Feuille d'exercices : Produits semi-direct

Exercice 1. Soient N et H des groupes et soit $\phi\colon \mathrm{H} \to \mathrm{Aut(N)}$ un morphisme de groupes. Notons $\mathrm{N} \rtimes_\phi \mathrm{H}$ l'ensemble $\mathrm{N} \times \mathrm{H}$ muni de la loi de composition définie par

$$(n_1, h_1) \rtimes_\phi (n_2, h_2) = \big(n_1\phi(h_1)(n_2), h_1h_2\big).$$

(1) Montrer que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe appelé produit semi-direct de H par N relativement à ϕ.

(2) Montrer que $\mathrm{N} \times \{e_\mathrm{H}\} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$ et $\{e_\mathrm{N}\} \times \mathrm{H} \subset \mathrm{N} \rtimes_\phi \mathrm{H}$.

(3) Identifier le quotient de $\mathrm{N} \rtimes_\phi \mathrm{H}$ par $\mathrm{N} \times \{e_\mathrm{H}\}$.

Solution 1. (1) Montrons que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe.

- Commençons par montrer que la loi est associative.
  Soient n_1, n_2 et n_3 dans N. Soient h_1, h_2 et h_3 dans H. Par définition du produit nous avons
  $$\big((n_1, h_1) \rtimes_\phi (n_2, h_2)\big) \rtimes_\phi (n_3, h_3) = \big(n_1\phi(h_1)(n_2), h_1h_2\big) \rtimes_\phi (n_3, h_3) = \big(n_1\phi(h_1)(n_2)\phi(h_1h_2)(n_3), h_1h_2h_3\big).$$
  De même nous avons
  $$(n_1, h_1) \rtimes_\phi \big((n_2, h_2) \rtimes_\phi (n_3, h_3)\big) = (n_1, h_1) \rtimes_\phi \big(n_2\phi(h_2)(n_3), h_2h_3\big) = \big(n_1\phi(h_1)\big(n_2\phi(h_2)(n_3)\big)\big), h_1h_2h_3\big).$$
  Or $\phi(h_1)$ et ϕ sont des morphismes donc
  $$\phi(h_1)\big(n_2\phi(h_2)(n_3)\big) = \phi(h_1)(n_2)(\phi(h_1) \circ \phi(h_2))(n_3) = \phi(h_1)(n_2)(\phi(h_1h_2))(n_3)$$
  dont on déduit que
  $$\big((n_1, h_1) \rtimes_\phi (n_2, h_2)\big) \rtimes_\phi (n_3, h_3) = (n_1, h_1) \rtimes_\phi \big((n_2, h_2) \rtimes_\phi (n_3, h_3)\big).$$
  Par conséquent le produit $\rtimes_\phi$ est associatif.
- On voit tout de suite que l'élément $(e_\mathrm{N}, e_\mathrm{H})$ est neutre pour la loi $\rtimes_\phi$.
- Montrons que tout élément admet un inverse.
  Soient $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Pour tous $n' \in \mathrm{N}$ et $h' \in \mathrm{H}$ nous avons
  $$(n, h) \rtimes_\phi (n', h') = (e_\mathrm{N}, e_\mathrm{H})$$
  si et seulement si
  $$(n\phi(n')(h'), hh') = (e_\mathrm{N}, e_\mathrm{H})$$
  si et seulement si $h' = h^{-1}$ et $n' = \phi(h^{-1})(n^{-1})$. Le calcul de $(n', h') \rtimes_\phi (n, h)$ est similaire ce qui assure que (n, h) est inversible et que son inverse est $(n, h)^{-1} = (\phi(h^{-1})(n^{-1}), h^{-1})$.

  Ainsi $\mathrm{N} \rtimes_\phi \mathrm{H}$ est bien un groupe.

(2) Montrons que $\mathrm{N} \times \{e_\mathrm{H}\} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$ et $\{e_\mathrm{N}\} \times \mathrm{H} \subset \mathrm{N} \rtimes_\phi \mathrm{H}$.

Les formules définissant le produit assurent que $\mathrm{N} \times \{e_\mathrm{H}\}$ et $\{e_\mathrm{N}\} \times \mathrm{H}$ sont bien des sous-groupes de $\mathrm{N} \rtimes_\phi \mathrm{H}$ car $\phi(h)(e_\mathrm{N}) = e_\mathrm{N}$ pour tout $h \in \mathrm{H}$.

Montrons que $\mathrm{N} \times \{e_\mathrm{H}\}$ est distingué dans $\mathrm{N} \rtimes_\phi \mathrm{H}$. Soient n, n' dans N et h' dans H. Alors

$$\begin{aligned}(n, h) \rtimes_\phi (n', e_\mathrm{H}) \rtimes_\phi (n, h)^{-1} &= (n, h) \rtimes_\phi (n', e_\mathrm{H}) \rtimes_\phi (\phi(h^{-1})(n^{-1}), h^{-1}) \\ &= n\phi(h)(n'), h() \rtimes_\phi (\phi(h^{-1})(n^{-1}), h^{-1}) \\ &= (n\phi(h)(n')\phi(h)\big(\phi(h^{-1})(n^{-1})\big), e_\mathrm{H}) \\ &= (n\phi(h)(n')n^{-1}, e_\mathrm{H}) \in \mathrm{N} \times \{e_\mathrm{H}\}\end{aligned}$$

Ainsi $\mathrm{N} \times \{e_\mathrm{H}\}$ est distingué dans $\mathrm{N} \rtimes_\phi \mathrm{H}$.

Un calcul analogue montre que $\{e_\mathrm{N}\} \times \mathrm{H}$ n'est pas distingué en général.

(3) Identifions le quotient de $\mathrm{N} \rtimes_\phi \mathrm{H}$ par $\mathrm{N} \times \{e_\mathrm{H}\}$.

Considérons l'application naturelle $\pi\colon \mathrm{N} \rtimes_\phi \mathrm{H} \to \mathrm{H}$ donnée par la seconde projection, *i.e.* $\pi(n,h) = h$.

Il est clair que π est surjective.

La définition de la loi de groupes assure que π est un morphisme de groupes.

Déterminons son noyau. Soient $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Nous avons $\pi(n,h) = e_\mathrm{H}$ si et seulement si $h = e_\mathrm{H}$; ainsi $\ker \pi = \mathrm{N} \times \{e_\mathrm{H}\}$.

Finalement l'application π passe au quotient par son noyau et induit un isomorphisme de groupes :

$$\overline{\pi}\colon {}^{\mathrm{N} \rtimes_\phi \mathrm{H}}\!\!\diagup_{\mathrm{N} \times \{e_\mathrm{H}\}} \xrightarrow{\sim} \mathrm{H}$$

Exercice 2. Soit G un groupe. Soient N et H deux sous-groupes de G tels que $\mathrm{N} \cap \mathrm{H} = \{e\}$, $\mathrm{G} = \mathrm{NH}$ et $\mathrm{N} \triangleleft \mathrm{G}$.

(1) Montrer que l'application

$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$

est un morphisme de groupes.

(2) Montrer que

$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$

est un isomorphisme de groupes.

On dit alors que G est le produit semi-direct de H par N.

Solution 2. (1) Montrons que l'application

$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$

est un morphisme de groupes.

L'application i est bien définie car $\mathrm{N} \triangleleft \mathrm{G}$. On vérifie directement que c'est un morphisme de groupes.

(2) Montrons que

$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$

est un morphisme de groupes. Soient n, n' dans N et h, h' dans H. On a

$$f(n,h)f(n',h') = nhn'h'$$

et

$$f\big((n,h) \rtimes_i (n',h')\big) = f\big(ni(h)(n'), hh'\big) = f(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h'$$

ce qui assure que $f\big((n,h) \rtimes_i (n',h')\big) = f(n,h)f(n',h')$. Ainsi f est bien un morphisme de groupes.

Montrons maintenant que f est un isomorphisme de groupes. L'hypothèse $\mathrm{NH} = \mathrm{G}$ assure que f est surjectif et l'hypothèse $\mathrm{N} \cap \mathrm{H} = \{e\}$ assure que le noyau de f est trivial. Par suite f est un isomorphisme.

Exercice 3. Montrer que le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si ϕ est le morphisme trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \triangleleft \mathrm{N} \rtimes_\phi \mathrm{H}$.

Solution 3. Le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si pour tous n, $n' \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a

$$(n,h) \rtimes_\phi (n',h') = (n', hh')$$

si et seulement si pour tous n, $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $n\phi(h)(n') = nn'$ si et seulement si pour tous $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $\phi(h)(n') = nn'$ si et seulement si ϕ est le morphisme trivial.

Pour tous $n \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a

$$(n,h) \rtimes_\phi (e_\mathrm{N}, h') \rtimes_\phi (n,h)^{-1} = \big(n\phi(hh'h^{-1})(n^{-1}), hh'h^{-1}\big).$$

Ainsi le morphisme ϕ est trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \triangleleft \mathrm{N} \rtimes_\phi \mathrm{H}$.

Exercice 4. Soit

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

une suite exacte (courte).

(1) Montrer que si G est le produit direct de H et N ou bien un produit semi-direct de H par N, alors on a une telle suite exacte.

(2) Réciproquement soit une telle suite exacte. Si p possède une section, c'est-à-dire s'il existe un morphisme de groupes $s\colon \mathrm{H} \to \mathrm{G}$ tel que $p \circ s = \mathrm{id}_{\mathrm{H}}$, montrer que G est le produit semi-direct de H par N pour l'opération $h \cdot n = s(h)ns(h)^{-1}$.

(3) Donner un exemple de suite exacte courte qui n'est pas un produit semi-direct.

Solution 4. (1) Supposons que $\mathrm{G} = \mathrm{N} \rtimes_\phi \mathrm{H}$. D'après l'Exercice 1 3. on dispose d'un morphisme surjectif $\pi\colon \mathrm{G} \to \mathrm{H}$ dont le noyau est le sous-groupe $\mathrm{N} \rtimes_\phi \{e_{\mathrm{H}}\}$ qui est isomorphe à N. Par suite on a bien une suite exacte

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

où $i\colon \mathrm{N} \to \mathrm{G}$ est défini par $i(n) = (n, e_{\mathrm{H}})$. De plus on peut vérifier que l'application

$$\mathrm{H} \to \mathrm{G} \qquad\qquad h \mapsto (e_{\mathrm{N}}, h)$$

est une section de π.

(2) C'est une conséquence de l'Exercice 2 appliqué aux sous-groupes $\mathrm{N}' = i(\mathrm{N})$ et $\mathrm{H}' = s(\mathrm{H})$ de G. Il suffit donc de vérifier que N′ et G′ satisfont les hypothèses de l'Exercice 2. Le groupe N′ est distingué dans G car $\mathrm{N}' = \ker p$. Soit $g \in \mathrm{G}$. Posons $h = s(\pi(g)) \in \mathrm{H}'$. Alors

$$\pi(h) = \pi(s(\pi(g))) = \pi(g)$$

donc $n = gh^{-1}$ appartient à $\ker \pi = \mathrm{N}'$. Finalement nous avons bien $\underbrace{g}_{\in \mathrm{G}} = \underbrace{n}_{\in \mathrm{N}'}\underbrace{h}_{\in \mathrm{H}'}$ ce qui assure que $\mathrm{G} = \mathrm{N}'\mathrm{H}'$. Soit $g \in \mathrm{N}' \cap \mathrm{H}'$. Puisque $g \in \mathrm{H}'$ il existe $h \in \mathrm{H}$ tel que $g = s(h)$. Comme $g \in \mathrm{N}'$ nous avons $\pi(g) = e_{\mathrm{H}}$. Par suite $\pi(s(h)) = e_{\mathrm{H}}$, *i.e.* $h = e_{\mathrm{H}}$, donc $g = s(e_{\mathrm{H}}) = e_{\mathrm{G}}$. Il s'en suit que $\mathrm{N}' \cap \mathrm{H}' = \{e_{\mathrm{G}}\}$. Nous pouvons donc bien appliquer l'Exercice 2 pour conclure.

(3) Considérons la suite exacte courte

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

où p est la réduction modulo 2. C'est bien une suite exacte courte, en revanche p n'admet pas de section puisque l'élément non trivial du quotient $\mathbb{Z}/2\mathbb{Z}$ est d'ordre 2 alors que tous ses antécédents par p sont d'ordre 4. Il s'en suit que $\mathbb{Z}/4\mathbb{Z}$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Un autre exemple est donné par le groupe des quaternions $\mathbb{H}_8$ dont le centre $Z(\mathbb{H}_8)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le quotient correspondant est $\mathbb{H}_8/Z(\mathbb{H}_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ce qui fournit une suite exacte

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{H}_8 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

telle que p n'admet pas de section (on peut par exemple le voir en listant les éléments d'ordre 2 dans $\mathbb{H}_8$). Il en résulte que $\mathbb{H}_8$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 5. Nous avons vu en cours que

$$\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{GL}(n, \Bbbk) \simeq \mathrm{SL}(n, \Bbbk) \rtimes \Bbbk^*.$$

Ces produits semi-directs sont-ils directs ?

Solution 5. On peut vérifier que les produits

$$\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad\qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

ne sont pas directs (sauf pour $n = 2$) quelle que soit la section choisie. On peut en fait vérifier qu'il n'existe pas d'isomorphisme (quelconque) entre ces groupes et les produits directs correspondants.

Le cas $\mathrm{GL}(n, \Bbbk) \simeq \mathrm{SL}(n, \Bbbk) \rtimes \Bbbk^*$ est moins évident pour $n \geqslant 2$. Si $x \mapsto x^n$ est un automorphisme de $\Bbbk^*$, on note $a\colon \Bbbk^\times \to \Bbbk^\times$ son inverse. L'application

$$\alpha\colon \mathrm{SL}(n, \Bbbk) \times \Bbbk^* \to \mathrm{GL}(n, \Bbbk) \qquad\qquad (A, t) \mapsto A\mathrm{diag}(a(t), a(t), \ldots, a(t))$$

est un isomorphisme.

Réciproquement supposons qu'il existe un isomorphisme de groupes

$$\alpha\colon \mathrm{SL}(n,\Bbbk)\times\Bbbk^*\to\mathrm{GL}(n,\Bbbk)\qquad\qquad (A,t)\mapsto\phi(A)s(t).$$

Le sous-groupe dérivé de $\mathrm{SL}(n,\Bbbk)\times\Bbbk^*$ est $\mathrm{SL}(n,\Bbbk)\times\{1\}$ et celui de $\mathrm{GL}(n,\Bbbk)$ est $\mathrm{SL}(n,\Bbbk)$. Par conséquent ϕ est un automorphisme de $\mathrm{SL}(n,\Bbbk)$. De plus $\alpha(\Bbbk^*)=s(\Bbbk^*)$ commute avec tout élément de $\mathrm{GL}(n,\Bbbk)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}(n,\Bbbk)$ est formé des homothéties). Ainsi l'application $t\mapsto s(t)$ est un morphisme injectif de $\Bbbk^*$ vers $\mathrm{GL}(n,\Bbbk)$ de la forme $t\mapsto\mathrm{diag}(a(t),a(t),\dots,a(t))$.

Le noyau de det étant $\mathrm{SL}(n,\Bbbk)$ on a $a(t)^n=1$ si et seulement si $a(t)=1$. Puisque $t\mapsto a(t)$ est injectif, $t\mapsto a(t)^n$ l'est aussi. Or det est surjectif sur $\Bbbk^*$ donc $t\mapsto a(t)^n=a(t^n)$ est bijectif. Il en résulte que $x\mapsto x^n$ est bijectif et donc un automorphisme de $\Bbbk^*$.

Ainsi $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$ si et seulement si le morphisme $(\cdot)^n\colon\Bbbk^*\to\Bbbk^*$ est un automorphisme. En particulier

- si $\Bbbk=\mathbb{R}$ et n est impair, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$;
- si $\Bbbk$ est un corps fini de caractéristique p et si n est égal à une puissance de p, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$.

Exercice 6. Soit $\mathrm{G}=\mathrm{N}\rtimes\mathrm{H}$. Soit K un sous-groupe de G contenant N. Montrer que $\mathrm{K}=\mathrm{N}\rtimes(\mathrm{K}\cap\mathrm{H})$.

Solution 6. On va appliquer ce qu'on a vu dans l'Exercice 2 :

— $\mathrm{N}\triangleleft\mathrm{G}$ et $\mathrm{N}\subset\mathrm{K}$ donc $\mathrm{N}\triangleleft\mathrm{K}$;
— $\mathrm{H}\subset\mathrm{G}$ et $\mathrm{K}\subset\mathrm{G}$ donc $\mathrm{H}\cap\mathrm{K}\subset\mathrm{K}$;
— $\mathrm{N}\cap\mathrm{H}=\{e\}$ donc $\mathrm{N}\cap(\mathrm{K}\cap\mathrm{N})=\{e\}$;
— $\mathrm{NH}=\mathrm{G}$ donc si $k\in\mathrm{K}$, alors $k=nh$ avec $n\in\mathrm{N}$ et $h\in\mathrm{H}$. Puisque $\mathrm{N}\subset\mathrm{K}$ nous en déduisons que $h\in\mathrm{H}\cap\mathrm{K}$. D'où $\mathrm{N}(\mathrm{H}\cap\mathrm{K})=\mathrm{K}$.

Exercice 7. Soient H et N des groupes. Soient φ, $\psi\colon\mathrm{H}\to\mathrm{Aut}(\mathrm{N})$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $\mathrm{N}\rtimes_\varphi\mathrm{H}$ et $\mathrm{N}\rtimes_\psi\mathrm{H}$ soient isomorphes.

(1) S'il existe un automorphisme α de H tel que $\psi=\varphi\circ\alpha$ montrer que $\mathrm{N}\rtimes_\varphi\mathrm{H}$ et $\mathrm{N}\rtimes_\psi\mathrm{H}$ sont isomorphes.
(2) S'il existe un automorphisme u de N tel que
$$\forall\, h\in\mathrm{H}\qquad\phi(h)=u\psi(h)u^{-1}$$
montrer que $\mathrm{N}\rtimes_\varphi\mathrm{H}$ et $\mathrm{N}\rtimes_\psi\mathrm{H}$ sont isomorphes.
(3) Si H est cyclique et si $\varphi(\mathrm{H})=\psi(\mathrm{H})$ montrer que $\mathrm{N}\rtimes_\varphi\mathrm{H}$ et $\mathrm{N}\rtimes_\psi\mathrm{H}$ sont isomorphes.

Solution 7.

(1) Le morphisme
$$\mathrm{N}\rtimes_\varphi\mathrm{H}\to\mathrm{N}\rtimes_\psi\mathrm{H}\qquad\qquad(n,h)\mapsto(n,\alpha(h))$$
est un isomorphisme.
(2) Le morphisme
$$\mathrm{N}\rtimes_\varphi\mathrm{H}\to\mathrm{N}\rtimes_\psi\mathrm{H}\qquad\qquad(n,h)\mapsto(u(n),h)$$
est l'isomorphisme.
(3) Le groupe H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\operatorname{im}\varphi=\operatorname{im}\psi$ est isomorphe à $\mathbb{Z}/m\mathrm{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1)=d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application
$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\to\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$
est surjective, il existe $d'\in\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ qui s'envoie sur d.

La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait les conditions de 1. d'où le résultat.

Exercice 8. Montrer que tout groupe d'ordre 255 est cyclique.

Solution 8. Soit G un groupe d'ordre $255 = 3 \times 5 \times 17$. Soit n_3 (resp. n_5, resp. n_{17}) le nombre de 3-Sylow (resp. 5-Sylow, resp. 17-Sylow) de G. Les théorèmes de Sylow assurent que

$$n_3 \in \{1, 85\}, \qquad n_5 \in \{1, 51\} \qquad n_{17} = 1.$$

On ne peut pas avoir $(n_3, n_5) = (85, 51)$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$.

Supposons que $n_3 = 1$ (le cas $n_5 = 1$ se résoud de manière analogue). Notons S_3 le seul 3-Sylow de G, S_{17} le seul 17-Sylow de G et S_5 un 5-Sylow quelconque. Nous avons

— $S_3S_{17} \simeq S_3 \times S_{17} \lhd \mathrm{G}$;
— $S_3S_{17} \cap S_5 = \{e\}$;
— $S_3S_{17}S_5 = \mathrm{G}$.

L'exercice 2 assure que $\mathrm{G} \simeq S_3S_{17} \rtimes S_5$. Soit $\phi\colon S_5 \to \mathrm{Aut}(S_3S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3S_{17}) \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{16\mathbb{Z}}$ donc ϕ est trivial et le produit semi-direct. On conclut par le lemme chinois.

Exercice 9. Soit p un nombre premier impair.

(1) Déterminer les p-Sylow de $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$.

(2) Soient ϕ et ψ des morphismes non triviaux de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ dans $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$. Pour tout entier k notons ϕ_k le morphisme ϕ_k défini par $\phi_k(x) = \phi(kx)$. Montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$ tels que $\psi = P\phi_k P^{-1}$.

(3) Montrer qu'il existe un produit semi-direct non trivial $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^2 \rtimes {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.

(4) Montrer que le centre de ce dernier groupe est isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. (On rappelle que si G est un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène, alors G est abélien.)

(5) Supposons que G est un groupe fini. Notons p le plus petit nombre premier divisant le cardinal de G.

Montrer que tout sous-groupe de G d'indice p est distingué (indication : commencer par montrer que tout sous-groupe H de G d'indice p agit trivialement sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$, en déduire que H est distingué dans G).

(6) Soit G un groupe d'ordre p^3 non cyclique contenant un élément g d'ordre p^2. Montrer que $\langle g \rangle$ est distingué dans G et que G est un produit semi-direct de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ par $\langle g \rangle \simeq {}^{\mathbb{Z}}\!/_{p^2\mathbb{Z}}$.

Solution 9. (1) Les p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe

$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p \right\}$$

des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ et que tous sont conjugués, une matrice de $\mathrm{GL}(2, \mathbb{F}_p)$ est dans un p-Sylow si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre p^2 telles matrices (à la main...) et donc $(p+1)$ p-Sylow distincts (car deux p-Sylow distincts ne s'intersectent qu'en l'élément neutre). Remarquons que ce sont les conjugués de U par les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(2) Puisque les images de ψ et φ sont des p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ elles sont conjuguées par une matrice $P \in \mathrm{GL}(2, \mathbb{F}_p)$. Notons

$$\varphi_{(P)}\colon {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \to \psi\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right) \qquad x \mapsto P\varphi(x)P^{-1}$$

c'est un isomorphisme. Dès lors $(\varphi_{(P)})^{-1} \circ \psi$ est un automorphisme de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, *i.e.* de la forme $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.

(3) Puisque $\mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right) \simeq \mathrm{GL}(2, \mathbb{F}_p)$ le 1. assure l'existence d'un produit semi-direct non trivial $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^2 \rtimes {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.

(4) Comme le centre d'un p-groupe est non trivial, le centre de $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ est d'ordre p, p^2 ou p^3. Si $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ était d'ordre p^2 ou p^3, alors $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ serait abélien (en effet si G est un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est monogène, alors G est abélien) : contradiction avec le fait que le produit semi-direct n'est pas trivial. Il s'en suit que $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(5) Notons p le plus petit nombre premier divisant le cardinal de G. Soit H un sous-groupe de G d'indice p. Posons $X = \mathrm{G}/\mathrm{H}$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi\colon \mathrm{G} \to \mathcal{S}_X$. Intéressons-nous à la restriction de cette action au sous-groupe H, autrement dit au morphisme $\varphi\colon \mathrm{H} \to \mathcal{S}_X$. Puisque H agit trivialement sur la classe x_0 de H dans $X = \mathrm{G}/\mathrm{H}$ l'action de H sur X induit une action de H sur $X' = X \setminus \{x_0\}$ c'est-à-dire un morphisme de groupes $\psi\colon \mathrm{H} \to \mathcal{S}_{X'}$. Or $|X'| = p-1$ donc tous les facteurs premiers de $|\mathcal{S}_{X'}|$ sont strictement inférieurs à p. Or les facteurs premiers de $|\mathrm{H}|$ sont par hypothèse tous supérieurs ou égaux à p. Par suite $|\mathrm{H}|$ et $|\mathcal{S}_{X'}|$ sont premiers entre eux. Le morphisme ψ est donc trivial. Il en résulte que H agit trivialement sur X' et donc aussi sur X.

Montrons que cela implique que G est distingué dans G. Soit $h \in \mathrm{H}$ et soit $g \in \mathrm{G}$. Puisque H agit trivialement sur X on a $h \cdot (g\mathrm{H}) = g\mathrm{H}$ donc $(g^{-1}hg)\mathrm{H} = \mathrm{H}$, par suite $g^{-1}hg$ appartient à H, *i.e.* H est distingué dans G.

(6) Le sous-groupe $\langle g\rangle$ est d'indice p dans un groupe d'ordre p^3. D'après 5. le groupe $\langle g\rangle$ est donc distingué dans G.

De plus le quotient $\mathrm{G}/\langle g\rangle$ est d'ordre p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Soit $y \in \mathrm{G} \setminus \langle g\rangle$. Alors y^p appartient à $\langle g\rangle$ et $y^{p^2} = e$. Il existe donc $k \in \mathbb{Z}$ tel que $y^p = g^{pk}$. Comme $\langle g\rangle$ est distingué dans G il existe un entier $r \geqslant 0$ tel que $y^{-1}gy = g^r$. Alors pour tout $\ell \in \mathbb{N}$ nous avons $g^\ell y = yg^{\ell r}$. On cherche $z \in \mathrm{G} \setminus \langle g\rangle$ d'ordre p ; plus précisément on cherche $z \in \mathrm{G} \setminus \langle g\rangle$ d'ordre p sous la forme $z = yg^n$. Alors

$$z^p = (yg^n)^p = yg^nyg^n \dots yg^n;$$

une simple récurrence assure que

$$z^p = y^p g^{n(r^{p-1}+r^{p-2}+\dots+r+1)} = g^{pk+n(r^{p-1}+r^{p-2}+\dots+r+1)}.$$

Par suite z est d'ordre p si et seulement si

$$pk + n(r^{p-1} + r^{p-2} + \dots + r + 1) \equiv 0 \mod p^2. \tag{1}$$

On cherche donc à résoudre (1) dont l'inconnue est $n \in \mathbb{Z}$. Posons $S := r^{p-1} + r^{p-2} + \dots + r + 1$. Alors $(r-1)S \equiv r - 1 \bmod p$ donc
— soit $r \not\equiv 1 \bmod p$ et $S \equiv 1 \bmod p$;
— soit $r \equiv 1 \bmod p$ et on vérifie que dans ce cas $S \equiv p \bmod p^2$ (utiliser que p est impair).
Dans les deux cas l'équation (1) admet une solution $n_0 \in \mathbb{Z}$. Ainsi $z_0 = yg^{n_0} \in \mathrm{G} \setminus \langle g\rangle$ est d'ordre p. Les deux sous-groupes $\mathrm{N} = \langle g\rangle$ et $\mathrm{H} = \langle z\rangle$ satisfont les hypothèses de l'Exercice 2 ce qui assure que G est produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p^2\mathbb{Z}$.