UNIVERSITÉ DE RENNES 1

Théorie des Groupes et Géométrie

Contrôle Continu n°1 :
Groupes et Géométrie
Une heure
Corrigé

Il n'est pas nécessaire de faire l'intégralité du contrôle pour avoir la note maximale. Les questions marquées d'une étoile sont probablement plus difficiles que les autres.

Questions de cours

1. *Rappeler la définition d'un groupe résoluble.*
   Un groupe G est dit résoluble s'il existe une suite de sous-groupes $G = G_1 \rhd G_2 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{1\}$ (chaque G_{i+1} est distingué dans G_i) avec G_i/G_{i+1} abélien. C'est équivalent à dire que $D^s(G) = \{1\}$ pour un certain $s \in \mathbb{N}^*$.
2. *Donner un plan (vague si nécessaire) de la preuve du fait que $\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*
   On montre d'abord que $\mathfrak{A}_5$ est simple en comptant le cardinal de chaque classe de conjugaison. Si ensuite H est un sous-groupe distingué non trivial de $\mathfrak{A}_n$ pour $n \geqslant 5$, on montre, à l'aide d'un comumutateur de permutations bien choisies, qu'il existe un ensemble E de cardinal 5 tel que $H \cap \mathfrak{A}(E)$ est non trivial, donc $H = \mathfrak{A}(E) \simeq \mathfrak{A}_5$. On en déduit que H possède un 3-cycle, donc H possède tous les 3-cycles de $\mathfrak{A}_n$ (car H est distingué et que tous les 3-cycles sont conjugués, car l'action de $\mathfrak{A}_n$ est $n-2 \geqslant 3$-transitive) donc $H = \mathfrak{A}_n$.

Exercice 1

On considère le sous-groupe de $\mathrm{GL}_3(\mathbb{R})$ *suivant :*

$$H = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \quad | \quad x, y, z \in \mathbb{R} \right\}$$

Sur un coin de feuille, noter proprement le résultat de la multiplication gh de deux éléments $g, h \in H$.
Si $g = \left(\begin{smallmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right)$ et $h = \left(\begin{smallmatrix} 1 & u & w \\ 0 & 1 & v \\ 0 & 0 & 1 \end{smallmatrix}\right)$ alors $gh = \left(\begin{smallmatrix} 1 & x+u & xv+z+w \\ 0 & 1 & y+v \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

1. *Si $g \in H$, calculer explicitement g^{-1}.*
   Par le calcul précédent, si $g = \left(\begin{smallmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right)$ alors $g^{-1} = \left(\begin{smallmatrix} 1 & -x & xy-z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{smallmatrix}\right)$.
2. *Si $g, h \in H$, calculer explicitement $[g, h]$.*
   Soient $g = \left(\begin{smallmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right)$ et $h = \left(\begin{smallmatrix} 1 & u & w \\ 0 & 1 & v \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Par les calculs précédents on a

$$\begin{aligned}
[g,h] &= ghg^{-1}h^{-1} \\
&= gh(hg)^{-1} \\
&= \begin{pmatrix} 1 & x+u & xv+z+w \\ 0 & 1 & y+v \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x+u & yu+z+w \\ 0 & 1 & y+v \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & x+u & xv+z+w \\ 0 & 1 & y+v \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x-u & (x+u)(y+v)-(yu+z+w) \\ 0 & 1 & -y-v \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & x+u & xv+z+w \\ 0 & 1 & y+v \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x-u & xy+xv+uv-z-w \\ 0 & 1 & -y-v \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} 1 & 0 & -(x+u)(y+v)+(xv+z+w)+(xy+xv+uv-z-w) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & xv-yu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Il est bon, outre de vérifier les calculs, de vérifier que le résultat est cohérent : en inversant le résultat on devrait trouver $[g,h]^{-1} = [h,g]$. On a

$$\begin{aligned} [g,h]^{-1} &= \begin{pmatrix} 1 & 0 & xv-yu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 0 & -xv+yu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & uy-vx \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= [h,g], \end{aligned}$$

donc le résultat n'a pas l'air absurde.

3. *Montrer que H est résoluble.*

   La question précédente montre que $D(H) \subseteq \left\{ \left(\begin{smallmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid z \in \mathbb{R} \right\}$. Par le calcul du coin de la feuille, ce dernier groupe est abélien (et même isomorphe à $\mathbb{R}$), donc son groupe dérivé est trivial. Ainsi, on a $D^2(H) = \{1\}$ donc H est résoluble.

   On considère le sous-ensemble N de H donné par :

$$N = \left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \quad \middle| \quad y,z \in \mathbb{R} \right\}$$

4. *Montrer que N est un groupe, $N \lhd H$, $H/N \simeq \mathbb{R}$ et $N \simeq \mathbb{R}^2$. Dans l'ordre que vous souhaitez.*

   Par le calcul du coin de la feuille, l'application f qui à $g = \left(\begin{smallmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right) \in H$ associe $x \in \mathbb{R}$ est un morphisme de groupes. Ainsi, le noyau de f est un sous-groupe distingué de H. Ce noyau est exactement N donc on a bien $N \lhd H$. De plus, puisque f est surjective on a $H/N = H/\ker f \simeq \mathbb{R}$. Finalement, le calcul du coin de la feuille montre que l'application qui à $g = \left(\begin{smallmatrix} 1 & 0 & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right) \in N$ associe $(y,z) \in \mathbb{R}^2$ est un morphisme de groupes. C'est clairement un isomorphisme, donc $N \simeq \mathbb{R}^2$.

5. *En déduire une suite exacte **scindée** $1 \to \mathbb{R}^2 \to H \to \mathbb{R} \to 1$.*
   On considère la suite $1 \to \mathbb{R}^2 \xrightarrow{i} H \xrightarrow{p} \mathbb{R} \to 1$ où :
   - le morphisme i est défini par $i : (y,z) \mapsto \left(\begin{smallmatrix} 1 & 0 & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right)$;
   - le morphisme p est défini par $p : \left(\begin{smallmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right) \mapsto x$.

   Cette suite est exacte puisque $\operatorname{im} i = N = \ker p$. Le morphisme $s : \mathbb{R} \to H$ donné par $s : x \mapsto \left(\begin{smallmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ (c'est bien un morphisme, toujours par le calcul du coin de la feuille) vérifie $p \circ s(x) = p\left(\begin{smallmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) = x$ donc $p \circ s = \mathrm{Id}_{\mathbb{R}}$ donc la suite est scindée.

6*. *Donner une suite exacte **non-scindée** $1 \to \mathbb{R} \to H \to \mathbb{R}^2 \to 1$.*
   Considérons les applications $j : \mathbb{R} \to H$ définie par $z \mapsto \left(\begin{smallmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ et $q : H \to \mathbb{R}^2$ définie par $\left(\begin{smallmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right) \mapsto (x,y)$ (on n'a pas vraiment le choix si on ne veut pas retomber sur l'étude précédente). D'après le calcul du coin de la feuille, ces applications sont des morphismes. De plus, si $K := \left\{ \left(\begin{smallmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid z \in \mathbb{R} \right\}$ alors $\operatorname{im} j = K = \ker q$ donc la suite $1 \to \mathbb{R} \to H \to \mathbb{R}^2 \to 1$ associée est exacte. On peut intuiter qu'elle n'est pas scindée puisqu'un sous-ensemble naturel de H sur lequel q réalise un isomorphisme avec $\mathbb{R}^2$ est $E := \left\{ \left(\begin{smallmatrix} 1 & x & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid x,y \in \mathbb{R} \right\}$, mais E n'est pas un sous-groupe (toujours d'après le calcul du coin de la feuille). Et en effet, supposons que la suite est scindée, c'est-à-dire qu'il existe un morphisme $t : \mathbb{R}^2 \to H$ vérifiant $q \circ t = \mathrm{Id}_{\mathbb{R}^2}$. Par cette

dernière hypothèse, on peut écrire $t(x,y) = \left(\begin{smallmatrix} 1 & x & w(x,y) \\ 0 & 1 & y \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Puisque t est un morphisme, on a, toujours d'après le calcul du coin de la feuille :

$$t(x+x', y+y') = t(x,y)t(x',y') = \begin{pmatrix} 1 & x+x' & xy' + w(x,y) + w(x',y') \\ 0 & 1 & y+y' \\ 0 & 0 & 1 \end{pmatrix}.$$

Mais $\mathbb{R}^2$ est commutatif donc

$$t(x,y)t(x',y') = t(x+x', y+y') = t(x'+x, y'+y) = t(x',y')t(x,y).$$

En regardant le coefficient en haut à droite dans ce produit, on obtient

$$xy' + w(x,y) + w(x',y') = x'y + w(x',y') + w(x,y).$$

Ainsi, on a $xy' = x'y$ pour tout $(x,y), (x',y') \in \mathbb{R}^2$, ce qui est bien sûr absurde. Finalement, on a bien montré que la suite $1 \to \mathbb{R} \xrightarrow{j} H \xrightarrow{q} \mathbb{R}^2 \to 1$ n'est pas scindée.

Rq : (Autre méthode) Par l'absurde. Supposons la suite exacte $1 \to \mathbb{R} \to H \to \mathbb{R}^2 \to 1$ scindée par un morphisme $t : \mathbb{R}^2 \to H$ vérifiant $q \circ t = \mathrm{Id}_{\mathbb{R}^2}$. L'action de $t(\mathbb{R}^2)$ sur K est donnée par la conjugaison dans H. Mais K est inclus dans le centre de H (par le calcul de commutateur Q2) par conséquent l'action de $t(\mathbb{R}^2)$ sur K est triviale. Autrement dit, H est le produit direct $K \times t(\mathbb{R}^2)$ donc H est abélien. Absurde. Donc la suite exacte n'est pas scindée.

Rq : Il n'est pas difficile de montrer que K est le centre de H.

Exercice 2

Soit G un groupe d'ordre $455 = 5 \cdot 7 \cdot 13$. Si p est un nombre premier, on note s_p le nombre de p-Sylow de G.

1. *Montrer que $s_{13} = s_7 = 1$.*
   Par les théorèmes de Sylow on sait d'une part que s_{13} divise $5 \cdot 7$ donc $s_{13} \in \{1, 5, 7, 35\}$. D'autre part, on a $s_{13} \equiv 1 \pmod{13}$ donc la seule possibilité est $s_{13} = 1$. De même, on a s_7 divise $5 \cdot 13$ donc $s_7 \in \{1, 5, 13, 65\}$ mais $s_7 \equiv 1 \pmod{7}$ donc $s_7 = 1$.
2. *En déduire une suite exacte $1 \to N \to G \to K \to 1$ où N est un groupe d'ordre 91 et K un groupe d'ordre 5. Montrer que cette suite exacte est scindée.*
   Soit S_7 (respectivement S_{13}) l'unique 7-Sylow (resp. 13-Sylow) de G. Les groupes S_7 et S_{13} sont distingués dans G (car ce sont des uniques p-Sylow), leur intersection est triviale puisque leurs ordres 7 et 13 sont premiers entre eux donc $N := S_7 S_{13} \simeq S_7 \times S_{13}$ est un sous-groupe distingué de G. Ainsi, si K est un 5-Sylow de G alors NK est un sous-groupe de G (puisque N est distingué). De plus, puisque 91 et 5 sont premiers entre eux on a $N \cap K = \{1\}$, donc $G = NK = N \rtimes K$ puisque $455 = 91 \cdot 5$. Ainsi, la suite canonique $1 \to N \xrightarrow{i} G \xrightarrow{p} K \to 1$ est exacte, et scindée par l'inclusion $K \hookrightarrow G$. On rappelle que $i : N \to G$ est l'inclusion et que $p : G \to K$ est donnée par $p(nk) = k$. L'application p est bien définie par unicité de la décomposition (unicité qui provient de $N \cap K = \{1\}$) et bien un morphisme car N est distingué. Finalement, l'inclusion $K \hookrightarrow G$ est bien une section puisque $p(1k) = p(k) = k$ pour tout $k \in K$.

3*. *Montrer que G est une extension triviale de N et K.*
Dans la suite exacte scindée précédente, on doit montrer que K centralise N, c'est-à-dire que les éléments de K et N commutent. Considérons l'action de K sur N par conjugaison, autrement dit, l'action définissant le produit semi-direct $G = N \rtimes K$. Puisque $N \simeq S_7 \times S_{13} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \simeq \mathbb{Z}/91\mathbb{Z}$ (par théorème chinois ; on a bien 7 et 13 premiers entre eux) et que K est d'ordre 5, l'action est donnée par un morphisme $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/91\mathbb{Z})$. En rappelant que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ si p est premier et que $(A \times B)^\times \simeq A^\times \times B^\times$ si A et B sont des anneaux unitaires, on a :

$$\begin{aligned} \mathrm{Aut}(\mathbb{Z}/91\mathbb{Z}) &\simeq (\mathbb{Z}/91\mathbb{Z})^\times \\ &\simeq (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z})^\times \\ &\simeq (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/13\mathbb{Z})^\times \\ &\simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \end{aligned}$$

Ainsi, si le morphisme ϕ n'est pas trivial, puisque $\mathbb{Z}/5\mathbb{Z}$ est simple ϕ est nécessairement injectif donc $\mathrm{Aut}(\mathbb{Z}/91\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ contiendrait une copie de $\mathbb{Z}/5\mathbb{Z}$, en particulier, un élément d'ordre 5. Mais ceci est impossible puisque tout élément de $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ a un ordre qui divise 12. (Remarquez que

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ n'est *pas* isomorphe à $\mathbb{Z}/72\mathbb{Z}$. Le théorème chinois ne s'applique pas, et puisque $6 \mid 12$ la décomposition $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ est en fait celle, unique, du théorème de structure des groupes abéliens finis.) Finalement, le morphisme ϕ est trivial : on en déduit que tout élément $k \in K$ agit trivialement par conjugaison sur tout élément de N, c'est-à-dire commute avec les éléments de N. On a bien montré que G est une extension triviale de N et K.

Rq : On a pas besoin de se rappeler que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ si p est premier. Il suffit de se rappeler que $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1$ pour conclure. Tout d'abord, il est clair que $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1$ puisque $\mathbb{Z}/p\mathbb{Z}$ est le corps de cardinal p. Enfin, en utilisant ce dernier fait, on obtient que $\mathrm{Aut}(\mathbb{Z}/91\mathbb{Z})$ est d'ordre $6 \cdot 12$ non divisible par 5. Ce qui implique la trivialité du morphisme ϕ.

3. *Montrer que G est cyclique.*
   La suite exacte scindée précédente est triviale donc $G \simeq N \times K$. En effet, les éléments de K et N commutent, le groupe $K \simeq \mathbb{Z}/5\mathbb{Z}$ est commutatif donc les éléments de K et $G = NK$ commutent. On a vu dans la question précédente que $N \simeq \mathbb{Z}/91\mathbb{Z}$, donc puisque 91 et 5 sont premiers entre eux on en déduit par le théorème chinois que $G \simeq \mathbb{Z}/455\mathbb{Z}$ est cyclique.

Exercice 3

Soit σ la permutation de $\{1, \dots, n\}$ donnée par :

$$\sigma = (1\,2\,\cdots\,n)$$

On note T le groupe engendré par σ.

1. *Montrer que T agit transitivement sur $\{1, \dots, n\}$.*
   Dans cet exercice, les classes de congruences modulo n seront prises dans $\{1, \dots, n\}$. Pour tout $k \in \mathbb{N}$ on a $\sigma^k(1) = 1 + k \pmod n$, l'orbite de 1 sous l'action de T est $\{1, \dots, n\}$ donc T agit transitivement sur $\{1, \dots, n\}$.
2. *Montrer que le centralisateur de T dans $\mathfrak{S}_n$ est égal au groupe T.*
   Tout d'abord, puisque $T = \langle\sigma\rangle$ est commutatif il est inclus dans son centralisateur. Soit maintenant ρ dans le centralisateur dans $\mathfrak{S}_n$ de T. Les permutations ρ et σ commutent, donc $\rho\sigma\rho^{-1} = \sigma$. Par la formule de conjugaison, on obtient donc :
   $$\big(\rho(1)\,\rho(2)\,\cdots\,\rho(n)\big) = \sigma.$$
   Ainsi, pour tout k on a $\sigma\big(\rho(k)\big) = \rho(k{+}1)$ donc $\rho(k{+}1) = \rho(k){+}1 \pmod n$, autrement dit $\rho(k) = \rho(1){+}k{-}1 \pmod n$. Par ailleurs, puisque $\sigma^i(j) = j{+}i \pmod n$ pour tout i, j on en déduit que $\sigma^{\rho(1)-1}(k) = k{+}\rho(1){-}1 \pmod n = \rho(k)$ donc $\rho = \sigma^{\rho(1)-1} \in T$. On a donc montré que le centralisateur est inclus dans T, et finalement par double inclusion il est exactement égal à T.

3*. *Déterminer le normalisateur de T.*
   Soit ρ dans le normalisateur dans $\mathfrak{S}_n$ de T. On a $\rho\sigma\rho^{-1} \in T$, donc il existe a tel que $\rho\sigma\rho^{-1} = \sigma^a$. Par la formule de conjugaison précédente on a donc $\sigma^a\big(\rho(k)\big) = \rho(k+1)$ pour tout k, et en utilisant l'expression de σ^a précédente on trouve
   $$\rho(k+1) = \rho(k) + a \pmod n,$$
   donc
   $$\rho(k) = \rho(1) + (k-1)a \pmod n,$$
   pour tout k. Puisque ρ est surjective, nécessairement $\big\{\rho(k) : k \in \{1, \dots, n\}\big\} = \big\{\rho(1) + ka : k \in \{1, \dots, n\}\big\} = \{1, \dots, n\}$, en particulier a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (puisqu'il existe l tel que $la = 1 \pmod n$). Ainsi, si $i \coloneqq \rho(1)$ alors ρ est la permutation donnée par
   $$\rho(k) = i + (k-1)a \pmod n,$$
   pour tout $k \in \{1, \dots, n\}$. Réciproquement, si $i, a \in \{1, \dots, n\}$ avec a inversible modulo n alors l'application $\rho_{i,a} : \{1, \dots, n\} \to \{1, \dots, n\}$ définie par
   $$\rho_{i,a} : k \mapsto i + (k-1)a \pmod n,$$
   est une permutation (elle est bien bijective puisque a est inversible modulo n). Elle normalise T puisque
   $$\begin{aligned}\rho_{i,a}\sigma\rho_{i,a}^{-1} &= \big(\rho_{i,a}(1) \quad \rho_{i,a}(2) \quad \cdots \quad \rho_{i,a}(n)\big)\\ &= \big(i \quad i+a \quad \cdots \quad i+(n-1)a\big)\\ &= \sigma^a.\end{aligned}$$

On a donc montré que le normalisateur N dans $\mathfrak{S}_n$ de T est le sous-groupe formé des permutations de la forme

$$\rho_{i,a} : k \mapsto i + ka \pmod{n},$$

où $i, a \in \{1, \dots, n\}$ avec a premier à n.

Complément. On peut en dire un peu plus sur ce normalisateur. On a

$$\begin{aligned}\rho_{i,a}\big(\rho_{j,b}(k)\big) &= i + \rho_{j,b}(k)a \\ &= i + (j + kb)a \\ &= i + ja + kab \\ &= \rho_{i+ja,ab}(k),\end{aligned}$$

donc $\rho_{i,a}\rho_{j,b} = \rho_{i+ja,ab}$. Ainsi, le groupe N est bien en bijection avec l'ensemble $\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times$, mais la loi de groupe $\star$ sur le produit cartésien est donnée par

$$(i, a) \star (j, b) = (i + ja, ab) = (i + \phi_a(j), ab),$$

où ϕ est l'action par automorphisme (multiplication) de $(\mathbb{Z}/n\mathbb{Z})^\times$ sur $\mathbb{Z}/n\mathbb{Z}$. On en déduit donc que

$$N \simeq \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times.$$