DM 17 : un corrigé

Partie I : Automorphismes de groupes

1°) Notons $S(H)$ l'ensemble des bijections de H dans H. Muni de la loi de composition, $S(H)$ est un groupe d'après le cours (en effet, la loi est bien interne, associative, Id_H est l'élément neutre et le symétrique de tout $f \in S(H)$ est sa bijection réciproque). Il suffit donc de montrer que $\mathrm{Aut}(H)$ est un sous-groupe de $S(H)$.
Or Id_H est un automorphisme du groupe H, donc $\mathrm{Aut}(H)$ est non vide et, pour tout $f, g \in \mathrm{Aut}(H)$, fg^{-1} est encore un automorphisme d'après le cours. Ainsi $\mathrm{Aut}(H)$ est bien un groupe pour la loi de composition.

2°) Notons f_x l'application de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même définie par $f_x(y) = xy$.
Pour tout $y, z \in \mathbb{Z}/n\mathbb{Z}$, $f_x(y+z) = xy + xz$ d'après la distributivité dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, donc $f_x(y+z) = f_x(y) + f_x(z)$, ce qui prouve que f_x est un endomorphisme de groupe.
Supposons que f_x est bijectif. Alors $\overline{1}$ possède un antécédent : il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy = \overline{1}$, donc x est inversible. Réciproquement, si x est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, alors on peut considérer l'application $f_{x^{-1}}$ et il est clair que $f_x \circ f_{x^{-1}} = f_{x^{-1}} \circ f_x = Id_{\mathbb{Z}/n\mathbb{Z}}$, donc f_x est un automorphisme.
Ainsi $f_x \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ si et seulement si x est inversible, c'est-à-dire en notant $x = \overline{h}$ avec $h \in \mathbb{Z}$, si et seulement si $h \wedge n = 1$.

3°) Notons U le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et
notons $\begin{array}{rccc} \varphi : & U & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ & x & \longmapsto & f_x \end{array}$. Montrons que φ est un isomorphisme de groupes.
Pour tout $x, y \in U$, pour tout $z \in \mathbb{Z}/n\mathbb{Z}$,
$\varphi(xy)(z) = f_{xy}(z) = xyz$ et $\varphi(x) \circ \varphi(y)(z) = f_x(yz) = xyz$, donc $\varphi(xy) = \varphi(x)\varphi(y)$.
Ainsi, φ est un morphisme de groupes.
Soit $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Posons $x = f(\overline{1})$. Alors, pour tout $y = \overline{h} \in \mathbb{Z}/n\mathbb{Z}$, avec $h \in \mathbb{Z}$, $f(y) = f(\overline{h}) = f(h\overline{1}) = hf(\overline{1})$, par propriété du morphisme de groupe f,
donc $f(y) = \overline{h}f(\overline{1}) = yf(\overline{1}) = xy = f_x(y)$. Ainsi, $f = f_x$. De plus, $f = f_x$ est un automorphisme, donc d'après la question 2, $x \in U$. Ainsi, on peut écrire que $f = \varphi(x)$: φ est surjective.
Soit $x \in \mathrm{Ker}(\varphi)$: $\varphi(x) = Id_{\mathbb{Z}/n\mathbb{Z}}$, donc pour tout $y \in \mathbb{Z}/n\mathbb{Z}$, $xy = f_x(y) = y$. En particulier avec $y = \overline{1}$, on obtient $x = \overline{1}$, donc $\mathrm{Ker}(\varphi) = \{\overline{1}\}$ ce qui prouve l'injectivité de φ.
En conclusion, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe au groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Partie II

4°) Soit $(h,k),(h',k'),(h'',k'') \in H \times K$.
$\diamond$ Loi interne : $\varphi(k) \in \mathrm{Aut}(H)$, donc $\varphi(k)(h') \in H$. Ainsi, $(h,k).(h',k')$ est bien défini et c'est un élément de $H \times K$. La loi "." définie par l'énoncé est donc une loi interne sur $H \times K$.
$\diamond$ Associativité :

$$\begin{aligned}(h,k).((h',k').(h'',k'')) &= (h,k).(h'\varphi(k')(h''),k'k'')\\ &= (h\varphi(k)(h'\varphi(k')(h'')),kk'k'')\\ &= (h\varphi(k)(h')\varphi(kk')(h''),kk'k''),\ \text{car } \varphi \text{ est un morphisme.}\end{aligned}$$

D'autre part,
$((h,k).(h',k')).(h'',k'') = (h\varphi(k)(h'),kk').(h'',k'') = (h\varphi(k)(h')\varphi(kk')(h''),kk'k'')$, ce qui prouve l'associativité.
$\diamond$ Élément neutre : $(1,1).(h,k) = (1\ \varphi(1)(h),1\ k) = (h,k)$, car $\varphi(1) = 1_{\mathrm{Aut}(H)} = Id_H$ et $(h,k).(1,1) = (h\varphi(k)(1),1\ 1) = (h,1)$, car $\varphi(k)$ est un morphisme.
Ainsi, $(1,1)$ est l'élément neutre de $H \rtimes_\varphi K$.
$\diamond$ Symétrique : $(h,k).(\varphi(k^{-1})(h^{-1}),k^{-1}) = (h\ \varphi(k)(\varphi(k^{-1})(h^{-1})),kk^{-1}) = (h\ h^{-1},1)$, car $\varphi(k)\varphi(k^{-1}) = \varphi(1) = Id_H$, donc $(h,k).(\varphi(k^{-1})(h^{-1}),k^{-1}) = (1,1)$. De plus, $(\varphi(k^{-1})(h^{-1}),k^{-1}).(h,k) = (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h),k^{-1}k) = (\varphi(k^{-1})(1),1) = (1,1)$, donc le symétrique de (h,k) est égal à $(\varphi(k^{-1})(h^{-1}),k^{-1})$.
En conclusion, $H \rtimes_\varphi K$ est bien un groupe.

5°) $\diamond$ Supposons que, H et K sont abéliens et que, pour tout $k \in K$,
$\varphi(k) = Id_H = 1_{\mathrm{Aut}(H)}$: φ est bien un morphisme.
Alors, pour tout $(h,k),(h',k') \in H \times K$, $(h,k).(h',k') = (hh',kk')$, donc $H \rtimes_\varphi K$ est le produit usuel des deux groupes H et K. Il est bien commutatif.
$\diamond$ Supposons que $H \rtimes_\varphi K$ est commutatif.
Alors, pour tout $(h,k),(h',k') \in H \times K$, $(h,k).(h',k') = (h',k').(h,k)$, c'est-à-dire $(h\varphi(k)(h'),kk') = (h'\varphi(k')(h),k'k)$, donc $kk' = k'k$, ce qui prouve que K est abélien, et (1) : $h\varphi(k)(h') = h'\varphi(k')(h)$.
En particulier, avec $k = k' = 1_K$, $hh' = h'h$, donc H est aussi abélien.
Alors, l'égalité (1) avec $h' = 1$ et $k = k'$ donne : $h\varphi(k)(1) = \varphi(k)(h)$, c'est-à-dire $\varphi(k)(h) = h$, donc $\varphi(k) = Id_H$, pour tout $k \in K$, ce qu'il fallait démontrer.

6°) Si φ est un morphisme du groupe $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ différent de $x \longmapsto Id_{\mathbb{Z}/7\mathbb{Z}}$, alors d'après la question précédente, $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ est un groupe non commutatif dont l'ordre est égal au cardinal de $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, c'est-à-dire à 21. Il suffit donc de construire un tel morphisme [1].
D'après la question 3, l'application $x \longmapsto f_x$ est un automorphisme de $U(\mathbb{Z}/7\mathbb{Z}) = \mathbb{Z}/7\mathbb{Z} \setminus \{0\}$ dans $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$.

1. On peut montrer que le seul morphisme de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ (qui est de cardinal 2 d'après la question 3) est $x \longmapsto Id_{\mathbb{Z}/3\mathbb{Z}}$, donc on ne peut pas permuter les rôles joués par $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.

Dans $\mathbb{Z}/7\mathbb{Z}$, on a $\overline{3}^2 = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{18} = \overline{4}$, $\overline{3}^5 = \overline{12} = \overline{5}$ et $\overline{3}^6 = \overline{15} = \overline{1}$, donc $U(\mathbb{Z}/7\mathbb{Z}) = \{\overline{3}^i \ / \ i \in \mathbb{Z}\}$: il est cyclique d'ordre 6.
On en déduit que $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) = \{y \longmapsto \overline{3}^i y \ / \ i \in \mathbb{Z}\}$.
Notons $\begin{array}{rccc} \varphi : & \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \\ & \overline{k} & \longmapsto & (y \longmapsto \overline{3}^{2k} y) \end{array}$. φ est correctement définie car, si $k, k' \in \mathbb{Z}$ avec $\overline{k} = \overline{k'}$ dans $\mathbb{Z}/3\mathbb{Z}$, alors il existe $\alpha \in \mathbb{Z}$ tel que $k' = k + 3\alpha$, donc pour tout $y \in \mathbb{Z}/7\mathbb{Z}$, $\overline{3}^{2k'} y = \overline{3}^{2k} y \overline{3}^{6\alpha} = \overline{3}^{2k} y$, car on a vu que dans $\mathbb{Z}/7\mathbb{Z}$, $\overline{3}^6 = \overline{1}$.
De plus, on vérifie que $\varphi(\overline{kk'}) = \varphi(\overline{k}) \circ \varphi(\overline{k'})$, donc φ est un morphisme du groupe $\mathbb{Z}/3\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$. Il est différent de $x \longmapsto Id_{\mathbb{Z}/7\mathbb{Z}}$ car $\varphi({}^3\overline{1})({}^7\overline{1}) = {}^7\overline{3}^2 = {}^7\overline{2}$, donc $\varphi(\overline{1}) \neq Id_{\mathbb{Z}/7\mathbb{Z}}$.
Ainsi, $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ est un groupe non commutatif d'ordre 21, dont la loi est définie par : pour tout $h, k, h', k' \in \mathbb{Z}$, $({}^7\overline{h}, {}^3\overline{k}).({}^7\overline{h'}, {}^3\overline{k'}) = (\overline{h}\varphi(\overline{k})(\overline{h'}), \overline{kk'}) = (\overline{h}\overline{3}^{2k}\overline{h'}, \overline{kk'})$, soit $({}^7\overline{h}, {}^3\overline{k}).({}^7\overline{h'}, {}^3\overline{k'}) = ({}^7\overline{hh'}\ \overline{3}^{2k}, {}^3\overline{kk'})$.

7°)

- Soit $(h, k) \in E \cap F$. $(h, k) \in E$, donc $k = 1$. $(h, k) \in F$, donc $h = 1$. Ainsi, $(h, k) = (1, 1)$. Réciproquement $(1, 1) \in E \cap F$, donc $E \cap F = \{1_{H \rtimes_\varphi F}\}$.
- Soit $(h, k) \in H \times K$. $(h, 1).(1, k) = (h\varphi(1)(1), 1\ k) = (h, k)$ donc $(h, k) \in E.F$. Ainsi, $E.F = H \rtimes_\varphi K$ (en effet, l'ensemble sous-jacent du groupe $H \rtimes_\varphi K$ est $H \times K$).
- $(1, 1) \in F$, donc $F \neq \emptyset$. Soit $(1, k)$ et $(1, k')$ deux éléments de F.
  $(1, k).(1, k') = (1\ \varphi(k)(1), kk') = (1, kk') \in F$ et
  $(1, k)^{-1} = (\varphi(k^{-1})(1^{-1}), k^{-1}) = (1, k^{-1}) \in F$,
  donc F est un sous-groupe de $H \rtimes_\varphi K$ et l'application $k \longmapsto (1, k)$ est un isomorphisme de K dans F.
- $(1, 1) \in E$, donc $E \neq \emptyset$. Soit $(h, 1)$ et $(h', 1)$ deux éléments de E.
  $(h, 1).(h', 1) = (h\varphi(1)(h'), 1\ 1) = (hh', 1) \in E$
  et $(h, 1)^{-1} = (\varphi(1^{-1})(h^{-1}), 1^{-1}) = (h^{-1}, 1) \in E$,
  donc E est un sous-groupe de $H \rtimes_\varphi K$ et l'application $h \longmapsto (h, 1)$ est un isomorphisme de H dans E. .
  De plus, si $(h, k) \in H \rtimes_\varphi K$ et $(h', 1) \in E$, alors
  $$\begin{aligned} (h, k).(h', 1).(h, k)^{-1} &= (h\varphi(k)(h'), k).(\varphi(k^{-1})(h^{-1}), k^{-1}) \\ &= (h\varphi(k)(h')\varphi(k)(\varphi(k^{-1})(h^{-1})), 1) \\ &= (h\ \varphi(k)(h')\ h^{-1}, 1) \in E, \end{aligned}$$
  donc E est bien un sous-groupe distingué de $H \rtimes_\varphi K$.

Partie III : construction réciproque

8°) $\diamond$ $E.F = G$, donc p est surjective. Montrons qu'elle est également injective :
soit $(e, f), (e', f') \in E \times F$ tels que $ef = e'f'$. Alors $e'^{-1}e = f'f^{-1} \in E \cap F = \{1\}$, donc $e'^{-1}e = f'f^{-1} = 1$, donc $(e, f) = (e', f')$.
Ainsi, p est une bijection.

$\diamond$ Cherchons φ tel que p soit un isomorphisme de $E \rtimes_\varphi F$ dans G, par analyse-synthèse.
Si φ est solution, pour tout $(e,f),(e',f') \in E \times F$,
$efe'f' = p(e,f).p(e',f') = p(e\varphi(f)(e'), ff') = e\ \varphi(f)(e')\ ff'$, donc $\varphi(f)(e') = fe'f^{-1}$.
Nous pouvons maintenant faire la synthèse.
Pour tout $f \in F$, notons $\varphi(f)$ l'application $\begin{array}{ccc} E & \longrightarrow & E \\ e & \longmapsto & fef^{-1} \end{array}$. $\varphi(f)$ est correctement définie car E est un sous-groupe distingué de G. On a bien, pour tout $e, e' \in E$, $\varphi(f)(ee') = fee'f^{-1} = (fef^{-1})(fe'f^{-1}) = \varphi(f)(e)\ \varphi(f)(e')$, donc $\varphi(f)$ est un endomorphisme.
De plus, pour tout $f, f' \in F$ et $e \in E$, $\varphi(f) \circ \varphi(f')(e) = ff'ef'^{-1}f^{-1} = \varphi(ff')(e)$, donc $\varphi(f) \circ \varphi(f') = \varphi(ff')$.
En particulier, $\varphi(f)$ est un automorphisme dont l'automorphisme réciproque est $\varphi(f^{-1})$, et donc φ est un morphisme de F dans $\mathrm{Aut}(E)$.
Soit maintenant $(e,f),(e',f') \in E \rtimes_\varphi F$.
$p((e,f).(e',f')) = p(e\varphi(f)(e'), ff') = e\varphi(f)(e')\ ff' = efe'f^{-1}ff' = efe'f'$, donc $p((e,f).(e',f')) = p(e,f)p(e',f')$: p est bien un isomorphisme de $E \rtimes_\varphi F$ dans G.

9°) Par hypothèse, il existe un isomorphisme f_H de H dans H' et un isomorphisme f_K de K dans K'. Pour tout $k' \in K'$, posons $\varphi'(k') = f_H \circ \varphi(f_K^{-1}(k')) \circ f_H^{-1}$. Par composition d'automorphisme, $\varphi'(k') \in \mathrm{Aut}(H')$.
Soit $k, k' \in K'$. Alors $\varphi'(kk') = f_H\varphi(f_K^{-1}(k)f_K^{-1}(k'))f_H^{-1}$, or φ est un morphisme donc $\varphi(f_K^{-1}(k)f_K^{-1}(k')) = \varphi(f_K^{-1}(k))\varphi(f_K^{-1}(k'))$, donc on vérifie aisément que
$\varphi'(kk') = \varphi'(k)\varphi'(k')$, ce qui montre que φ' est un morphisme de K' dans $\mathrm{Aut}(H')$.
Pour tout $(h,k) \in H \rtimes_\varphi K$, posons $g(h,k) = (f_H(h), f_K(k))$ et montrons que g est un isomorphisme de $H \rtimes_\varphi K$ dans $H' \rtimes_{\varphi'} K'$.
Clairement, l'application de $H' \rtimes_{\varphi'} K'$ dans $H \rtimes_\varphi K$ définie par
$(h',k') \longmapsto (f_H^{-1}(h'), f_K^{-1}(k'))$ est l'application réciproque de g, donc g est bijective.
Soit $(h,k),(h',k') \in H \rtimes_\varphi K$.
$g((h,k).(h',k')) = g(h\varphi(k)(h'), kk') = (f_H(h)[f_H \circ \varphi(k)](h'), f_K(k)f_K(k'))$ et
$\begin{aligned} g(h,k).g(h',k') &= (f_H(h), f_K(k)).(f_H(h'), f_K(k')) \\ &= (f_H(h)\varphi'(f_K(k))(f_H(h')), f_K(k)f_K(k')), \end{aligned}$
or $\varphi'(f_K(k))(f_H(h')) = f_H \circ \varphi(k) \circ f_H^{-1}(f_H(h')) = f_H \circ \varphi(k)(h')$, donc on a bien $g((h,k).(h',k')) = g(h,k).g(h',k')$ et g est un isomorphisme de $H \rtimes_\varphi K$ dans $H' \rtimes_{\varphi'} K'$.

10°) a) $Id_{\mathbb{C}} \in D_n$, donc $D_n \neq \emptyset$.
Soit $s, s' \in D_n$. Alors $ss'(\mathbb{U}_n) = s(s'(\mathbb{U}_n)) = \mathbb{U}_n$, donc $ss' \in \mathbb{U}_n$. De plus, $s(\mathbb{U}_n) = \mathbb{U}_n$, donc en prenant l'image de cette égalité par s^{-1}, $\mathbb{U}_n = s^{-1}(\mathbb{U}_n)$, ce qui prouve que $s^{-1} \in \mathbb{U}_n$. En conclusion, D_n est un sous-groupe du groupe des bijections de $\mathbb{C}$ dans $\mathbb{C}$.

10°) b) Posons $\omega = e^{\frac{2i\pi}{n}}$. Ainsi, $\mathbb{U}_n$ est le groupe engendré par ω.
De plus, $\displaystyle\sum_{x \in \mathbb{U}_n} x = \sum_{k=0}^{n-1} \omega^k = \frac{1-\omega^n}{1-\omega}$, car $\omega \neq 1$, donc $\displaystyle\sum_{x \in \mathbb{U}_n} x = 0$.

Soit $s \in D_n$. Alors $s|_{\mathbb{U}_n}^{\mathbb{U}_n}$ est une bijection, donc par changement de variable dans une somme finie, $0 = \sum_{x\in\mathbb{U}_n} x = \sum_{x\in\mathbb{U}_n} s(x)$.
Supposons d'abord que s est une similitude directe : il existe $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$ tel que, pour tout $z \in \mathbb{C}$, $s(z) = az + b$. Alors la relation précédente devient
$0 = \sum_{x\in\mathbb{U}_n} (ax + b) = nb$, donc $s(0) = b = 0$.
Si s est une similitude indirecte, il existe $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$ tel que, pour tout $z \in \mathbb{C}$, $s(z) = a\overline{z} + b$. Alors on obtient $0 = \sum_{x\in\mathbb{U}_n} (a\overline{x} + b) = nb$, donc on a encore $s(0) = b = 0$.

10°) c) Soit $s \in D_n$.
$\diamond$ Supposons d'abord que s est une similitude directe. D'après le b), il existe $\rho \in \mathbb{R}_+^*$ et $\theta \in [0, 2\pi[$ tels que, pour tout $z \in \mathbb{C}$, $s(z) = \rho e^{i\theta} z$.
$1 \in \mathbb{U}_n$, donc $\rho e^{i\theta} = s(1) \in \mathbb{U}_n$. Ainsi, $\rho = 1$ et il existe $k \in \{0, \dots, n-1\}$ tel que $\theta = \frac{2k\pi}{n}$. Donc s est la rotation de centre 0 et d'angle $\frac{2k\pi}{n}$, que l'on notera r_k. Réciproquement, si s est cette rotation, $s(\mathbb{U}_n) = \{e^{\frac{2i(h+k)\pi}{n}} \ / \ h \in \mathbb{Z}\} = \mathbb{U}_n$, donc $s \in D_n$.
Ainsi, en notant S^+ le groupe des similitudes directes, $D_n \cap S^+$ est le groupe Z_n constitué par les rotations de centre 0 et d'angle $\frac{2k\pi}{n}$, avec $k \in \mathbb{Z}$. C'est le groupe cyclique d'ordre n engendré par la rotation, notée r, de centre 0 et d'angle $\frac{2\pi}{n}$. Il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
$\diamond$ Supposons maintenant que s est indirecte. Il existe $\rho \in \mathbb{R}_+^*$ et $\theta \in [0, 2\pi[$ tels que, pour tout $z \in \mathbb{C}$, $s(z) = \rho e^{2i\theta}\overline{z}$.
$1 \in \mathbb{U}_n$, donc $\rho e^{2i\theta} = s(1) \in \mathbb{U}_n$. Ainsi, $\rho = 1$ et il existe $k \in \{0, \dots, n-1\}$ tel que $2\theta = \frac{2k\pi}{n}$. Alors s est l'application $z \longmapsto \overline{z} e^{\frac{2ik\pi}{n}}$ de $\mathbb{C}$ dans $\mathbb{C}$. Il s'agit de la réflexion selon la droite $\mathbb{R}e^{\frac{ik\pi}{n}}$, c'est-à-dire de la symétrie orthogonale par rapport à cette droite.
Réciproquement, pour $k \in \{0, \dots, n-1\}$, notons s_k la réflexion selon la droite $\mathbb{R}e^{\frac{ik\pi}{n}}$. Alors $s_k(\mathbb{U}_n) = \{e^{\frac{2ik\pi}{n}} e^{-\frac{2ih\pi}{n}} \ / \ h \in \mathbb{Z}\} = \mathbb{U}_n$, donc $s_k \in D_n$.
Ainsi, $D_n \cap S^- = \{s_k \ / \ k \in \{0, \dots, n-1\}\}$.

10°) d) Posons $E = Z_n$ et $F = \{Id_{\mathbb{C}}, s_1\}$.
- On sait déjà que E est un sous-groupe de D_n isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Montrons qu'il est distingué :
  Soit $k \in \{0, \dots, n-1\}$ et $s \in D_n$. Il s'agit de montrer que $sr_ks^{-1} \in E$. C'est évident lorsque $s \in E$, car E est un groupe. Il reste à le vérifier lorsque $s = s_h$ avec $h \in \{0, \dots, n-1\}$. Or, pour tout $z \in \mathbb{C}$,
  $s_h r_k s_h^{-1}(z) = s_h r_k s_h(z) = e^{\frac{2ih\pi}{n}} \overline{e^{\frac{2ik\pi}{n}} e^{\frac{2ih\pi}{n}} \overline{z}} = e^{-\frac{2ik\pi}{n}} z$, donc $s_h r_k s_h^{-1} = r_{-k} \in E$.
- $s_1^2 = Id_{\mathbb{C}}$, donc F est un sous-groupe, cyclique d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
- Clairement, $E \cap F = \{1_{D_n}\}$.
- Soit $k \in \{0, \dots, n-1\}$. Pour tout $z \in \mathbb{C}$, $r_{k-1}s_1(z) = e^{\frac{2i(k-1)\pi}{n}} e^{\frac{2i\pi}{n}} \overline{z} = s_k(z)$, donc $E.F = E \cup \{r_k.s_1 \ / \ k \in \mathbb{Z}\} = D_n$.

Alors, d'après la question 8, D_n est isomorphe à un produit semi-direct de E par F, puis d'après la question 9, D_n est isomorphe à un produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.
En reprenant les différentes constructions des questions précédentes, on peut vérifier que l'isomorphisme est $\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} & \longrightarrow & D_n \\ (\overline{k}, \overline{i}) & \longmapsto & r_k s_1^i \end{array}$, où $\varphi(\overline{0}) = Id_{\mathbb{Z}/n\mathbb{Z}}$ et $\varphi(\overline{1}) = -Id_{\mathbb{Z}/n\mathbb{Z}}$.