Feuille d'exercices n° 4

Exercice 1
Classifier les groupes d'ordre 15.

Solution 1
Soit G un groupe d'ordre 15. Nous avons $15 = 3 \times 5$. Le nombre de 5-Sylow de G divise 3 et est congru à 1 modulo 5, le groupe G contient donc exactement un 5-Sylow que l'on note H. Puisque H est d'ordre 5 il est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Soit K un 3-Sylow de G ; il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Le groupe H est distingué dans G, |H| et |K| sont premiers entre eux et $|\mathrm{H}| \cdot |\mathrm{K}| = |\mathrm{G}|$. Par conséquent G s'identifie à $\mathrm{H} \rtimes_\psi \mathrm{K}$ pour un certain morphisme $\psi \colon \mathrm{K} \to \mathrm{Aut}(\mathrm{N})$ *i.e.* $\mathrm{G} \simeq \mathbb{Z}/5\mathbb{Z} \rtimes_\psi \mathbb{Z}/3\mathbb{Z}$. Comme 3 est premier à $\left|\left(\mathbb{Z}/5\mathbb{Z}\right)^\times\right| = 4$ le morphisme ψ est trivial [1] et G est isomorphe au produit direct $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ c'est-à-dire à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 2
Classifier les groupes d'ordre 21.

Solution 2
Soit G un sous-groupe d'ordre $21 = 3 \times 7$. Soit n_7 le nombre de 7-Sylow de G. Alors $n_7 \equiv 1 \bmod 7$ et $n_7 | 3$, *i.e.* $n_7 = 1$. Le groupe G contient donc un unique 7-Sylow H qui est donc distingué dans G. Puisque $|\mathrm{H}| = 7$, nous avons l'isomorphisme $\mathrm{H} \simeq \mathbb{Z}/7\mathbb{Z}$. Soit K un 3-Sylow de G ; il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Comme

- $\mathrm{H} \triangleleft \mathrm{G}$,
- |H| et |K| sont premiers entre eux,
- $|\mathrm{H}| \cdot |\mathrm{K}| = |\mathrm{G}|$

le groupe G s'identifie à $\mathrm{H} \rtimes_\psi \mathrm{K}$ pour un certain morphisme $\psi \colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$. Il existe donc un morphisme

$$\varphi \colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right)$$

tel que $\mathrm{G} \simeq \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. Nous sommes dans l'un des deux cas suivants, exclusifs l'un de l'autre :

- G est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$;
- G est isomorphe à $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où $\varphi(\underbrace{\overline{r}}_{\bmod 3})(x) = \underbrace{\overline{2}^r}_{\bmod 7} x$.

En effet nous allons décrire tous les produits semi-directs de la forme $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. Rappelons que $\mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right) \simeq \left(\mathbb{Z}/7\mathbb{Z}\right)^\times$. Le groupe $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$ est égal à $\{-\overline{3}, -\overline{2}, -\overline{1}, \overline{1}, \overline{2}, \overline{3}\}$; il est cyclique (en effet si $\Bbbk$ est un corps commutatif et si G est un sous-groupe fini de $\Bbbk^\times$, alors G est cyclique). Nous avons $\overline{2} \neq \overline{1}$ et $\overline{2}^3 = \overline{8} = \overline{1}$. Par suite $\overline{2}$ est d'ordre 3 et $\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}\}$ est donc l'unique sous-groupe d'ordre 3 de $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$ qui est aussi le groupe des éléments de 3-torsion de $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$. Les produits semi-directs cherchés sont en conséquence les suivants :

- le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{1}}} \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$;
- le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ dont la loi interne est donnée par

$$(\overline{u}, \overline{r}) \cdot (\overline{v}, \overline{s}) = (\overline{u} + \overline{2}^r \overline{v}, \overline{r} + \overline{s});$$

1. Supposons que m est premier au cardinal de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Dans ce cas tout élément de m-torsion de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est trivial ; le seul produit semi-direct de la forme $\mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ est donc le produit direct $\mathbb{Z}/n\mathbb{Z} \times_\varphi \mathbb{Z}/m\mathbb{Z}$.

◇ le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ dont la loi interne est donnée par

$$(\overline{u}, \overline{r}) \cdot (\overline{v}, \overline{s}) = (\overline{u} + \overline{4}^{r}\overline{v}, \overline{r} + \overline{s}).$$

Les groupes $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ sont non abéliens. En effet dans $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ nous avons

$$(\overline{1}, \overline{0}) \cdot (\overline{0}, \overline{1}) = (\overline{1}, \overline{1}) \neq (\overline{2}, \overline{1}) = (\overline{0}, \overline{1}) \cdot (\overline{1}, \overline{0})$$

et dans $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ nous avons

$$(\overline{1}, \overline{0}) \cdot (\overline{0}, \overline{1}) = (\overline{1}, \overline{1}) \neq (\overline{4}, \overline{1}) = (\overline{0}, \overline{1}) \cdot (\overline{1}, \overline{0})$$

En particulier ils sont tous deux non isomorphes au produit direct $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Par contre $(\overline{u}, \overline{r}) \mapsto (\overline{u}, 2\overline{r})$ définit un isomorphisme de groupes de $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ de réciproque donnée par la même formule.

Exercice 3

Soient p et q des nombres premiers avec $p < q$. Montrer que

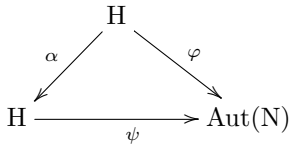
◇ si p ne divise pas $q - 1$, alors tout groupe d'ordre pq est cyclique.

◇ si p divise $q - 1$, il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi-direct non abélien.

Solution 3

Énonçons le résultat suivant dont nous aurons besoin :

Lemme 0.1 *Soient* H *et* N *deux groupes. Soient* φ *et* ψ *deux opérations de* H *sur* N *et* α *un automorphisme de* H *tels que le diagramme suivant commute*



i.e. $\varphi = \psi \circ \alpha$.

L'application $(n, h) \mapsto (n, \alpha(h))$ *est un isomorphisme de* $\mathrm{N} \rtimes_{\psi} \mathrm{H}$ *sur* $\mathrm{N} \rtimes_{\varphi} \mathrm{H}$.

Soit G un groupe d'ordre pq où p et q désignent des nombres premiers tels que $p < q$. Soit Q un q-Sylow de G.

D'après les théorèmes de Sylow

$$\begin{cases} n_q \text{ divise } p \\ n_q \equiv 1 \bmod q \end{cases}$$

où n_q est le nombre de q-Sylow de G. Par suite $n_q = 1$ et Q est distingué dans G.

Puique p est premier, $\mathbb{Q} \simeq \mathbb{Z}/q\mathbb{Z}$. De même $\mathrm{G}/\mathrm{Q} \simeq \mathbb{Z}/p\mathbb{Z}$. Si P est un p-Sylow quelconque il fournit un relèvement de G/Q et donc

$$\mathrm{G} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Calculons ces produits. Nous avons $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ [2]. L'opération de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ correspond donc à un morphisme

$$\varphi \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}.$$

Nous avons l'alternative suivante :

2. Les groupes $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ et $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ sont isomorphes

$$\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$$

En particulier $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est un groupe abélien de cardinal $\varphi(n)$.

De plus, si p est un nombre premier, alors

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

- ◇ p ne divise pas $q-1$, alors φ est trivial, le produit est direct et $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{pq\mathbb{Z}}$ est cyclique.
- ◇ p divise $q-1$, ${}^{\mathbb{Z}}\!/_{(q-1)\mathbb{Z}}$ possède un unique sous-groupe d'ordre p, il y a donc une opération non triviale. De plus deux telles opérations diffèrent d'un automorphisme de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Le lemme 0.1 assure que les produits correspondants sont isomorphes.

Exercice 4

Montrer que tout groupe d'ordre 217 est cyclique (Indication : commencer par calculer le nombre de p-Sylow pour chaque diviseur premier p de 217).

Solution 4

Soit G un groupe d'ordre 217. Notons que $217 = 7 \times 31$ et que 7 et 31 sont premiers. Le nombre de 7-Sylow de G est congru à 1 modulo 7 et divise 31 : la seule possibilité est donc 1. D'autre part le nombre de 31-Sylow est congru à 1 modulo 31 et divise 7 ; de nouveau la seule possibilité est 1. Ainsi G contient un unique 7-Sylow $S_7 \subset \mathrm{G}$, qui est donc distingué, et de même contient un unique 31-Sylow $S_{31} \subset \mathrm{G}$, lui-aussi distingué.

L'intersection $S_7 \cap S_{31}$ est triviale par Lagrange.

Puisque S_7 est distingué dans G, $S_7 S_{31}$ est un sous-groupe de G [3]. Comme il contient strictement S_7 et S_{31}, son ordre est un multiple strict de 7 et de 31, la seule possibilité est donc 217 et on conclut que $\mathrm{G} = S_7 \times S_{31}$.

Puisque S_7 et S_{31} sont d'ordre premiers ils sont cycliques et $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{7\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{31\mathbb{Z}}$; par le théorème chinois on conclut que $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{217\mathbb{Z}}$.

Exercice 5

Soient p un nombre premier et n un entier naturel avec $p > n$. Considérons un groupe G d'ordre pn et H un sous-groupe de G d'ordre p. Montrer que H est un sous-groupe distingué de G.

Indication : compter les p-Sylow de G.

Solution 5

D'après les hypothèses, $\mathrm{pgcd}(p, n) = 1$, donc H est un p-Sylow de G. Notons n_p le nombre de p-Sylow de G. Alors par les théorèmes de Sylow, $n_p \equiv 1 \bmod p$ et $n_p | n$. Si $n_p \neq 1$, alors $n_p \geqslant p+1$, ce qui contredit que n_p divise n puisque $n < p$. Ainsi, $n_p = 1$ et H est l'unique p-Sylow de G donc est distingué dans G.

Exercice 6

Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_2)$ le groupe des matrices à coefficients dans le corps à deux éléments et de déterminant 1.

1. Quel est l'ordre de G ? Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
2. Soit X l'ensemble des 2-Sylow de G. Donner la liste de ses éléments.
   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose
   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}$$
   Montrer par un calcul direct que cette action est transitive.
   Quel est le stabilisateur de
   $$S_0 = \left\{ \mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} ?$$
3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.
   Montrer que
   $$\phi \colon \mathrm{G} \to \mathcal{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$
   est un isomorphisme de groupes.

Solution 6

3. On utilise la propriété suivante : si $\mathrm{K} \subset \mathrm{G}$ est un sous-groupe distingué, et $\mathrm{H} \subset \mathrm{G}$ est un sous-groupe, alors $\mathrm{KH} = \{kh \mid k \in \mathrm{K},\ h \in \mathrm{H}\}$ est un sous-groupe de G ; cela découle de :
$$\forall\, k_1,\, k_2 \in \mathrm{K},\ \forall\, h_1,\, h_2 \in \mathrm{H} \qquad (k_1 h_1)(k_2 h_2) = \underbrace{k_1 h_1 k_2 h_1^{-1}}_{\in \mathrm{K}} \underbrace{h_1 h_2}_{\in \mathrm{H}} \in \mathrm{KH}$$

1. Déterminons l'ordre de G. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de G. Nous avons $ad + bc = \overline{1}$ donc
   — ou bien $ad = \overline{1}$ et $bc = \overline{0}$;
   — ou bien $ad = \overline{0}$ et $bc = \overline{1}$.
   On a $ad = \overline{1}$ et $bc = \overline{0}$ si et seulement si $(a, b, c, d) = (1, 0, 1, 1)$ ou $(a, b, c, d) = (1, 1, 0, 1)$ ou $(a, b, c, d) = (1, 0, 0, 1)$ ce qui donne 3 possibilités.
   De même $ad = \overline{0}$ et $bc = \overline{1}$ donne 3 possibilités.
   Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
   Soient n_2 le nombre de 2-Sylow de G et n_3 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 | 3$$

   et

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 | 2$$

   Par conséquent $n_3 = 1$, *i.e.* G contient un unique 3-Sylow qui est donc distingué dans G. Le seul sous-groupe d'ordre 3 est constitué de l'identité, de $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $D^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.
   Les éléments d'ordre 2 sont

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

2. Soit X l'ensemble des 2-Sylow de G. La liste des éléments de X est : $\{\langle A\rangle, \langle B\rangle, \langle C\rangle\}$.
   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

$$g \cdot S = gSg^{-1} = \{ghg^{-1} \,|\, h \in S\}$$

   Montrons par un calcul direct que cette action est transitive :

$$B \cdot \langle A\rangle = \langle C\rangle \qquad A \cdot \langle C\rangle = \langle B\rangle \qquad C \cdot \langle B\rangle = \langle A\rangle$$

   Quel est le stabilisateur de

$$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\} ?$$

   Déterminons le stabilisateur de $\langle A\rangle$. C'est un sous-groupe de G dont l'ordre divise $|\mathrm{G}|$. Il contient Id et A mais ni B, ni C : $B \cdot \langle A\rangle = \langle C\rangle$ et $C \cdot \langle A\rangle = \langle B\rangle$. Ce stabilisateur est donc $\langle A\rangle$.
3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.
   Montrer que

$$\phi \colon \mathrm{G} \to \mathcal{S}_X, \qquad\qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.
   Puisque G agit sur X le morphisme ϕ est un morphisme de groupes. Il est injectif car

$$\begin{aligned} \ker \phi &= \{g \in \mathrm{G} \,|\, \phi(g) = \mathrm{id}_X\} \\ &= \{g \in \mathrm{G} \,|\, g \cdot S = S \quad \forall\, S \in X\} \\ &= \bigcup_{S \in X} \mathrm{G}_S \\ &= \{e_{\mathrm{G}}\}. \end{aligned}$$

   Comme $\mathcal{S}_X$ et G ont même ordre (6) nous obtenons que ϕ est un isomorphisme.

Exercice 7

Expliciter les sous-groupes de Sylow des groupes alternés $\mathcal{A}_4$ et $\mathcal{A}_5$.

Solution 7

Déterminons les sous-groupes de Sylow de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.
Les théorèmes de Sylow assurent que

— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;
— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.

Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de KLEIN $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Si c'est 4 l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathcal{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathcal{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_5$ ne contient pas d'élément d'ordre 4. En effet les éléments d'ordre 4 du groupe symétrique $\mathcal{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de {1, 2, 3, 4, 5}. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à {e}. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.

Exercice 8

Soit G un groupe d'ordre 2009.

1. Montrer que $G \simeq P \times Q$ où P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. En déduire que chaque groupe d'ordre 2009 est abélien.
2. Classifier à isomorphisme près tous les groupes d'ordre 2009.
3. Soient P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. Montrer que $\mathrm{Aut}(G) \simeq \mathrm{Aut}(P) \times \mathrm{Aut}(Q)$.
4. Montrer que
   a) si Q est cyclique, alors Aut(Q) est cyclique aussi. Quel est l'ordre de Aut(Q) quand Q est cyclique ?
   b) si Q n'est pas cyclique, alors Aut(Q) est isomorphe à $\mathrm{GL}(2, \mathbb{F}_7)$ où $\mathbb{F}_7$ est le corps à 7 éléments. Quel est l'ordre de $\mathrm{GL}(2, \mathbb{F}_7)$?

Solution 8

1. Notons que $|G| = 2009 = 7^2 \times 41$. D'après le premier théorème de Sylow le groupe G possède un 41-Sylow P d'ordre 41 et un 7-Sylow Q d'ordre 49. Notons n_p le nombre de p-Sylow de G. D'après le troisième théorème de Sylow
   ◇ n_{41} est congru à 1 modulo 41 et divise 49 donc est égal à 1 ;
   ◇ n_7 est congru à 1 modulo 7 et divise 41 donc est égal à 1.

   Nous en déduisons que $P \triangleleft G$ et $Q \triangleleft G$.

   Nous constatons aussi que $P \cap Q = \{e\}$, que $G = PQ$ et que les deux sous-groupes dans le produit sont distingués dans G. Tout ceci revient à dire $G \simeq P \times Q$.

   Reste à montrer que G est abélien. Notons que P et Q sont abéliens puisque P est d'ordre premier et que Q est d'ordre premier au carré. Par ailleurs les éléments de P commutent avec ceux de Q. Ainsi G est abélien.

2. D'après 1. tous les groupes d'ordre 2009 sont abéliens, il suffit donc pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupe non isomorphes d'ordre 2009

$$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$$

soit encore

$$\mathbb{Z}/2009\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z}$$

3. **Remarque**. Si φ est un automorphisme de G, alors $\varphi(\mathrm{P}) = \mathrm{P}$ et $\varphi(\mathrm{Q}) = \mathrm{Q}$. En effet comme dans tout groupe et pour tout p premier l'image par un morphisme d'un p-élément est un p-élément et que P et Q sont les seuls 41-Sylow et 7-Sylow de G respectivement, $\varphi(\mathrm{P}) \subset \mathrm{P}$ et $\varphi(\mathrm{Q}) \subset \mathrm{Q}$. Comme φ est une bijection ces deux inclusions sont en fait des égalités.

   Il découle de la Remarque précédente que la restriction de tout automorphisme $\varphi \in \mathrm{Aut(G)}$ au sous-groupe P (respectivement Q) est un automorphisme qu'on appellera φ_P (respectivement φ_Q) de P (respectivement Q). Les automorphismes de φ_P et φ_Q ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes P et Q respectivement.

   Considérons l'application

$$\Phi\colon \mathrm{Aut(G)} \to \mathrm{Aut(P)} \times \mathrm{Aut(Q)}, \qquad \varphi \mapsto (\varphi_\mathrm{P}, \varphi_\mathrm{Q})$$

   Remarquons que $\Phi(\mathrm{id}) = (\mathrm{id}, \mathrm{id})$. Soient φ et ϕ deux éléments de Aut(G). Alors d'une part

$$\begin{aligned}(\varphi \circ \phi)_\mathrm{P}(\mathrm{P}) &= (\varphi \circ \phi)(\mathrm{P}) \\ &= \varphi(\phi(\mathrm{P})) \\ &= \varphi_\mathrm{P}(\phi_\mathrm{P}(\mathrm{P})) \\ &= (\varphi_\mathrm{P} \circ \phi_\mathrm{P})(\mathrm{P})\end{aligned}$$

   et d'autre part

$$\begin{aligned}(\varphi \circ \phi)_\mathrm{Q}(\mathrm{Q}) &= (\varphi \circ \phi)(\mathrm{Q}) \\ &= \varphi(\phi(\mathrm{Q})) \\ &= \varphi_\mathrm{Q}(\phi_\mathrm{Q}(\mathrm{Q})) \\ &= (\varphi_\mathrm{Q} \circ \phi_\mathrm{Q})(\mathrm{Q})\end{aligned}$$

   Autrement dit Φ est un morphisme de groupes.

   Montrons maintenant que Φ est un isomorphisme.

   Commençons par montrer que Φ est injective. Un automorphisme φ de Aut(G) appartient à $\ker\Phi$ si et seulement si $\varphi_\mathrm{P} = \mathrm{id}_\mathrm{P}$ et $\varphi_\mathrm{Q} = \mathrm{id}_\mathrm{Q}$. Or tout élément de G s'écrit sous la forme xy avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. Ainsi

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi_\mathrm{P}(x)\varphi_\mathrm{Q}(y) = \mathrm{id}_\mathrm{P}(x)\mathrm{id}_\mathrm{Q}(y) = xy.$$

   Montrons que Φ est surjective. Soient φ_1 dans Aut(P) et φ_2 dans Aut(Q). Considérons l'application

$$\varphi\colon \mathrm{G} \to \mathrm{G}, \qquad xy \mapsto \varphi_1(x)\varphi_2(y)$$

   avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. L'application σ est définie sans ambiguïté puisque G étant la somme directe de P et de Q chacun de ses éléments s'écrit de manière unique comme produit d'un élément de P et d'un autre de Q Montrons que φ est un automorphisme de G dont l'image sous l'action de Φ est (φ_1, φ_2).

   Le fait que φ_1 et φ_2 soient des morphismes de groupes entraîne que φ est un morphisme de groupes. Il en est de même pour la surjectivité de φ. Supposons que $\varphi(xy) = 1$ pour $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. La définition de φ implique que $\varphi_1(x)\varphi_2(x) = 1$. Or $\varphi_1(x)$ appartient à P, $\varphi_2(y)$ appartient à Q et $\mathrm{P} \cap \mathrm{Q} = \{e\}$ donc $\varphi_1(x) = \varphi_2(y) = 1$. Puisque φ_1 est un automorphisme de P et φ_2 un automorphisme de Q nous obtenons $x = y = 1$. Comme $\mathrm{G} = \mathrm{PQ}$ tout élément de $\ker\varphi$ s'écrit comme produit d'un $x \in \mathrm{P}$ et d'un $y \in \mathrm{Q}$. Ainsi $\ker\varphi = \{e\}$.

   Finalement φ est un automorphisme de G. Il s'ensuit de la définition de φ que $\varphi_\mathrm{P} = \varphi_1$ et $\varphi_\mathrm{Q} = \varphi_2$. Par conséquent $\Phi(\varphi) = (\varphi_1, \varphi_2)$. Ainsi Φ est surjective.

4. a) Si Q est cyclique, il est isomorphe à $\left(\mathbb{Z}/_{49\mathbb{Z}}, +\right)$. Alors $|\mathrm{Aut}(\mathrm{Q})| = \varphi(49) = 7 \times 6 = 42$ où φ est la fonction indicatrice d'Euler. Comme $42 = 2 \times 3 \times 7$ le théorème chinois assure que $\mathrm{Aut}(\mathrm{Q})$ est cyclique d'ordre 42.

   b) Supposons maintenant que Q soit non cyclique. Alors $\mathrm{Q} \simeq \left(\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}}, +\right)$. Ce dernier groupe peut aussi être considéré comme l'espace vectoriel de dimension 2 sur le corps $\mathbb{F}_7$ avec la base canonique $e_1 = (1,0)$ et $e_2 = (0,1)$. La loi externe induite par $\mathbb{F}_7$ est décrite par les identités

$$\lambda e_1 = \underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}} \qquad \lambda e_2 = \underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}$$

   avec $\lambda \in \mathbb{F}_7$, identités qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.
   Soit $\varphi \in \mathrm{Aut}(\mathrm{Q})$, alors

$$\begin{aligned}
\varphi(\lambda e_1) &= \varphi(\underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}}) \\
&= \underbrace{\varphi(1,0) + \varphi(1,0) + \ldots + \varphi(1,0)}_{\lambda \text{ fois}} \\
&= \lambda\varphi((1,0)) \\
&= \lambda\varphi(e_1)
\end{aligned}$$

   et

$$\begin{aligned}
\varphi(\lambda e_2) &= \varphi(\underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}) \\
&= \underbrace{\varphi(0,1) + \varphi(0,1) + \ldots + \varphi(0,1)}_{\lambda \text{ fois}} \\
&= \lambda\varphi((0,1)) \\
&= \lambda\varphi(e_2)
\end{aligned}$$

   Ainsi φ est une application linéaire. Étant bijectif $\varphi \in \mathrm{GL}(2, \mathbb{F}_7)$. Par suite $\mathrm{Aut}(\mathrm{Q}) \subset \mathrm{GL}(2, \mathbb{F}_7)$. L'autre inclusion est claire car chaque bijection linéaire de $\mathbb{F}_7 \times \mathbb{F}_7$ est aussi un automorphisme du groupe $\mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}}$. Finalement $|\mathrm{GL}(2, \mathbb{F}_7)| = (7^2 - 1)(7^2 - 7)$.

Exercice 9

1. Soit G un groupe fini. Notons $\mathrm{Syl}_p(\mathrm{G})$ l'ensemble des p-sous-groupes de Sylow de G. Supposons que $|\mathrm{Syl}_p(\mathrm{G})| = m$. Montrons qu'il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathcal{S}_m$.
2. Soit G un groupe de cardinal 36. Montrer qu'il n'est pas simple.

Solution 9

1. D'après les théorèmes de Sylow l'action par conjugaison

$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}) \qquad (g, P) \mapsto gPg^{-1}$$

   est transitive et détermine donc un morphisme non trivial $\rho\colon \mathrm{G} \to \mathrm{Bij}\big(\mathrm{Syl}_p(\mathrm{G})\big) \simeq \mathcal{S}_m$.
2. Remarquons que $|\mathrm{G}| = 2^2 \times 3^2$. Soit n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise $2^2 = 4$ et que $n_3 \equiv 1 \bmod 3$, autrement dit que n_3 appartient à $\{1, 4\}$.
   Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est forcément distingué dans G ; en particulier G n'est pas simple.
   Si $n_3 = 4$, alors d'après 1. il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathcal{S}_4$. Puisque $|\mathrm{G}| = 36$ et $|\mathcal{S}_4| = 24$ ce morphisme n'est pas injectif. Ainsi $\ker\rho$ est un sous-groupe distingué non trivial et propre de G.