Chapitre II

Outils de base pour la classification des groupes de petit cardinal

Le titre est-il clair ? Que signifie petit ? Pas très grand, ok, mais pour quel ordre ?

Le but de ce cours est de fournir et de mettre en pratique quelques outils pour classifier les groupes finis. Avec ces outils, on devrait pouvoir classifier tous les groupes d'ordre compris entre 2 et 63, à l'exception de 16 et 32.

II.1 Sous-groupe d'indice donné

Quand on nous confie un sous-groupe H d'indice donné dans un groupe G, on doit tout d'abord considérer le quotient (l'ensemble des classes à gauche) G/H. Il n'a pas une structure de groupe en général, mais en revanche, il récupère une action naturelle de G par multiplication à gauche. Ce n'est peut-être pas grand chose pour vous, mais pour moi, ça veut dire beaucoup. Voici pour commencer une machine à dénicher des sous-groupes distingués.

Proposition II.1.1. *Soit G un groupe fini d'ordre n. Soit p le plus petit nombre premier qui divise n. On suppose que H est un sous-groupe d'indice p, alors H est distingué.*

Démonstration. On fait agir à gauche H sur G/H, ce dernier étant un ensemble de cardinal p. On obtient un morphisme de H dans $\mathcal{S}_p$. Or, H stabilise la classe de l'élément neutre puisque $H.H = H$. Donc permute les $p-1$ classes restantes. On en déduit un morphisme de H vers le sous-groupe isomorphe à $\mathcal{S}_{p-1}$ qui stabilise la classe du neutre. Mais aucun diviseur de $|H|$ ne divise $|\mathcal{S}_{p-1}|$. Donc, le morphisme est trivial.

On vient de montrer que pour tout g de G, $H.gH = gH$. Cela signifie que $g^{-1}Hg = H$. Donc, H est distingué.

Dans le même ordre d'idée, on a ce résultat classique :

Exercice II.1.2. Soit $n \geq 5$.

1. Montrer que tout sous-groupe distingué de $\mathcal{S}_n$ non trivial est $\mathcal{A}_n$.
   Ind. : Appelons-le G. Son intersection avec $\mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{A}_n$. Si l'intersection est triviale, G est d'ordre au plus 2. Si l'intersection est $\mathcal{A}_n$, alors G n'a pas trop le choix.
2. En déduire que tout sous-groupe G de $\mathcal{S}_n$ d'indice n est isomorphe à $\mathcal{S}_{n-1}$.
   Ind. : On fait agir $\mathcal{S}_n$ à gauche sur $\mathcal{S}_n/G$. On obtient un morphisme de $\mathcal{S}_n$ vers $\mathcal{S}_n$ (car $\mathcal{S}_n/G$ est de cardinal n). L'action est transitive, il en résulte que l'image du morphisme ne

peut être d'ordre inférieur à 2, et donc que le noyau ne peut être $\mathcal{S}_n$ ou $\mathcal{A}_n$. Ainsi, l'action est fidèle. On regarde la restriction de cette action à G et on récupère l'isomorphisme voulu.

II.2 Théorème de structure des groupes abéliens finis

Lorsque l'on veut classifier (à isomorphisme près !) les groupes d'ordre n, on commence par en trouver les abéliens. Cela n'est pas bien difficile quand on dispose du théorème de structure.

Théorème II.2.1. *Soit A un groupe abélien fini. Il existe une unique famille d'entiers positifs $(a_1, a_2, \cdots, a_k)$ telle que a_{i+1} divise a_i et*

$$A = \prod_i \mathbb{Z}/a_i\mathbb{Z}$$

Exercice II.2.2. Les groupes $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ et $\mathbb{Z}/180\mathbb{Z} \times \mathbb{Z}/108\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ sont-ils isomorphes ?

Exercice II.2.3. Soit $P(n)$ le nombre de partitions de du nombre naturel n.

1. Montrer que pour tout nombre premier, le nombre de groupes abéliens finis, à isomorphisme près, d'ordre p^n est égal à $P(n)$.
2. Soit q premier distinct de p, montrer que pour tout nombre premier, le nombre de groupes abéliens finis, à isomorphisme près, d'ordre $p^n q^m$ est égal à $P(n)P(m)$.
3. Combien y a-t-il de groupes abéliens finis d'ordre a donné ?

II.3 Produits semi-directs et isomorphismes

Lorsque l'on veut classifier des groupes de petit cardinaux, on tombe souvent sur des produits semi-directs de groupes classiques. Le problème est de déterminer si les sous-groupes obtenus sont isomorphes ou non. On présente ici un critère utile.

Le produit semi-direct $H \rtimes_\phi K$ des groupes H et K via le morphisme ϕ de K vers $\mathrm{Aut}(H)$ est défini par l'opération suivante sur $H \times K$

$$(h, k)(h', k') = (h\phi_k(h'), kk').$$

Remarque II.3.1. Le signe $\rtimes$ sous-entend que si K est distingué, alors le produit est direct. Ce qui est vrai : on voit en assimilant H à $H \times \{e_K\}$ et idem pour K que la composante en H de $h^{-1}kh$ est $h^{-1}\phi_k(h)$ et si K est distingué, cette composante se doit d'être neutre. Ce qui donne $\phi_k(h) = h$ et donc le produit est bien direct.

A quelle condition sur ϕ et ψ a-t-on deux produits semi-directs isomorphes ? Voici une condition nécessaire :

Proposition II.3.2. *Soit ϕ et ψ deux morphismes que K vers $\mathrm{Aut}(H)$. On suppose $\tau \in \mathrm{Aut}(K)$ et $\sigma \in \mathrm{Aut}(H)$ tels que le diagramme suivant soit commutatif*

$$\begin{array}{ccc} K & \xrightarrow{\phi} & \mathrm{Aut}(H) \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle Int_\sigma} \\ K & \xrightarrow{\psi} & \mathrm{Aut}(H) \end{array}$$

Alors, les produits semi-directs $H \rtimes_\phi K$ et $H \rtimes_\psi K$ sont isomorphes par l'isomorphisme ι : $(h, k) \mapsto (\sigma(h), \tau(k))$.

Démonstration. Le diagramme commutatif signifie que pour tout k de K,

$$\psi \circ \tau(k) = \sigma \circ \phi(k) \circ \sigma^{-1}$$

On note $\cdot_\phi$ et $\cdot_\psi$ pour différencier les deux multiplications dans les deux PSD. On calcule d'une part

$$\iota\big((h,k) \cdot_\phi (h',k')\big) = \iota(h\phi(k)(h'), kk') = (\sigma(h)\sigma \circ \phi(k)(h'), \tau(k)\tau(k'))$$

Et d'autre part

$$\iota(h,k) \cdot_\psi \iota(h',k') = (\sigma(h),\tau(k)) \cdot_\psi (\sigma(h'),\tau(k')) = (\sigma(h)\psi \circ \tau(k)(\sigma(h')), \tau(k)\tau(k'))$$

L'égalité est alors assurée par la formule $\psi \circ \tau(k) \circ \sigma = \sigma \circ \phi(k)$.

Exemple II.3.3. Soit p, q deux nombres premiers tels que p divise $q-1$. Alors il existe à isomorphisme près deux produits semi-directs (dont le direct !) $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Effectivement, on cherche les morphismes ϕ de $\mathbb{Z}/p\mathbb{Z}$ dans $\operatorname{Aut}\mathbb{Z}/q\mathbb{Z} \simeq (\mathbb{Z}/q\mathbb{Z})^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. Donc, on cherche $\phi(\bar{1})$, c'est-à-dire un élément de $\mathbb{Z}/(q-1)\mathbb{Z}$ annulé par p. Comme p est premier, cet élément est soit d'ordre 1, donc nul, soit d'ordre p. Le premier cas donne le produit direct. On veut montrer que si $\phi(\bar{1})$ et $\psi(\bar{1})$ sont d'ordre p, alors les deux PSD $H \rtimes_\phi K$ et $H \rtimes_\psi K$ sont isomorphes. Pour cela, on remarque encore une fois qu'il n'y a qu'un sous-groupe d'ordre p dans $\mathbb{Z}/(q-1)\mathbb{Z}$ (il est engendré par la classe de $\frac{q-1}{p}$). Donc, comme $\phi(\bar{1})$ et $\psi(\bar{1})$ engendrent tout deux un sous-groupe d'ordre p, il s'agit du même sous-groupe, et en exprimant que $\phi(\bar{1})$ se situe dans le sous-groupe engendré par $\psi(\bar{1})$, on obtient $\phi(\bar{1}) = k\psi(\bar{1}) = \psi(k.\bar{1})$, avec k non nul dans $\mathbb{Z}/p\mathbb{Z}$. Il vient que l'automorphisme τ de $\mathbb{Z}/p\mathbb{Z}$ donné par $\tau(h) = kh$ vérifie $\psi\tau = \phi$ (il suffit de le vérifier sur $\bar{1}$) et les conditions de la proposition sont vérifiées avec σ trivial.

Les produits semi-directs nous engagent à décrire le groupe des automorphismes d'un groupe donné. C'est en général difficile, mais en ce qui concerne les groupes abéliens finis, on peut parfois s'en sortir grâce au lemme chinois et aux résultats suivants

Proposition II.3.4. *On doit connaître les automorphismes de groupes suivants*

1. $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$
2. $\operatorname{Aut}\left((\mathbb{Z}/p\mathbb{Z})^n\right) \simeq \mathrm{GL}_n(\mathbb{F}_p)$
3. *Pour p impair,* $\operatorname{Aut}(\mathbb{Z}/p^n\mathbb{Z})$ *est cyclique d'ordre* $\phi(p^n) = p^{n-1}(p-1)$
4. *Si $m \geq 3$,* $\operatorname{Aut}(\mathbb{Z}/2^m\mathbb{Z})$ *est produit direct d'un groupe d'ordre 2 et d'un groupe cyclique d'ordre* 2^{m-2}
5. *Si G et H sont d'ordres premiers entre eux, alors* $\operatorname{Aut}(G \times H) \simeq \operatorname{Aut}(G) \times \operatorname{Aut}(H)$.

Démonstration. Dernier point : Soit ϕ un automorphisme de $G \times H$. Posons $\phi(g, e_H) = \phi_1(g)$. L'ordre o de $\phi_1(g)$ est égal à celui de (g, e_H) qui divise $|G|$. Donc si on pose $\phi_1(g) = (g', h')$, on obtient que l'ordre de (g', h') est d'une part o, d'autre part, le ppcm des ordres de g' et h', qui est par hypothèse le produit de ces ordres. Conclusion, l'ordre de h' est 1, et donc $h' = e_H$.

Il en résulte que $G \times \{e_H\} (\simeq G)$ est stabilisé par ϕ et on note ϕ_1 la restriction. De même pour la restriction ϕ_2 de ϕ à $\{e_G\} \times H$. On vérifie pour finir que $\phi \mapsto (\phi_1, \phi_2)$ fournit l'isomorphisme demandé.

II.4 Etude des p-groupes

L'étude des sous-groupes de Sylow est bien utilie pour pouvoir reconstituer le groupe tout entier. Mais encore faut-il savoir classifier les groupes d'ordre une puissance de p. Voici les premiers barreaux de l'échelle.

Définition II.4.1. Un p-groupe est un groupe d'ordre p^α, où p est un nombre premier et α non nul.

En appliquant la formule des classes à l'action d'un p-groupe par conjugaison sur lui-même, on obtient.

Proposition II.4.2. *Le centre d'un p-groupe est non trivial.*

Du coup, par récurrence sur l'ordre et en quotientant, on obtient ce que l'on peut voir comme une réciproque au théorème de Lagrange :

Proposition II.4.3. *Soit G un groupe d'ordre p^α. Alors, pour tout $\beta \leq \alpha$, il existe un sous-groupe distingué de G d'ordre p^β.*

Pour le problème de classification des p-groupes, un lemme est bien utile :

Lemme II.4.4. *Soit G un groupe et Z son centre. On suppose G/Z cyclique. Alors G est abélien.*

Démonstration. Soit a dans G tel que la classe de a modulo Z engendre le groupe cyclique G/Z. Alors, tout élément de G s'écrit sous la forme $a^k z$. Ceci implique directement que deux éléments de G commutent puisque $a^k z a^{k'} z = a^{k+k'} z z'$.

En particulier, on peut en déduire sans effort

Proposition II.4.5. *Tout groupe d'ordre p^2 est abélien. Il est donc isomorphe soit à $(\mathbb{Z}/p\mathbb{Z})^2$, soit à $\mathbb{Z}/p^2\mathbb{Z}$.*

Beaucoup plus astucieux :

Proposition II.4.6. *Tout groupe d'ordre p^3, p impair, est soit abélien, soit isomorphe à un produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$, ou $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. Chaque produit semi-direct est unique à isomorphisme près.*

Démonstration. Soit G un groupe d'ordre p^3. Il possède un centre non trivial et donc un sous-groupe non trivial H isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et distingué puisque central. Le quotient G/H est un groupe d'ordre p^2 donc abélien.

1. On suppose $G/H = \mathbb{Z}/p^2\mathbb{Z}$. Alors G est abélien par le lemme II.4.4.
2. On suppose $G/H = (\mathbb{Z}/p\mathbb{Z})^2$. Alors, comme G/H est abélien, on a $bcb^{-1}c^{-1} \in H$, $b, c \in G$ (prendre les projections sur G/H).

   Montrons que $g \mapsto g^p$ est un morphisme de groupe dont l'image est incluse dans H.

   Effectivement, $(gk)\cdots(gk) = g^p k^p h^{p(p-1)/2}$, où h est le commutateur de k et g (remarquer que h est central et que $kg = gkh$, puis faire un redressement par récurrence). Comme h est dans H, on a $h^p = e$ et comme p impair, on a $(gk)^p = g^p k^p$. De plus, on voit que $g^p \in H$ en prenant les projections sur G/H.

   Maintenant, on va décrire le noyau de ce morphisme. Par un argument de cardinalité, le noyau est d'ordre p^2 ou p^3.

(a) S'il est d'ordre p^3, cela signifie que tout élément a pour ordre p.
Un élément central h de H non trivial et un autre élément k non trivial (donc d'ordre p) engendrent un sous-groupe H' isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ dans G. Comme pour tout g de G, $ghg^{-1} = h$ et $gkg^{-1} \in kH$ (puisque $gkg^{-1}k^{-1} \in H$), le sous groupe H' est distingué. En prenant un élément k' non trivial, donc d'ordre p, hors de H', on engendre un sous-groupe $K' := \langle k' \rangle$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On vérifie que G est un produit semi-direct $H' \rtimes K'$. On obtient donc $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.
Ainsi, G est soit le produit direct $(\mathbb{Z}/p\mathbb{Z})^3$, soit $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$. On montrera plus tard, avec les groupes de Sylow, voir exercice II.5.11, qu'il n'y a qu'un seul produit semi-direct à isomorphisme près.

(b) S'il est d'ordre p^2.
On a donc dans le noyau un élément central h de H non trivial et un autre élément k non trivial (donc d'ordre p). Et de plus, il existe un élément c d'ordre plus grand que p, donc p^2 (le cas p^3 donne un groupe cyclique). Et c vérifie $c^p = h^l$, avec l non multiple de p, puisque c^p est dans H et non trivial. Résultat des courses, G est engendré par h, k, c tels que , $h^p = e$, $k^p = e$, $c^p = h^l$, $kc = ckh$ (G est non abélien et donc on peut toujours prendre $kck^{-1}c^{-1} = h$). Le groupe engendré par c (et donc qui contient h) est distingué puisque d'indice minimum premier. En choisissant pour H le sous-groupe engendré par c et K le sous-groupe engendré par k, on voit facilement que $G = \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.
Comme dans l'exemple précédent, on montre qu'il n'y a qu'un seul produit semi-direct à isomorphisme près.

Exercice II.4.7. Montrer que le groupe des matrices triangulaires supérieures de $\mathrm{GL}_3(\mathbb{F}_p)$ avec des 1 sur la diagonale est un groupe d'ordre p^3. A quel groupe de la classification correspond-il ?
Ind. : Quel est l'ordre de ses éléments ? La décomposition de Dunford est ton amie.

Le cas pair donne le premier exemple de groupe qui n'est pas produit semi-direct de groupes simples. Son petit nom : H_8, le groupe des quaternions. Il est défini par deux générateurs i et j et les relations $i^4 = 1$, $j^2 = i^2$, $ij = i^3j$.

Proposition II.4.8. *Un groupe d'ordre 8 non abélien est soit isomorphe à un PSD $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$, soit à H_8.*

Démonstration. Supposons qu'il existe un élément a d'ordre 4. Il engendre un sous-groupe cyclique H et distingué, puisque d'indice 2. Dans ce cas, deux sous-cas :

s'il existe un élément d'ordre 2 à l'extérieur de H, on a un produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

s'il n'y a pas d'élément d'ordre 2 à l'extérieur de H. Soit b un élément à l'extérieur. b^2 n'est pas e, ni a, ni a^3 (sinon b serait d'ordre 8), donc $b^2 = a^2$. On vérifie que seul $bab^{-1} = a^3$ est valable (bab^{-1} n'est pas a sinon le groupe serait abélien, ni a^2 ni e car il doit être de même ordre que a). C'est le groupe des quaternions.

Enfin, reste le cas où tous les éléments sont d'ordre 2, on tombe facilement sur le PSD $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Exercice II.4.9. Montrer que le groupe des matrices triangulaires supérieures de $\mathrm{GL}_3(\mathbb{F}_2)$ avec des 1 sur la diagonale est un groupe d'ordre 8. A quel groupe de la classification correspond-il ?
Ind. : Quel est l'ordre de ses éléments ? La décomposition de Dunford est toujours ton amie.

On réalise facilement H_8 dans le groupe SU_2

$$SU_2 = \{M \in \mathcal{M}_2(\mathbb{C}),\, M^*M = \mathrm{I}_2,\, \det M = 1\} = \{\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix},\, a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1\}$$

comme son intersection avec $\mathcal{M}_2(\mathbb{Z}[i])$, qui est bien un groupe. Si on pose $a = x + iy$, $b = z + it$, avec (x, y, z, t) dans $\mathbb{R}^4$, on obtient, 1 : $(1, 0, 0, 0)$, -1 : $(-1, 0, 0, 0)$, i : $(0, 1, 0, 0)$, -i : $(0, -1, 0, 0)$, 1 : $(1, 0, 0, 0)$, j : $(0, 0, 1, 0)$, -j : $(0, 0, -1, 0)$, k : $(0, 0, 0, -1)$, -k : $(0, 0, 0, 1)$

$$H_8 = \{1, -1, i, -i, j, -j, k, -k\}, \text{ avec les relations } i^2 = j^2 = k^2 = -1,\ ij = -ji = k.$$

II.5 Théorèmes de Sylow

On rappelle ici les théorèmes de Sylow et on commence à attaquer des exemples standard.

Proposition II.5.1 (Théorème de Cauchy)**.** *Soit G un groupe d'ordre n et p un nombre premier qui divise n. Alors, il existe un élément dans G d'ordre p.*

Théorème II.5.2 (Premier théorème de Sylow)**.** *Soit G un groupe d'ordre $p^\alpha m$ où p est premier et ne divise pas m. Alors il existe un sous-groupe de G d'ordre p^α.*

On appelle ces sous-groupes p-sous-groupes de Sylow, ou simplement p-Sylow.

Remarque II.5.3. Avec en renfort les résultats sur les p-groupes, on a l'existence d'un sous-groupe d'ordre p^β dans G pour tout $\beta \leq \alpha$.

Théorème II.5.4 (Deuxième théorème de Sylow)**.**

1. *Tout p-sous-groupe est inclus dans un p-Sylow,*
2. *les p-Sylow sont conjugués.*

On peut affiner le résultat de conjugaison.

Proposition II.5.5. *Soit G un groupe, S un p-Sylow de G et H un sous-groupe de G. Alors, il existe g dans G tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.*

Théorème II.5.6 (Troisième théorème de Sylow)**.** *Soit G un groupe d'ordre $p^\alpha m$ où p est premier et ne divise pas m. Soit n_p le nombre de p-Sylow.*

1. *$n_p | m$,*
2. *n_p est congru à 1 modulo p.*

Remarque II.5.7. Les théorèmes de Sylow permettent souvent de réaliser le groupe G comme produit semi-direct.

Si on montre que pour un p, $n_p = 1$, alors le deuxième théorème de Sylow assure que cet unique Sylow est distingué.

Reste à trouver une section. Mais, par exemple, si $n = p^\alpha q^\beta$, avec p, q premiers et $n_p = 1$. Alors, *un* q-Sylow S_q et *le* p-Sylow S_p fournissent tout ce qu'il faut pour obtenir un PSD $S_p \rtimes S_q$.

Exercice II.5.8. Montrer qu'un groupe non abélien d'ordre pq (p et q premiers), avec $p > q$, est un PSD $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$. Etudier ces PSD.

Exercice II.5.9. Classifiez tous les groupes d'ordre 2 à 15.

Exercice II.5.10. Soit G un groupe d'ordre pqr, avec $p > q > r$ trois nombres premiers. On suppose $n_p = 1$. Montrer qu'il existe un sous-groupe distingué d'ordre pq, puis que G est PSD (au sens large) $(\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}) \rtimes \mathbb{Z}/r\mathbb{Z}$.
Pour la première question utiliser le p-Sylow S_p distingué, un q-Sylow S_q. On montre d'une part que S_pS_q est un sous-groupe, puis qu'il est distingué car d'indice premier minimal.

Exercice II.5.11. Montrer que $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$. Quels sont (à iso près) les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$? En déduire que tous les morphismes de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{GL}_2(\mathbb{F}_p)$ sont reliés par un diagramme comme dans le lemme II.4.4. En déduire l'unicité d'un PSD (non direct) $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

Exercice II.5.12.

1. Remarquer que H_8 est le seul groupe d'ordre 8 à n'avoir qu'un seul élément d'ordre 2. En déduire qu'un 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ est isomorphe à H_8.
   Quelles sont les valeurs propres d'une matrice d'ordre 2 de $\mathrm{SL}_2(\mathbb{F}_3)$ *?*
2. Montrer que $\mathrm{PSL}_2(\mathbb{F}_3)$ est isomorphe à $\mathcal{A}_4$.
   Faire agir $\mathrm{SL}_2(\mathbb{F}_3)$ *sur les 4 droites de l'espace* $\mathbb{F}_3^2$.
3. Soit π l'application canonique de $\mathrm{SL}_2(\mathbb{F}_3)$ sur $\mathrm{PSL}_2(\mathbb{F}_3)$. Montrer que l'image d'un 2-Sylow par π est un 2-Sylow de $\mathrm{PSL}_2(\mathbb{F}_3)$. En déduire qu'un 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ est distingué.
   C'est l'image réciproque du groupe de Klein qui est distingué dans $\mathcal{A}_4$.
4. Montrer $\mathrm{SL}_2(\mathbb{F}_3) \simeq H_8 \rtimes \mathbb{Z}/3\mathbb{Z}$.

Exercice II.5.13. On se propose de montrer que tout groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$. Soit donc G un groupe simple d'ordre 60.

1. Montrer que $n_5 = 6$. (Par élimination)
2. En déduire que G agit par conjugaison sur l'ensemble de ses 5-Sylow et que cette action est fidèle.
3. Montrer que cette action fournit un morphisme injectif de G sur $\mathcal{A}_6$.
   Ind. : On utilise le fait que $D(G) = G$.
4. En déduire que G est isomorphe à un sous-groupe d'indice 6 de $\mathcal{A}_6$. On appelle encore G ce groupe.
5. On considère l'action de G à gauche sur $\mathcal{A}_6/G$. Montrer qu'il stabilise la classe du neutre et qu'il définit un morphisme injectif de G vers $\mathcal{S}_5$.
   Ind. : Toute la difficulté, c'est de montrer que ce morphisme est injectif, c'est-à-dire ici non trivial. Mais s'il était trivial, on aurait G *distingué dans* $\mathcal{A}_6$.
6. Conclure.