7. Applications dans la théorie des groupes

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

7.1. **Un critère suffisant pour la normalité d'un sous-groupe.** Premièrement nous donnerons une condition suffisante pour qu'un sous-groupe soit normal, une généralisation du fait que, si l'indice 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 $H < G$ un sous-groupe tel que son indice $p := (G : H)$ soit le plus petit diviseur premier de $O(G)$. Alors $H \lhd G$.*

Démonstration. Le groupe G agit sur $X := G/H$ par multiplication à gauche ; son sous-groupe H agit alors 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 $h \in H$ et donc si et seulement si $g^{-1}hg \in H$ ou $g \in N_G(H)$ (le normalisateur de H). Donc le nombre de points fixes sous l'action de H est

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

et

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

Par le 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.

7.2. **Action par conjugaison.** Notre seconde application concerne l'action d'un groupe G sur lui-même que nous avons introduite à la sous-section 6.6. Cette G-action est définie par

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

pour $g \in G$ et $x \in X := G$ et nous avons déjà vérifié que cette défintion satisfait les conditions caractérisant les actions de groupe. Les G-orbites de cette action sont appelées *classes de conjugaison.*

L'élément $x \in G$ est un point fixe pour cette action si et seulement si $gx = xg$ pour tout $g \in G$ 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 il est montré que, pour chaque matrice unitaire $u \in G$, il existe une autre matrice unitaire $v \in G$ telle que $v^{-1}uv = \Lambda$ où Λ est une matrice diagonale. En fait, on peut prendre comme i-ème colonne de v un vecteur propre de u avec valeur propre Λ_{ii}. Si $f(t)$ est un polynôme unitaire[20] 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. Il y a donc une bijection entre les classes de conjugaison de G et les polynômes unitaire de degré n dont toutes les racines sont de valeur absolue 1.

La preuve de la proposition suivante utilise l'action par conjugaison.

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}. Si P n'est pas abélien, alors $P/Z(P)$ n'est pas cyclique.

Démonstration. 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 le lemme 6.2. Donc p divise $|Z(P)|$. Mais le neutre est dans le centre et il y a donc encore au moins $p-1$ éléments dans $Z(P)$.

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

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

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 maintenant que $|Z(P)| = p^{r-1}$ et donc que P n'est pas abélien. Mais alors le groupe quotient $P/Z(P)$ est cyclique d'ordre p et P est abélien, ce qui est une contradiction. □

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

Exemple 7.2. Les groupes d'ordre p^3 ne sont pas nécessairement abéliens. Le groupe diédral D_4 (isomorphe à $U(3, \mathbb{F}_2)$) d'ordre 8 en est un exemple. Un second exemple est le groupe des quaternions de Hamilton : $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ de centre $\{1, -1\}$ et multiplication

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

Ce groupe Q possède six éléments d'ordre 4 et n'est donc pas isomorphe à D_4 qui n'en a que deux.

Exercice 7.4. Montrer qu'un groupe d'ordre p^s est résoluble (avec p un nombre premier).

20. Un polynôme de degré n est *unitaire* si le coefficient de son terme de degré n est 1. Le mot anglais pour cette propritété est *monic*.

7.3. **Théorème de Cauchy.** Notre troisième application est le théorème de Cauchy qui dit que, pour chaque diviseur premier de l'ordre du groupe, il existe un élément de cet ordre. Ce résultat est très utile. La preuve utilise aussi une action de groupe.

Théorème 7.1 (Cauchy[21]). *Soit G un groupe fini et soit p un diviseur premier de $|G|$. Alors le groupe contient au moins un élément d'ordre p.*

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 $p - 1$.

Démonstration. Dans cette preuve, ce n'est pas G qui agit, mais un groupe cyclique $P = \langle \sigma \rangle$ d'ordre p. Sur l'ensemble

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

définissons une P-action par

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

c'est-à-dire la permutation cyclique des coefficients. Donc σ^p agit trivialement et si $g_1 g_2 \ldots g_p = \mathbf{1}$, alors

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

Les points fixes sont facilement identifiables. Un point $(g_1, g_2, \ldots, g_p)$ appartient à 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

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

Si $g^p = 1$, alors $O(g) = p$ ou $O(g) = 1$ (et donc $g = \mathbf{1}_G$), puisque p est premier. Ainsi

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

L'application

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

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 le lemme 6.2), le nombre

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

est divisible par p. Par 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 $\langle x \rangle$). 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. □

21. Augustin-Louis Cauchy, mathématicien français, 1789-1857.

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 $H \neq G$, l'entier n divise l'indice $(G : H)$. 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 maintenant que le résultat soit vrai pour les groupes d'ordre inférieur à $O(G)$ et que p soit 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 $h \in G$ et on a donc trouvé un élément d'ordre p dans G. La preuve est alors complète pour ce cas.

Supposons, par contre, que l'entier p ne divise $O(H)$ pour aucun sous-groupe $H < G$ tel que $H \neq G$. Alors, pour chaque sous-groupe propre H, l'entier p divise l'indice $(G : H)$. Ceci implique que, pour chaque G-action et chaque orbite Orb telle que $|\operatorname{Orb}| > 1$, p divise $|\operatorname{Orb}|$. Considérons maintenant l'action de G sur soi-même par conjugaison. L'équation de classe donne

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

où la somme est sur les classes de conjugaison d'ordre > 1. Cette somme donc est divisible par p. On obtient que $O(Z(G))$ est aussi divisible par p. Il suit que $Z(G) = G$ et donc que G est abélien (car, par hypothèse, 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 $g \in G$ un élément distinct du neutre. Si $O(g) = np$ alors $O(g^n) = p$ et la preuve est terminée. Supposons alors que p ne divise pas $O(g) =: n$ et donc aussi que $H := \langle g \rangle \neq G$. 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'est-à-dire $kH \neq H$ et $k^pH = H$.

Parce que p et n sont relativement premiers, 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 $kH \neq H$.

L'identité $k^pH = H$ 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 et est donc de la forme $O(k) = mp$. Il suit que k^m est d'ordre p et que G contient donc 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 aussi 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 la 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

$$C_G(g_1) = G; \quad C_G(g_3) = \langle\, g_3 \,\rangle; \quad C_G(g_4) = \langle\, g_4 \,\rangle; \quad C_G(g_7) = \langle\, g_7 \,\rangle = \langle\, g_7^{-1} \,\rangle = C_G(g_7^{-1})$$

et

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

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

$$n_1 = 1, \quad n_2 = 21, \quad n_3 = 56, \quad n_4 = 42 \quad \text{et} \quad n_7 = 48$$

et $n_i = 0$ si $i \notin \{1, 2, 3, 4, 7\}$. Montrer que les polynômes caractéristiques de g_7 et g_7^{-1} sont différents et qu'il y a deux classes de conjugaison d'éléments d'ordre 7 et six classes de conjugaison en tout.

7.4. **Produits semi-direct.** 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

$$\phi :\ G \to \mathrm{Aut}\, N$$

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

$$N \rtimes_\phi G$$

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

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

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

Démonstration. L'application $\phi : G \to \mathrm{Aut}\, N$ 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 « $\circ$ » d'applications).

Vérifions maintenant l'associativité :

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

Il reste à trouver le neutre et montrer que toute paire $(n, g) \in N \times G$ possède un inverse pour $*$. C'est ce que l'exercice qui suit propose de faire. □

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

On peut caractériser les groupes qui sont isomorphes à des produits semi-directs. Le résultat principal est le suivant (comparer 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 $\phi : B \to \operatorname{Aut} A$ par $\phi(b)(a) := bab^{-1}$. Alors $H \simeq (A \rtimes_\phi B)$.*

Démonstration. L'application $\psi : A \rtimes_\phi B \to H$ définie par

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

est un homomorphisme de groupes puisque

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

Elle est surjective parce que $H = AB$ et injective 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. Le groupe alterné Alt_4 est un produit semi-direct du groupe V_4 de Klein et du groupe cyclique $C_3 \simeq \{\mathbf{1}, (123), (132)\}$. (Identifier lequel de ces sous-groupes joue le rôle de A ci-dessus, vérifier les hypothèses et vérifier que Alt_4 est bien $\simeq (A \rtimes_\phi B)$. Est-ce que Alt_4 est isomorphe à un produit direct de ces deux sous-groupes.)

Exercice 7.11. Les groupes diédraux D_n sont des produits semi-directs. (Suivre la description de la proposition ci-dessus : identifier un sous-groupe normal A et un sous-groupe B tels que $A \cap B = \{\mathbf{1}\}$ et $AB = D_n$. Vérifier enfin que le morphisme ϕ proposé avec la loi produit d'un groupe semi-direct reproduit l'opération interne de D_n.)

Exercice 7.12. Soit K un corps, B le groupe des matrices triangulaires supérieure inversibles, T celui des matrices diagonales inversibles et U celui des matrices triangulaires supérieures unipotentes. Si $n = 3$, les éléments de B, T et U sont respectivement de la forme

$$\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}, \qquad \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

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

Chaque groupe d'ordre pq est un produit semi-direct si p et q sont deux nombres premiers distincts.

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

Démonstration. 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 la proposition 7.1. On a $A \cap B = \{\mathbf{1}_G\}$ et $AB = G$. En effet tous les éléments de A sont d'ordre q (sauf l'identité) et tous ceux de B d'ordre p (sauf l'identité). Ceci mène à $A \cap B = \{\mathbf{1}_G\}$. De plus, deux paires distinctes (a, b) et (a', b') avec $a, a' \in A$ et $b, b' \in B$ produisent des éléments ab et $a'b'$ distincts, car $ab = a'b'$ implique $a'^{-1}a = b'b^{-1} \in A \cap B = \{\mathbf{1}_G\}$ et donc $a = a'$ et $b = b'$. Il y a pq paires distinctes (a, b) et donc $AB = G$. Donc, avec l'application $\phi : \ B \to \operatorname{Aut} A$ définie par $\phi(b)(a) := bab^{-1}$, la proposition précédente donne $G \simeq A \rtimes_\phi B$.

Le groupe G est abélien si et seulement si ϕ est trivial, c'est-à-dire $\phi(g) = \mathbf{1}$ pour tout g (exercice : le montrer). Examinons donc le cas où ϕ est non triviale. Le groupe A est cyclique d'ordre q. Soit a un générateur de A. Alors $\phi(a)$ est aussi un générateur et il existe donc 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 $O(\operatorname{Aut}(A)) = q - 1$. Puisque ϕ n'est pas triviale, l'image $\phi(B)$ ne le sera pas non plus et sera donc isomorphe à B (parce que B est isomorphe au groupe cyclique d'ordre p avec p premier). Donc $p = O(B)$ divise $O(\operatorname{Aut}(A)) = q - 1$. □

Remarque. Pour connaître les groupes non abéliens d'ordre pq, il suffit donc de connaître $\operatorname{Aut} C_q$ et les homomorphismes $C_p \to \operatorname{Aut} C_q$. Soit a un générateur de C_q ; 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 montré à la proposition 4.6 que $(\mathbb{Z}/q\mathbb{Z})^\times$ est un groupe cyclique d'ordre $q - 1$. Un homomorphisme $\phi : C_p \to C_{q-1}$ est déterminé en donnant 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 les y^{im} pour $1 \leq i < p$.

Exercice 7.13. 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

Des résultats plus fins que celui de Cauchy peuvent être obtenus avec un peu plus de travail. Le résultat suivant n'est pas une curiosité : il est fondamental. Les quelques preuves de ce théorème utilisent diverses actions.

Théorème 8.1 (Sylow [22]). *Soit G un groupe d'ordre $p^s m$, où $p \nmid m$ et p est 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 élément $g \in G$ tel que

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

(iii) Le nombre de sous-groupes N_{p^s} de G de cardinalité p^s satisfait $N_{p^s} \equiv 1 \bmod p$. Si P est un sous-groupe d'ordre p^s, alors $N_{p^s} = (G : N_G(P))$ et donc N_{p^s} divise m.

Soit G un groupe d'ordre $p^s m$ où $p \nmid m$ et p est premier. Un sous-groupe d'ordre p^s est appelé un *p-sous-groupe de Sylow*. Les sous-groupes de G dont l'ordre est une puissance de p sont appelés p-sous-groupes. (En français, le nom de p-sous-groupe de Sylow est parfois raccourci en p-Sylow. Il faut alors distinguer les p-Sylow des p-sous-groupes, $1 \leq t < s$, dont l'existence est prédite par le théorème ci-dessus.)

Exercice 8.1. (i) Puisque $|S_4| = 2^3 \cdot 3$, ce groupe possède au moins un sous-groupe d'ordre 8. Trouver tous les sous-groupes d'ordre 8 de S_4 et vérifier que $N_{2^3} \equiv 1 \bmod 2$ et divise 3.
(ii) Même question pour Alt_4.

Exercice 8.2. Chaque sous-groupe d'ordre p^t est contenu dans un p-sous-groupe de Sylow.

Exemple 8.1. Comme exemple d'utilisation du théorème de Sylow, nous montrons qu'il n'existe pas un groupe simple d'ordre 36.

Soit G un groupe d'ordre 36. Si N_9 dénote le nombre de 3-sous-groupes de Sylow, alors $N_9 - 1$ 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-sous-groupe de Sylow qui est donc normal et propre, et G n'est pas simple. Sinon il y a quatre 3-sous-groupes de Sylow et l'action par conjugaison sur l'ensemble de ces 3-sous-groupes de Sylow est transitive et donne un homomorphisme non trivial $\phi : G \to S_4$ avec un noyau N. Alors $(G : N)$ divise $|S_4| = 24$ et donc $N \neq \{\mathbf{1}_G\}$. Ainsi G possède un sous-groupe normal propre et G n'est pas simple.

Exercice 8.3. Il n'existe pas de groupe simple d'ordre 42, 84, 126, 140, ou 280.
Indice : montrer qu'il existe un sous-groupe normal de sept éléments.

Exercice 8.4. Le théorème de Sylow permet de dresser une liste complète des groupes d'ordre ≤ 15 à isomorphisme près :

- les seuls groupes d'ordre 1, 2, 3, 5, 7, 11, 13, 15 sont les groupes cycliques de ces ordres ;
- il existe seulement deux groupes non isomorphes d'ordre 4, 6, 9, 10, 14 et

22. L. Sylow (1832-1918), mathématicien norvégien. Voir
http ://www.gap-system.org/∼history/Biographies/Sylow.html.

- il existe précisément cinq groupes non isomorphes d'ordre 8 (ce sont les groupes C_8,$C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 et Q) et cinq groupes non isomorphes d'ordre 12.

Indice pour l'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 $\phi : P_2 \to \operatorname{Aut} P_3$: ceci donne aussi deux possibilités différentes. 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 $\phi : P_3 \to \operatorname{Aut} P_2$ (seulement possible si $P_2 \simeq C_2 \times C_2$) : ceci donne un groupe. Le cas $N_4 = 3$ et $N_3 = 4$ est impossible car il y aurait alors un élément d'ordre 1, huit éléments d'ordre 3 et au moins cinq éléments d'ordre deux ou quatre pour un total dépassant 12.)

Exercice 8.5. 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-sous-groupes de Sylow par induction sur $O(G)$. Si $O(G) = 1$, il n'y a rien à montrer. Supposons l'existence d'un p-sous-groupe de Sylow pour les groupes d'ordre plus petit que $O(G) = p^s m$, où $p \nmid m$.

Soit X la collection des éléments d'ordre p de G. Le groupe G agit sur X par conjugaison. Le théorème de Cauchy donne que

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

Donc il existe au moins une orbite $\operatorname{Orb}(s)$ (c'est-à-dire une classe de conjugaison) telle que p ne divise pas son ordre. Si $\operatorname{Stab}_G(s)$ est le stabilisateur de s, alors p ne divise pas $|\operatorname{Orb}(s)| = O(G)/O(\operatorname{Stab}_G(s))$; donc p^s divise l'ordre de $\operatorname{Stab}_G(s)$.

Si $\operatorname{Stab}_G(s) \neq G$, alors l'hypothèse d'induction assure l'existence d'un sous-groupe de $\operatorname{Stab}_G(s)$ d'ordre p^s qui est la conclusion désirée. Sinon, $\langle s \rangle \lhd \operatorname{Stab}_G(s) = G$ et par induction $G/\langle s \rangle$ contient un sous-groupe Q d'ordre p^{s-1}, parce que $O(G/\langle s \rangle) = p^{s-1}m$. Par le théorème de correspondance, il existe un sous-groupe P contenant s tel que $Q = P/\langle s \rangle$. Puisque $|Q| = |P/\langle s \rangle| = p^{s-1}$, le théorème de Lagrange dit que $|P| = p^s$ et un p-Sylow a été trouvé. □

Pour finir la preuve de (i), on utilise l'exercice 7.7.

Le reste de la preuve du théorème de Sylow. On suppose encore que $O(G) = p^s m$, $p \nmid m$. Tout d'abord, soit Y la collection des p-Sylow de G ; la preuve d'existence a montré que Y n'est pas vide. Le groupe G agit sur Y par conjugaison et cette action a possiblement plusieurs orbites. Nous montrons maintenant qu'il n'y en a qu'une.

Soit P un p-Sylow quelconque. Soit X la G-orbite d'un autre des p-Sylow, disons Q ; donc

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

Le stabilisateur de Q pour cette G-action est exactement le normalisateur $N_G(Q)$ et $Q \lhd N_G(Q)$. Puisque $|Q| = p^s$, alors $|X| = O(G)/O(N_G(Q))$ divise m.

Par restriction, le groupe P agit aussi sur X par conjugaison. Puisque p divise l'ordre de P, le lemme 6.2 donne

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

Parce que $p \nmid |X|$, il suit que $p \nmid |X^P|$ et donc qu'il existe un point fixe pour l'action de P sur X, disons le p-Sylow $Q_1 \in X$. Ceci veut dire que, pour chaque $p \in P$, $pQ_1p^{-1} = Q_1$ ou encore 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 donc que P est l'unique point fixe dans X sous l'action par conjugaison de P. Mais deux G-orbites différentes sont disjointes, donc il n'existe qu'une seule G-orbite dans Y, c'est-à-dire, si P et Q sont deux p-sous-groupes de Sylow, alors il existe un $g \in G$ tel que $Q = gPg^{-1}$. Ainsi le nombre de p-Sylow est $N_{p^s} = |X|$ et divise donc m.

Finalement P est le seul point fixe sur $X = Y$ pour l'action de P par conjugaison ; donc, encore une fois, le lemme 6.2 donne

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

□

Exercice 8.6. VRAI ou FAUX.
(i) Le théorème de Sylow s'applique également quand $|G| = p^s$.
(ii) Un groupe fini abélien d'ordre $p^s m$ a un unique p-sous-groupe de Sylow.
(iii) Les groupes diédraux D_{p^s} avec p premier possèdent un unique p-sous-groupe de Sylow.

8.2. **Une autre preuve du théorème de Sylow.**[23] Nous allons présenter une deuxième preuve du théorème de Sylow, en utilisant d'autres actions.

Nous aurons besoin d'un résultat technique. Pour un ensemble X et un entier positif n, notons la collection des sous-ensembles de cardinalité n par

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

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

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

23. Ne fera pas partie de la matière à l'examen.

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

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

(ii) Soit X 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.

Démonstration. On a

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

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 $0 + p\mathbb{Z}$; il existe donc 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 $\mathbb{Z}/p\mathbb{Z}$:

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

Ainsi, $\left|\binom{X}{p^s}\right|$ n'est pas divisible par p. Alors, si P opère sur X, il existe un point fixe dans $\binom{X}{p^s}$ par le lemme 6.2. Ainsi 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. Chaque partie de la preuve utilise une action distincte.

(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.

D'une part, si A est en plus un sous-groupe de G, alors $\operatorname{Orb}(A) = \{gA;\ g \in G\} = G/A \subset \binom{G}{p^s}$ est la collection des translatés de A par un élément de G et $|\operatorname{Orb}(A)| = (G : A) = m$.

D'autre part, si A n'est pas le translaté d'un sous-groupe, alors p divise $|\operatorname{Orb}(A)|$; c'est ce que nous montrons maintenant. Soit $a \in A$, alors $\mathbf{1}_G \in a^{-1}A$. Si $g \in \operatorname{Stab}(a^{-1}A)$, alors $g\mathbf{1} = g \in a^{-1}A$ et $\operatorname{Stab}(a^{-1}A) \subset a^{-1}A$. Par hypothèse $a^{-1}A$ n'est pas un sous-groupe de G ; donc $\operatorname{Stab}(a^{-1}A) \subsetneq a^{-1}A$ et $|\operatorname{Stab}(a^{-1}A)| < p^s$ (inégalité stricte) ce qui donne

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

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

Donc p divise $|\operatorname{Orb}(A)|$ 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. Comme nous avons vu, 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 multiple de p. Par le lemme, p divise $|Y| - m$, donc p divise aussi $|Y'| - m$ et $N_{p^s} - 1$. En particulier, $N_{p^s} \geq 1$ et il existe alors un sous-groupe d'ordre p^s.

Pour finir la preuve de (i), on utilise comme précédemment l'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

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

l'orbite de P sous G. On a $\operatorname{Stab}_G(P) = N_G(P) > P$ et 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 et, par le lemme 6.2, il y a un point fixe dans Z pour cette action de Q, disons $A = g^{-1}Pg$. Donc gQg^{-1} fixe P, ce qui veut dire que $gQg^{-1} \subset N_G(P)$.

L'image $\nu_P(gQg^{-1})$ par l'application naturelle $\nu_P :\ N_G(P) \to N_G(P)/P$ est un sous-groupe de $N_G(P)/P$ dont l'ordre est un diviseur de m. Mais $\nu_P(gQg^{-1})$ est aussi un groupe quotient de gQg^{-1} et son ordre divise p^s. Donc cette image est triviale et $gQg^{-1} \subset P$. Mais les deux sous-groupes P et gQg^{-1} ont même cardinalité p^s et $P = gQg^{-1}$, qui est l'énoncé (ii).

Puisque Z est l'ensemble des sous-groupes de cardinalité p^s, le nombre N_{p^s} est par définition $|Z|$. Or nous avons noté plus haut que $|Z| = (G : N_G(P))$ divise m qui est l'énoncé (iii). $\square$