(iii) Un résultat difficile et fameux, dû à Feit-Thompson,[14] affirme que *tout groupe d'ordre impair est résoluble*. C'est un indicateur du fait qu'il est très difficile de classifier les groupes finis résolubles.

Terminons par un exemple important de groupes résolubles. Fixons k un corps, $n \geqslant 1$ un entier, notons $\mathrm{T}_n(k) \subset \mathrm{GL}_n(k)$ le sous-groupe des matrices triangulaires supérieures, et On a $\mathrm{T}_1(k) = k^\times$ qui est abélien, donc résoluble. Plus généralement, pour $n \geqslant 1$ on a une suite exacte courte

$$1 \longrightarrow \mathrm{U}_n(k) \xrightarrow{\text{can}} \mathrm{T}_n(k) \xrightarrow{\text{diag}} (k^\times)^n \to 1,$$

où $\mathrm{U}_n(k)$ est le sous-groupe de $\mathrm{T}_n(k)$ constitué des g tels que $g_{j,j} = 1$ pour tout $1 \leqslant j \leqslant n$ (*groupe des unipotents supérieurs*). Cela montre $\mathrm{D}(\mathrm{T}_n(k)) \subset \mathrm{U}_n(k)$. Pour $n = 2$, on constate que l'application $k \to \mathrm{U}_2(k)$, $x \mapsto \left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right]$, est un isomorphisme de groupes (où k est vu comme groupe additif), donc $\mathrm{T}_2(k)$ est résoluble.

Proposition 6.13. *Le groupe $\mathrm{T}_n(k)$ est résoluble de classe $\leqslant 1 + \lceil \log_2(n) \rceil$.*

Démonstration — Soient $G = \mathrm{T}_n(k)$ et $e_1, \ldots, e_n$ la base canonique de k^n. Pour $1 \leqslant i \leqslant n$, on pose $V_i = \sum_{j=1}^{i} k e_j$, et aussi $V_i = \{0\}$ pour $i \leqslant 0$. Pour tout $g \in G$ on a $g(V_i) \subset V_i$ pour tout i. Pour tout $j \geqslant 1$, on pose

$$G_j = \{ g \in G \mid (g-1)(V_i) \subset V_{i-j}, \quad \forall\ i = 1, \ldots, n \}.$$

On a $G_1 = \mathrm{U}_n(k)$, $G_{j+1} \subset G_j$, et $G_j = \{1\}$ pour $j \geqslant n$. Pour $j > 1$, observons que G_j est le sous-ensemble de $\mathrm{U}_n(k)$ des éléments de $j-1$ premières surdiagonales nulles. Un peu de calcul matriciel montre que G_i est un sous-groupe de G. Alternativement, on peut remarquer que pour $g \in G_j$ et $g' \in G_j$ on a $gg' - 1 = g(g'-1) + (g-1)$ puis $(gg'-1)(V_i) \subset V_{i-j} + V_{i-j} \subset V_{i-j}$. De plus, on a aussi $1 \in G_j$ et $g^{-1} \in G_j$ par l'écriture $g^{-1} - 1 = (1-g)g^{-1}$. Enfin, pour $g \in G_j$ et $h \in G_{j'}$ on a

$$[g,h] - 1 = ghg^{-1}h^{-1} - 1 = ((g-1)(h-1) - (h-1)(g-1))g^{-1}h^{-1},$$

et donc $[G_j, G_{j'}] \subset G_{j+j'}$. On en déduit $\mathrm{D}^m(G_1) \subset G_{2^m}$ pour $m \geqslant 1$, puis $\mathrm{D}^m(G_1) \subset G_n = \{1\}$ pour $2^m \geqslant n$. On conclut car on a $\mathrm{D}(G) \subset G_1$. □

7. Le dévissage en produit semi-direct

Commençons par définir la notion de *complément* d'un sous-groupe.

Définition 7.1. *Si H est un sous-groupe d'un groupe G, un complément de H dans G est un sous-groupe K vérifiant $G = HK$ et $H \cap K = \{1\}$.*

La notion est bien sûr symétrique en H et K.

Lemme 7.2. *Soient H et K deux sous-groupes de G.*

(i) H et K sont complémentaires si, et seulement si, l'application $H \times K \to G, (h,k) \mapsto hk$, est bijective.

14. W. Feit & J. G. Thompson, *Solvability of groups of odd order*, Pac. J. Math. 13, 775–1029 (1963).

(ii) On suppose H et K finis. On a $|HK| = |H||K|/|H \cap K|$. En particulier, H et K sont complémentaires si, et seulement si, on a $H \cap K = \{1\}$ et $|G| = |H||K|$.

Démonstration — Soit $f : H \times K \to G, (h,k) \mapsto hk$. On a bien sûr f surjective $\iff G = HK$. Pour (h,k) et (h',k') dans $H \times K$, on a aussi

$$h'k' = hk \iff h^{-1}h' = k(k')^{-1} \iff \exists x \in H \cap K \text{ avec } h' = hx \text{ et } k' = x^{-1}k.$$

On en déduit que f est injective si, et seulement si, $H \cap K = \{1\}$. On en déduit aussi que si H et K sont finis, les fibres de f ont $|H \cap K|$ éléments, ce qui montre $|KH||H \cap K| = |K||H|$. Supposant $H \cap K = \{1\}$ on a donc $|G| = |HK| \iff |G| = |H||K|$. □

Exemple 7.3. *(i) Les compléments de A_n dans S_n sont les $\langle\sigma\rangle$ avec $\sigma \in \mathrm{S}_n \smallsetminus \mathrm{A}_n$ d'ordre 2.*

(ii) Soit $S \subset \mathrm{S}_4$ le stabilisateur d'un point dans $\{1,\dots,4\}$. On a $S \simeq \mathrm{S}_3$ et S est un complément de K_4 dans S_4.

(iii) Soient G abélien p-élémentaire et H un sous-groupe de G. Les compléments de H dans G sont les supplémentaires de $H^\sharp$ dans $G^\sharp$.

(iv) Si G est cyclique d'ordre 4, disons $G = \mu_4$, le sous-groupe $H = \mu_2$ n'admet pas de complément. En effet, un complément serait d'ordre 2, mais H est l'unique sous-groupe d'ordre 2 de G.

(v) Si $G = \mathrm{H}_8$, le sous-groupe $H = \langle I\rangle \simeq \mathbb{Z}/4\mathbb{Z}$ n'admet pas de complément. En effet, un complément serait d'ordre 2, mais l'unique sous-groupe d'ordre 2 de G est $\{\pm 1\}$, qui est inclus dans H.

On s'intéresse maintenant à la structure d'un groupe G possédant deux sous-groupes[15] N et K avec N distingué dans G et K complément de N dans G. L'observation importante, à la base de toute la discussion qui suit, est que l'on peut écrire, pour tout $n, n' \in N$ et $k, k' \in K$,

$$(nk)(n'k') = n(kn'k^{-1})kk' \quad \text{avec } kn'k^{-1} \in N. \tag{22}$$

Autrement dit, on a $(nk)(n'k') = n\,\mathrm{int}_k(n')\,kk'$. Ainsi, *la structure de groupe de G se déduit de celle de N, K et de la connaissance de l'application*

$$\alpha : K \to \mathrm{Aut}(N), k \mapsto \mathrm{int}_{k|N}.$$

Noter que α est un morphisme de groupes. Cela suggère l'existence d'une construction intrinsèque de G à partir de N, K et α : c'est ce qui va nous conduire à la notion de produit semi-direct.

On oublie donc temporairement le groupe G et l'on se fixe N et K deux groupes ainsi qu'un morphisme de groupes $\alpha : K \to \mathrm{Aut}(N), k \mapsto \alpha_k$. *Insistons sur le fait que les groupes N et K, ainsi que le morphisme α, sont arbitraires.* On munit *l'ensemble produit* $N \times K$ d'une nouvelle loi $\star_\alpha$, dépendante du choix de α, par la formule

$$(n,k) \star_\alpha (n',k') := (n\,\alpha_k(n'), kk'). \tag{23}$$

15. Nous noterons désormais N ce sous-groupe distingué, plutôt que H, d'une part pour rappeler qu'il est *normal*, d'autre part car la similarité des lettres h et k au tableau crée des confusions. Bien noter que la situation n'est pas symétrique en N et K, car K n'est pas supposé distingué.

LEMME 7.4. *La loi $\star_\alpha$ sur l'ensemble $N \times K$ définie par* (23) *est une loi de groupe. Son neutre est* $(1,1)$ *et on a* $(n,k)^{-1} = (\alpha_{k^{-1}}(n^{-1}), k^{-1})$.

DÉMONSTRATION — Pour le neutre, on a $(1,1) \star_\alpha (n,k) = (\alpha_1(n),k) = (n,k)$ et $(n,k) \star_\alpha (1,1) = (n\alpha_k(1),k) = (n,k)$. Pour l'associativité, c'est le calcul suivant, dans lequel on a $h,h',h'' \in H$ et $k,k',k'' \in K$: on a d'une part

$$((n,k) \star_\alpha (n,k')) \star_\alpha (n'',k'') = (n\alpha_k(n'),kk') \star_\alpha (n'',k'') = (n\alpha_k(n')\alpha_{kk'}(n''),kk'k'')$$

et d'autre part

$$(n,k) \star_\alpha ((n',k') \star_\alpha (n'',k'')) = (n,k) \star_\alpha (n'\alpha_{k'}(n''),k'k'') = (n\alpha_k(n'\alpha_{k'}(n'')),kk'k'')$$
$$= (n\alpha_k(n')\alpha_k(\alpha_{k'}(n'')),kk'k'') = (n\alpha_k(n')\alpha_{kk'}(n''),kk'k'')$$

puis l'associativité. L'assertion sur l'inverse est un simple calcul. Une autre manière de la vérifier consiste à constater que l'inverse de $(1,k)$ est $(1,k^{-1})$, l'inverse de $(n,1)$ est $(n^{-1},1)$, donc $(n,k) = (n,1)\star_\alpha(1,k)$ est nécessairement inversible d'inverse $(1,k^{-1}) \star_\alpha (n^{-1},1) = (\alpha_{k^{-1}}(n^{-1}),k^{-1})$. □

DÉFINITION 7.5. *Soient N et K deux groupes et $\alpha : K \to \mathrm{Aut}(N)$ un morphisme de groupes. La loi $\star_\alpha$ munit l'ensemble $N \times K$ d'une structure de groupe noté $N \rtimes_\alpha K$ et appelé* produit semi-direct (externe) de K par N associé à α.

Noter que dans le cas particulier $\alpha_k = \mathrm{id}_N$ pour tout k (morphisme trivial $\alpha = 1$), la loi $\star_\alpha$ est simplement la loi de groupe produit, et on a l'égalité de groupes

$$N \rtimes_1 K = N \times K.$$

Donnons un autre exemple plus intéressant.

EXEMPLE 7.6. Soit $\alpha : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, le morphisme défini par $\alpha_{\overline{k}}(x) = (-1)^k x$, pour $\overline{k} \in \mathbb{Z}/2\mathbb{Z}$ et $x \in \mathbb{Z}/m\mathbb{Z}$. La loi du groupe $\mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ s'écrit alors

$$(\overline{m},\overline{k}) \star_\alpha (\overline{m'},\overline{k'}) = (\overline{m} + (-1)^k\overline{m'}, \overline{k+k'}).$$

Pour $n \geqslant 3$, c'est un groupe non commutatif et on a un isomorphisme

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{D}_{2n},\ (\overline{m},\overline{k}) \mapsto c^m\tau^k.$$

En effet, la bijectivité est le fait que C et $\langle\tau\rangle$ sont compléments dans D_{2n} et le fait que c'est un morphisme est la relation $c^m\tau^k c^{m'}\tau^{k'} = c^{m+(-1)^k m'}\tau^{k+k'}$ pour $m,m',k,k' \in \mathbb{Z}$, qui se déduit de $\tau c = c^{-1}\tau$.

Revenons à la situation de la Définition 7.5 et terminons l'analyse-synthèse entamée depuis le début. Observons que $N' = N \times \{1\}$ et $K' = \{1\} \times K$ sont des sous-groupes de $N \rtimes_\alpha K$ respectivement isomorphes à N et K via $n \mapsto (n,1)$ et $k \mapsto (1,k)$. De plus, K' est un complément de N' dans $N \rtimes_\alpha K$: on a $N' \cap K' = \{(1,1)\}$ et $(n,k) = (n,1) \star_\alpha (1,k)$. Mieux, on a une suite exacte courte manifeste

$$1 \longrightarrow N \overset{n\mapsto(n,1)}{\longrightarrow} N \rtimes_\alpha K \overset{(n,k)\mapsto k}{\longrightarrow} K \longrightarrow 1.$$

Ainsi, N' est distingué dans $N \times_\alpha K$. Enfin, on a $(1,k) \star_\alpha (n,1) \star_\alpha (1,k)^{-1} = (\alpha_k(n),k) \star_\alpha (1,k^{-1}) = (\alpha_k(n),1)$: on est bien retombé sur la situation initiale ! La proposition suivante conclut cette longue discussion.

PROPOSITION 7.7. *Soient G un groupe, N un sous-groupe distingué de G et K un complément de N dans G. Soit $\alpha : K \to \mathrm{Aut}(N), k \mapsto \alpha_k$, le morphisme de groupes défini par $\alpha_k(n) = knk^{-1}$. Alors la bijection $N \times K \to G$, $(n,k) \mapsto nk$, est un isomorphisme de groupes $N \rtimes_\alpha K \xrightarrow{\sim} G$.*

Noter que le morphisme α de l'énoncé est bien défini car on a $N \lhd G$. On dit aussi que G est *produit semi-direct interne* de K par N et on écrit $G = N \rtimes K$. Le morphisme α est alors sous-entendu : c'est l'action de K par conjugaison sur N.

DÉMONSTRATION — On a $f((n,k) \star_\alpha (n',k')) = f(n\alpha_k(n'), kk') = n\alpha_k(n')kk' = nkn'k^{-1}kk' = nkn'k' = f(n,k)f(n,k')$ (c'est juste l'observation initiale (22) !). □

L'Exemple 7.3 fournit déjà quelques situations de produits semi-directs internes Mentionnons que lorsqu'on ne cherche pas à préciser le choix du morphisme α dans un produit semi-direct externe, on le note (dangereusement) parfois aussi $N \rtimes K$. Une proposition utile est alors la suivante.

PROPOSITION 7.8. (Suivi des isomorphismes) *Soient G, N et K comme dans la Prop. 7.7. Soient $a : N' \xrightarrow{\sim} N$ et $b : K' \xrightarrow{\sim} K$ des isomorphismes de groupes. Alors la bijection $N' \times K' \to G, (n',k') \mapsto a(n')b(k')$ est un isomorphisme de groupes $N' \rtimes'_\alpha K' \xrightarrow{\sim} G$, où $\alpha' : K' \to \mathrm{Aut}(N'), k' \mapsto \alpha_{k'}$, est le morphisme défini par*

$$\alpha'_{k'} = a^{-1} \circ \mathrm{int}_{b(k')} \circ a, \text{ pour } k' \in K'.$$

Autrement dit, si f désigne la bijection $N' \times K' \to G$ de l'énoncé, la loi défini sur $N' \times K'$ par transport de structure de celle de G via f est la loi $\star_{\alpha'}$.

DÉMONSTRATION — La formule donnée montre $\alpha_{k'} \in \mathrm{Aut}(N)$ (composé d'isomorphismes). On a bien $\alpha'_{k'k''} = \alpha'_{k'}\alpha'_{k''}$, donc α' est un morphisme de groupes. On conclut car pour, $n, n' \in N'$ et $k, k' \in K'$, et f comme ci-dessus, on a :

$$a(n')b(k')a(n'')b(k'') = a(n')\mathrm{int}_{b(k')}(a(n''))b(k'k'') = a(n'\alpha'_{k'}(n''))b(k'k'').$$

□

EXEMPLE 7.9. On a un isomorphisme $\mathrm{S}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathrm{S}_3$. En effet, on a $\mathrm{S}_4 = \mathrm{K}_4 \rtimes S$ (produit semi-direct interne) par l'Exemple 7.3 (iii) et la Proposition 7.7. On a $\mathrm{K}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et $S \simeq \mathrm{S}_3$. Il ne serait en fait pas très difficile de voir que pour tout isomorphisme $\alpha : \mathrm{S}_3 \xrightarrow{\sim} \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on a $\mathrm{S}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes_\alpha \mathrm{S}_3$.

Illustrons cette discussion par une application à la classification des groupes d'ordre $2p$ avec p premier impair.

PROPOSITION 7.10. *Un groupe d'ordre $2p$ avec p premier impair est soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$, soit isomorphe à D_{2p}.*

DÉMONSTRATION — Par Cauchy (Théorème 4.8 Chap. 2), il existe $c \in G$ d'ordre p et $\tau \in G$ d'ordre 2. Le sous-groupe $C = \langle c \rangle$ est d'indice 2 dans G. On a $\tau \notin C$ (car $p > 2$) et donc $G = C \coprod \tau C$, ce qui montre que $D = \langle \tau \rangle$ est un complément de C dans G. On est donc dans une situation de produit semi-direct interne $G = C \rtimes D$. On a des isomorphismes $a : \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} C, m \mapsto c^m$, et $b : \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} D, m \mapsto \tau^m$, de sorte que par suivi des isomorphismes on en déduit un isomorphisme

$$\mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z} \simeq G$$

pour un certain morphisme de groupes $\alpha : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$.

En fait, il n'existe que deux morphismes de groupes $\alpha : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$. En effet, on rappelle qu'on a un isomorphisme de groupes $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \operatorname{Aut}(\mathbb{Z}/p\mathbb{Z}), k \mapsto \varphi_k$, défini par $\varphi_k(x) = kx$ pour $x \in \mathbb{Z}/p\mathbb{Z}$ (Prop. 3.9 Chap. 2). Mais pour $k \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $k^2 = 1$ si, et seulement si, $(k-1)(k+1) = 0$ dans le corps $\mathbb{Z}/p\mathbb{Z}$, soit encore $k = \pm 1$. On en déduit que les deux seuls morphismes de groupes $\mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ sont le morphisme trivial, et le morphisme envoyant $\overline{1}$ sur φ_1. Ce dernier n'est autre que le morphisme de l'Exemple 7.6. Ainsi, on a montré que l'on a soit $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (produit direct), soit $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ (produit semi-direct de l'exemple ci-dessus), auquel cas on a déjà vu $G \simeq \mathrm{D}_{2p}$ (ce que l'on retrouve aussi en appliquant cette discussion à D_{2p} lui-même !). On conclut car $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est cyclique d'ordre $2p$ (par exemple, par l'isomorphisme chinois). □

⚠ Il faut être prudent avec l'écriture $N \rtimes K$ pour un produit semi-direct externe car il est très possible d'avoir $N \rtimes_{\alpha_1} K \not\simeq N \rtimes_{\alpha_2} K$ pour des choix différents de α_1 et α_2, même tous deux non triviaux, comme dans l'exemple ci-dessous.

Exemple 7.11. Soient p, q deux nombres premiers impairs distincts, et $n := pq$. Par l'isomorphisme chinois, il existe $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$ tels que $a \equiv 1 \bmod p$, $a \equiv -1 \bmod q$, $b \equiv -1 \bmod p$ et $b \equiv 1 \bmod q$. Il existe exactement 4 éléments $s \in (\mathbb{Z}/n\mathbb{Z})^\times$ tels que $s^2 = 1$, à savoir $1, a, b$ et $ab = -1$. Pour chaque tel s, il existe un unique morphisme $\alpha : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ envoyant $\overline{1}$ sur l'automorphisme $x \mapsto sx$ de $\mathbb{Z}/n\mathbb{Z}$ (de carré 1). Notons $G_s = \mathbb{Z}/n\mathbb{Z} \rtimes_\alpha \mathbb{Z}/2\mathbb{Z}$ le produit semi-direct défini par ce α (il dépend de s). On a par exemple $G_1 = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $G_{-1} \simeq \mathrm{D}_{2n}$. Il n'est pas difficile de vérifier que le centre de G_s est de cardinal $2n$, 2, $2p$, $2q$ quand s vaut respectivement $1, -1, a, b$. Ces 4 produits semi-directs sont donc non isomorphes.

Proposition 7.12. *À isomorphisme près, les groupes non abéliens d'ordre $\leqslant 8$ sont S_3, D_8 et H_8.*

Démonstration — Un groupe d'ordre premier est cyclique, donc abélien. Un groupe non abélien d'ordre 6 est isomorphe à $\mathrm{D}_6 = \mathrm{S}_3$ (Proposition 7.10). On peut donc supposer G non abélien d'ordre 8. Alors G n'a pas d'élément d'ordre 8 (sinon il serait cyclique), et tous ses éléments ne sont pas d'ordre 2 (Exercice 3.7 Chap. 3). Il existe donc $x \in G$ d'ordre 4. Le groupe $H = \langle x \rangle$ est distingué dans G, car d'indice 2. Choisissons $y \in G \smallsetminus H$ et posons $K = \langle y \rangle$. On a $G = \langle x, y \rangle$. Comme H est distingué dans G, int_y est un automorphisme de H, il envoie donc le générateur x de $H \simeq \mathbb{Z}/4\mathbb{Z}$ sur un autre générateur, *i.e.* sur x ou x^{-1}. Le premier cas est exclus car sinon $G = \langle x, y \rangle$ serait abélien. On a donc $yxy^{-1} = x^{-1}$. Si y est d'ordre 2, alors G est produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/4\mathbb{Z}$ pour l'inversion : on a $G \simeq \mathrm{D}_8$. Sinon y est d'ordre 4. Alors y^2 est d'ordre 2 et dans H, et donc $y^2 = x^2$. Ainsi, x^2 est dans le centre de $G = \langle x, y \rangle$, et on a $yx = x^{-1}y = (x^2)xy$. On constate qu'on a un isomorphisme $\mathrm{H}_8 \xrightarrow{\sim} G$ envoyant I sur x, J sur y et $x^2 = y^2$ sur -1. □