)](n_3), g_2 g_3) \\
&= (n_1, g_1) \circ ((n_2, g_2) \circ (n_3, g_3)).
\end{aligned}$$

□

Exercice 7.9. Montrer que $(\mathbf{1}_N, \mathbf{1}_G)$ est le neutre de $N \rtimes_\phi G$, et trouver l'inverse de (n, g).

Définissons $A := \{(n, \mathbf{1}_G);\ n \in N\}$ et $B := \{(\mathbf{1}_N, g);\ g \in G\}$. Montrer que $A \lhd (N \rtimes_\phi G)$, $B < (N \rtimes_\phi G)$, $A \cap B = \{(\mathbf{1}_N, \mathbf{1}_G)\}$ et $AB = N \rtimes_\phi G$.

On peut caractériser les groupes qui sont isomorphes aux produits semi-directs. Le résultat principal est le suivant (comparez avec le deuxième théorème d'isomorphisme).

Proposition 7.3. *Supposons que H est un groupe avec deux sous-groupes A et B tels que $A \lhd H$, $A \cap B = \{\mathbf{1}_H\}$ et $AB = H$. Définissons $\phi : B \longrightarrow \operatorname{Aut} A$ par $\phi(b)(a) := bab^{-1}$. Alors $H \simeq (A \rtimes_\phi B)$.*

Preuve. L'application $\psi :\ A \rtimes_\phi B \longrightarrow H$ définie par

$$\psi(a, b) := ab$$

est un homomorphisme de groupes, parce que

$$\begin{aligned}
\psi((a_1, b_1) \circ (a_2, b_2)) &= \psi((a_1 \cdot [\phi(b_1)](a_2), b_1 b_2)) = a_1 \cdot [\phi(b_1)](a_2) \cdot b_1 b_2 = \\
&= a_1 \cdot b_1 a_2 b_1^{-1} \cdot b_1 b_2 = a_1 b_1 a_2 b_2 = \psi((a_1, b_1))\psi((a_2, b_2)).
\end{aligned}$$

C'est surjectif, parce que $H = AB$ et injectif parce que (a_1, b_1) est dans le noyau si et seulement si $a_1 b_1 = \mathbf{1}_H$, ou $a_1 = b_1^{-1}$, donc $a_1 \in A \cap B = \{\mathbf{1}_H\}$. Donc ψ est un isomorphisme de groupes. □

Exercice 7.10. Soit K un corps et B le groupe des matrices triangulaire supérieure inversibles, T le groupe des matrices diagonale inversibles et U le groupe des matrices triangulaire supérieure unitaires. Si $n = 3$:

$$B = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix};\ T = \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix};\ U = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

Montrer que B est un produit semi-direct de T et U.

Chaque groupe d'ordre pq est un produit semi-direct, où $p \neq q$ sont deux nombres premier.

Proposition 7.4. *Soit G un groupe d'ordre pq, où $p < q$ sont deux nombres premiers.*
Alors il existe un homomorphisme $\phi : C_p \longrightarrow \operatorname{Aut} C_q$ tel que

$$G \simeq C_q \rtimes_\phi C_p.$$

Si G est abélien, alors G est cyclique. Si p ne divise pas $q-1$, alors G est abélien et donc cyclique.

Preuve. Par le théorème de Cauchy il existe un sous-groupe $B < G$ d'ordre p et un sous-groupe $A < G$ d'ordre q. L'index de $(G : A) = p$ est le plus petit diviseur premier de $|G|$, donc $A \lhd G$ par Proposition 7.1. On a $A \cap B = \{\mathbf{1}_G\}$ et $AB = G$. Donc avec $\phi : B \longrightarrow \operatorname{Aut} A$ défini par $\phi(b)(a) := bab^{-1}$ on a $G \simeq A \rtimes_\phi B$, par le résultat plus haut. On a que G est abélien si et seulement si ϕ est trivial (ça veut dire $\phi(g) = \mathbf{1}$ pour chaque g) (exercice : montrer ça). Ici le groupe A est cyclique d'ordre q, disons avec générateur a. Alors $\phi(a)$ est aussi un générateur, donc il existe un unique $1 \leq i < q$ tel que $\phi(a) = a^i$. Par contre, $a \mapsto a^i$, où $1 \leq i < q$, définit un automorphisme de A. Donc $O(\mathrm{Aut}(A)) = q - 1$. Si ϕ n'est pas trivial, alors l'image $\phi(B)$ n'est pas trivial, donc isomorphe à B (parce que B est isomorphe au groupe cyclique d'ordre p, où p est premier). Donc $p = O(B)$ divise $O(\mathrm{Aut}(A)) = q - 1$. □

Remarque. Pour connaître les groupes non-abélien d'ordre pq il suffit de connaître $\operatorname{Aut} C_q$ et les homomorphismes $C_p \longrightarrow \operatorname{Aut} C_q$. Soit $C_q =< a >$, alors a^i est aussi un générateur si et seulement se i n'est pas divisible par q. Donc $\operatorname{Aut} C_q \simeq (\mathbb{Z}/q\mathbb{Z})^\times$. Nous avons démontré dans Proposition 4.6 que $(\mathbb{Z}/q\mathbb{Z})^\times$ est un groupe cyclique d'ordre $q-1$. Les homomorphismes $\phi : C_p \longrightarrow C_{q-1}$ sont déterminés par donner l'image d'un générateur (d'ordre p). Donc les homomorphismes non-triviaux sont en correspondance biunivoque avec les éléments d'ordre p de C_{q-1}. Si y est un générateur de C_{q-1} et $q - 1 = pm$, alors les éléments d'ordre p sont y^{im} où $1 \leq i < p$.

Exercice 7.11. Montrer directement que

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/210\mathbb{Z}.$$

mais que $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/420\mathbb{Z}$.

8. Théorèmes de Sylow

On a des résultats plus forts que celui de Cauchy, avec un peu plus de travail. Le résultat suivant n'est pas une curiosité, mais est fondamental. La plupart des preuves disponibles utilise des actions particulières.

Théorème 8.1 (Sylow). [18] *Soit G un groupe d'ordre $p^s m$, où $p \nmid m$ et p un nombre premier.*

(i) Pour chaque $1 \leq t \leq s$ il existe un sous-groupe $P < G$ d'ordre p^t.

(ii) Si P et Q sont deux sous-groupes de cardinalité p^s, alors il existe un $g \in G$ tel que

$$P = gQg^{-1}.$$

(iii) Soit N_{p^s} le nombre de sous-groupes de G de cardinalité p^s. On a que $N_{p^s} \equiv 1 \mod p$. Fixons un sous-groupe P d'ordre p^s. Alors $N_{p^s} = (G : N_G(P))$, donc N_{p^s} divise m.

Soit G un groupe d'ordre $p^s m$, où $p \nmid m$ et p premier. Un sous-groupe d'ordre p^s est appelé un *p-Sylow sous-groupe.*

Exercice 8.1. Chaque sous-groupe d'ordre p^t est contenu dans un p-Sylow-sous-groupe.

Exemple 8.1. Comme exemple d'utilisation du théorème de Sylow on va montrer qu'il n'existe pas un groupe simple d'ordre 36. Donc soit G un groupe d'ordre 36.

Si N_9 dénote le nombre de 3-Sylow sous-groupes, on a que $N_9 - 1$ est divisible par 3 et N_9 divise $36/9 = 4$. Donc $N_9 = 1$ ou 4. Si $N_9 = 1$, alors il existe un seul 3-Sylow-sous-groupe, donc est normal et propre et G n'est pas simple. Sinon on a quatre 3-Sylow-sous-groupes, donc l'action transitive par conjugaison sur l'ensemble des 3-Sylow-sous-groupes donne un homomorphisme non-trivial $\phi : G \longrightarrow S_4$ avec un noyau N. Alors $(G : N)$ divise $|S_4| = 24$ et donc $N \neq \{\mathbf{1}_G\}$. Alors G a un sous-groupe normal propre et G n'est pas simple.

Exercice 8.2. Il n'existe pas un groupe simple d'ordre 42, 84, 126, 140, ou 280. Indice: Montrer qu'il existe un sous-groupe normal de sept éléments.

Exercice 8.3. On connaît essentiellement les groupes d'ordre ≤ 15 :

Il existe essentiellement seulement un groupe d'ordre 1, 2, 3, 5, 7, 11, 13, 15 (le groupe cyclique).

Il existe seulement deux groupes non-isomorphes d'ordre 4, 6, 9, 10, 14.

Il existe seulement cinq groupes non-isomorphes d'ordre 8 (les groupes C_8,$C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 et Q ne sont pas isomorphes) et aussi cinq groupes non-isomorphes d'ordre 12.

(Indice pour ordre 12. Un 3-Sylow P_3 est C_3, un 2-Sylow P_2 est C_4 ou $C_2 \times C_2$. On a $N_3 = 1$ ou 4 et $N_4 = 1$ ou 3. G est abélien si et seulement si $N_4 = N_3 = 1$: deux possibilités. Si $N_3 = 1$ et $N_4 \neq 1$, alors $P_3 \lhd G$ et $G \simeq P_3 \rtimes_\phi P_2$ pour un homomorphisme non-trivial $\phi : P_2 \longrightarrow \operatorname{Aut} P_3$: ça donne aussi deux possibilités différents. Si $N_4 = 1$ et $N_3 \neq 1$, alors $P_2 \lhd G$ et $G \simeq P_2 \rtimes_\phi P_3$ pour un homomorphisme non-trivial $\phi : P_3 \longrightarrow \operatorname{Aut} P_2$; seulement possible si $P_2 \simeq C_2 \times C_2$: ça donne un groupe. Le cas $N_4 = 3$ et $N_3 = 4$ est impossible : sinon on aurait un élément d'ordre 1, huit éléments d'ordre 3 et au moins cinq éléments d'ordre deux ou quatre : c'est trop.)

[18] L. Sylow (1832-1918), mathématicien norvégien, voir http://www.gap-system.org/ history/Biographies/Sylow.html.

Exercice 8.4. Chaque groupe d'ordre p^2q possède un sous-groupe normal propre, où p, q sont des nombres premiers.

8.1. **Première preuve du théorème de Sylow.** Nous allons briser la preuve du théorème en deux parties.

Preuve d'existence de p-Sylow sous-groupes. Nous allons utiliser induction sur $O(G)$; si $O(G) = 1$ il n'y a rien à montrer. Supposons l'existence d'un p-Sylow sous-groupe pour les groupes d'ordre plus petit que $O(G) = p^s m$, où $p \not| m$.

Soit X la collection des éléments d'ordre p de G. On laisse G agir sur X par conjugaison. Par le théorème de Cauchy on a que

$$|X| = n_p \equiv p - 1 \mod p.$$

Donc il existe au moins une orbite (classe de conjugaison) $\mathrm{Orb}(s)$ telle que p ne divise pas son ordre. Le stabilisateur de s est égal au centralisateur $C_G s$ et p ne divise pas $|\mathrm{Orb}(s)| = O(G)/O(C_G s)$; donc p^s divise l'ordre de $C_G s$.

Si $C_G s \neq G$ on conclut par induction que $C_G s$ a un sous-groupe d'ordre p^s, et on est prêt. Sinon, $< s > \lhd C_G s = G$ et par induction $G/ < s >$ contient un sous-groupe Q d'ordre p^{s-1}, parce que $O(G/ < s >) = p^{s-1}m$. Par le théorème de correspondance il existe un sous-groupe P contenant s tel que $Q = P/ < s >$ et alors $|P/ < s > | = p^{s-1}$. Donc par Lagrange on a $|P| = p^s$ et on a trouvé un p-Sylow sous-groupe. □

Pour finir la preuve de (i) on utilise Exercice 7.7.

La partie restante de la preuve du théorème de Sylow. On suppose encore que $O(G) = p^s m$, $p \not| m$. Premièrement, soit Y la collection des p-Sylow sous-groupes de G; on vient de montrer que Y n'est pas vide. Le groupe G agit sur Y par conjugaison et agit possiblement avec plusieurs orbites. On va montrer qu'il n'y a qu'une. Soit P un p-Sylow sous-groupe quelconque.

Soit X le G-orbite d'une des p-Sylow sous-groupes, disons Q; donc

$$X = \mathrm{Orb}(Q) = \{gQg^{-1}; g \in G\} \subseteq Y.$$

Le stabilisateur de Q pour cette G-action est exactement le normalisateur $N_G Q$ et $Q \lhd N_G Q$. Donc $|X| = O(G)/O(N_G Q)$ divise m et p ne divise pas $|X|$.

Par restriction, le groupe P agit aussi sur X par conjugaison. On a, par Lemma 6.2 car P est un p-groupe,

$$|X| \equiv |X^P| \mod p.$$

Parce que $p \not| |X|$, il suit que $p \not| |X^P|$ et qu'il existe un point fixe pour P sur X, disons le p-Sylow sous-groupe $Q_1 \in X$. Cela veut dire que pour chaque $p \in P$ on a $pQ_1p^{-1} = Q_1$, ou que $P \subseteq N_G Q_1$.

Par le deuxième théorème d'isomorphisme PQ_1 est un sous-groupe d'ordre

$$O(P)O(Q_1)/O(P \cap Q_1),$$

alors $O(PQ_1)$ est de la forme p^t où $t \geq s$. Mais s est le maximum possible. Il suit que $O(PQ_1) = O(P) = O(Q_1) = p^s$ et $P = Q_1$.

La conclusion est que P est l'unique point fixe dans chaque G-orbite X. Mais deux G-orbites différentes sont disjointes, donc il n'existe qu'une seule G-orbite sur Y. C'est à dire, si P et Q sont deux p-Sylow sous-groupes, alors il existe un $g \in G$ tel que $Q = gPg^{-1}$.

Il suit aussi que N_{p^s} (le nombre de p-Sylow sous-groupes) est égal à $O(G)/O(N_G P) = (G : N_G P)$ et donc divise $O(G)/O(P) = m$.

Et finalement P est le seul point fixe sur $X = Y$ pour l'action de P par conjugaison, donc encore une fois par Lemme 6.2 on a

$$N_{p^s} = |Y| \equiv |Y^P| = 1 \mod p.$$

□

8.2. **Une autre preuve du théorème de Sylow.** [19] Nous allons présenter une deuxième preuve du théorème de Sylow, en utilisant d'autre actions.

Nous aurons besoin d'un résultat plus général. Pour un ensemble X et un entier positif n nous notons

$$\binom{X}{n} := \{A \subset X;\ |A| = n\},$$

pour la collection des sous-ensembles de cardinalité n. Nous avons choisi cette notation parce que

$$\left|\binom{X}{n}\right| = \binom{|X|}{n}.$$

Si X est un G-ensemble avec l'opération $g \bullet x$, alors $\binom{X}{n}$ devient aussi un G-ensemble avec l'opération

$$g \bullet A := \{g \bullet a;\ a \in A\} \in \binom{X}{n}.$$

Lemme 8.1. *Soit X un ensemble de cardinalité $|X| = p^s m$, où $p \nmid m$ et p un nombre premier. Et soit P un groupe d'ordre p^r, pour un $r \in \mathbb{Z}$.*

(i) Alors $\binom{|X|}{p^s} \equiv m \mod p$.

(ii) Supposons que X est un P-ensemble. Alors il existe un sous-P-ensemble Y de X de cardinalité p^s.

(iii) En particulier, si $s = 0$, il existe un point fixe dans X pour l'opération de P.

Preuve. On a

$$\binom{|X|}{p^s} = \binom{p^s m}{p^s} = \prod_{i=0}^{p^s-1} \frac{p^s m - i}{p^s - i}.$$

Soit $0 < i < p^s$, alors on peut écrire $i = p^{t_i} n_i$, où $p \nmid n_i$ et $0 \leq t_i < s$. Donc

$$\frac{p^s m - i}{p^s - i} = \frac{p^{s-t_i} m - n_i}{p^{s-t_i} - n_i}.$$

Le translaté $(p^{s-t_i} - n_i) + p\mathbb{Z} = -n_i + p\mathbb{Z}$ n'est pas $0 + p\mathbb{Z}$, donc il existe un inverse

$$(-n_i + p\mathbb{Z})^{-1} = r_i + p\mathbb{Z}$$

dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors on peut calculer dans $\mathbb{Z}/p\mathbb{Z}$:

[19] Ne fait pas partie de la matière examen

$$\begin{aligned}\binom{|X|}{p^s}+p\mathbb{Z} &= m\prod_{i=1}^{p^s-1}\frac{p^{s-t_i}m-n_i}{p^{s-t_i}-n_i}+p\mathbb{Z}\\ &= (m+p\mathbb{Z})\prod_{i=1}^{p^s-1}\left((p^{s-t_i}m-n_i)+p\mathbb{Z}\right)\left((p^{s-t_i}-n_i)+p\mathbb{Z}\right)^{-1}\\ &= (m+p\mathbb{Z})\prod_{i=1}^{p^s-1}(-n_i+p\mathbb{Z})\,(-n_i+p\mathbb{Z})^{-1}\\ &= m+p\mathbb{Z}.\end{aligned}$$

En particulier $\left|\binom{X}{p^s}\right|$ n'est pas divisible par p. Donc si P opère sur X il existe un point fixe dans $\binom{X}{P^s}$ par Lemme 6.2. Donc il existe un sous-P-ensemble de X de cardinalité p^s. □

Maintenant nous pouvons donner la deuxième preuve du théorème de Sylow.

Preuve du théorème de Sylow. Dans chaque partie de la preuve on va utiliser une autre action.

(i) Le groupe G agit sur $X = G$ par $g \bullet x := gx$ (la multiplication du groupe). Donc G agit aussi sur $Y := \binom{G}{p^s}$. Soit $A \in Y$; alors A est un sous-ensemble de G de p^s éléments.

Si A est même un sous-groupe de G, alors $\mathrm{Orb}(A) = \{gA;\ g \in G\} = G/A \subset \binom{G}{p^s}$ est la collection des translatés de A par un élément de G, donc $|\,\mathrm{Orb}(A)| = (G : A) = m$.

Supposons que A n'est pas un translaté d'un sous-groupe. Soit $a \in A$, alors $\mathbf{1}_G \in a^{-1}A$. Si $g \in \mathrm{Stab}(a^{-1}A)$ alors $g\mathbf{1} = g \in a^{-1}A$, donc $\mathrm{Stab}(a^{-1}A) \subset a^{-1}A$. Par hypothèse $a^{-1}A$ n'est pas un sous-groupe de G donc $|\,\mathrm{Stab}(a^{-1}A)| < p^s$ (strict) et

$$|\,\mathrm{Orb}(A)| = |\,\mathrm{Orb}(a^{-1}A)| = \frac{|G|}{|\,\mathrm{Stab}(a^{-1}A)|} > \frac{p^s m}{p^s} = m$$

et $|\,\mathrm{Orb}(A)|$ divise $p^s m$. Alors p divise $|\,\mathrm{Orb}(A)|$.

Donc p divise $|\,\mathrm{Orb}(A)|$ si et seulement si A n'est pas un translaté d'un sous-groupe.

Soit $Y' \subset Y$ la collection des translatés des sous-groupes d'ordre p^s. Un tel sous-groupe a exactement m translatés. Donc $N_{p^s} = \frac{|Y'|}{m}$ et on vient de montrer que $|Y| - |Y'|$ est un p-multiple. Par le lemme p divise $|Y| - m$, donc p divise aussi $|Y'| - m$ et $N_{p^s} - 1$. En particulier, $N_{p^s} \geq 1$, alors il existe un sous-groupe d'ordre p^s.

Pour finir la preuve de (i) on utilise Exercice 7.7.

(ii) Soient P et Q deux sous-groupes de cardinalité p^s. Laissons G agir maintenant sur $X = G$ par conjugaison. Donc il y a aussi une G-opération sur $Y = \binom{G}{p^s}$ définie par $g \odot A := \{gag^{-1}; a \in A\}$. On peut interpréter P et Q comme éléments de Y. Soit

$$Z := \mathrm{Orb}_G(P) = \{gPg^{-1};\ g \in G\}$$

sa G-orbite. On a $\mathrm{Stab}_G(P) = N_G P > P$, donc $|Z| = |G|/|N_G P|$ divise m.

Par restriction on peut aussi considérer Z comme Q-ensemble. Le groupe Q a cardinalité p^s, donc par Lemme 6.2 il y a un point fixe dans Z, disons $A = g^{-1}Pg$, pour cette opération de Q. Donc gQg^{-1} fixe P, ça veut dire que $gQg^{-1} \subset N_G(P)$.

L'image $\nu_P(gQg^{-1})$ par l'application naturelle $\nu_P : \ N_G(P) \longrightarrow N_G(P)/P$ est un sous-groupe de $N_G(P)/P$, donc son ordre est un diviseur de m. Mais $\nu_P(gQg^{-1})$ est aussi un groupe quotient de gQg^{-1}, donc son ordre divise p^s. Donc l'image est trivial et $gQg^{-1} \subset P$. Mais les deux sous-groupes P et gQg^{-1} ont cardinalité p^s, donc

$$P = gQg_{-1}.$$

D'où (ii).

Et Z est l'ensemble des sous-groupes de cardinalité p^s, donc par définition $|Z| = N_{p^s}$. Alors $N_{p^s} = (G : N_G(P))$. Alors (iii). □

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA