Quelques compléments sur les groupes

D. Harari

Agrégation 2015

1. Produit semi-direct

Commençons par rappeler quelques notions. Si H et N sont deux groupes, on dit qu'un groupe G est une *extension de*[1] H *par* N s'il existe une suite exacte courte

$$1 \to N \to G \to H \to 1.$$

L'ensemble $\mathtt{Aut}\, N$ des automorphismes de groupe de N est lui-même un groupe pour la loi $\circ$. Par exemple si n est un entier ≥ 2, le groupe des automorphismes du groupe additif $\mathbf{Z}/n\mathbf{Z}$ est isomorphe au groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Si p est un nombre premier, le groupe des automorphismes du groupe abélien $(\mathbf{Z}/p\mathbf{Z})^r$ est le groupe mutliplicatif $\mathrm{GL}_r(\mathbf{Z}/p\mathbf{Z})$.

Soient N et H deux groupes. Le *produit direct* $N \times H$ de N et H est le groupe dont l'ensemble sous-jacent est l'ensemble produit $N \times H$, avec la loi $(n.h).(n', h') = (nn', hh')$ pour tous $n, n' \in N$ et $h, h' \in H$.

Le produit semi-direct est une généralisation de cette notion. Soit $\varphi : H \to \mathtt{Aut}\, N$ un morphisme de groupes, qui définit en particulier une action $h.n := \varphi(h)(n)$ de N sur G (mais on demande en plus ici que l'image de φ soit incluse dans $\mathtt{Aut}\, N$, et pas seulement dans $\mathcal{S}(N)$).

Proposition 1.1 *On définit une loi de groupes sur l'ensemble produit $N \times H$ en posant*

$$(n, h).(n', h') := (n(h.n'), hh')$$

Ce groupe s'appelle le produit semi-direct de N par H relativement à l'action φ ; on le note $N \rtimes_\varphi H$ (ou simplement $N \rtimes H$ si l'action φ est sous-entendue).

1. Certains auteurs, par exemple D. Perrin, disent plutôt extension de N par H.

Démonstration : Clairement $(1,1)$ est élément neutre pour la loi définie (on utilise déjà ici que $h.1 = 1$, qui vient du fait que l'action est à valeurs dans $\mathtt{Aut}\, N$). D'autre part (n,h) a pour inverse $(h^{-1}.n^{-1}, h^{-1})$ (ici on utilise $h^{-1}.(nn^{-1}) = (h^{-1}.n)(h^{-1}.n^{-1})$). Il reste à vérifier l'associativité.

On a

$$[(n_1,h_1)(n_2,h_2)](n_3,h_3) = (n_1(h_1.n_2),h_1h_2)(n_3,h_3) = (n_1(h_1.n_2)[(h_1h_2).n_3], h_1h_2h_3)$$

et

$$(n_1,h_1)[(n_2,h_2)](n_3,h_3)] = (n_1,h_1)(n_2(h_2.n_3),h_2h_3) = (n_1[h_1.(n_2(h_2.n_3))], h_1h_2h_3)$$

Or $(h_1.n_2)[(h_1h_2).n_3] = [h_1.(n_2(h_2.n_3))]$ d'après les axiomes des actions de groupe et le fait que $n \mapsto h_1.n$ soit un automorphisme de N. D'où le résultat.

□

Remarque 1.2 a) Parler "du" produit semi-direct de N par H n'a de sens que si on précise l'action, il peut exister plusieurs actions de H sur N, donc plusieurs produits semi-directs. On fera aussi attention au fait que H et N ne jouent pas des rôles symétriques.

b) L'action triviale correspond au produit direct.

Proposition 1.3 *Avec les notations ci-dessus, soit $G = N \rtimes H$. Alors :*

1. *On a une suite exacte*

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

avec $i(n) = (n,1)$ et $p(n,h) = h$. En particulier N s'identifie à un sous-groupe distingué (noté encore N)[2] dans G. Ainsi un produit semi-direct de N par H est une extension de H par N.

2. *La suite exacte est scindée, i.e. il existe un morphisme $s : H \to G$ ("section") vérifiant $p \circ s = \mathrm{Id}_H$. Ainsi H s'identifie à un sous-groupe (encore noté H) de G.*

3. *Dans G, on a $N \cap H = \{1\}$ et $NH = G$, où NH est par définition l'ensemble des nh avec $n \in N$ et $h \in H$. De plus l'opération de H sur N est décrite par $h.n = hnh^{-1}$, le produit de droite étant effectué dans G.*

2. N comme "normal" ; le symbole $\rtimes$ ressemble à $\lhd$ et permet de se rappeler le "sens" dans lequel on effectue le produit semi-direct.

Démonstration : 1. On a que i et n sont des morphismes via $(n,1)(n',1) = (n(1.n'),1) = (nn',1)$ et $(n,h)(n',h') = (n(h.n'),hh')$. Le fait que la suite soit exacte est immédiat.

2. Il suffit de poser $s(h) = (1,h)$.

3. D'après 1., $N \cap H$ est l'ensemble des (n,h) avec $n = h = 1$, donc il est réduit au neutre de G. si $g = (n,h)$ est un élément de G, on a $g = (n,1).(1,h)$, donc $G = NH$. Enfin on a dans G : $hnh^{-1} = (1,h)(n,1)(1,h^{-1}) = (h.n,h)(1,h^{-1}) = (h.n,1) = h.n$.

□

Remarque 1.4 Via la proposition précédente, on peut désormais écrire les éléments de $N \rtimes H$ de manière unique sous la forme nh ($n \in N, h \in H$) avec la règle de commutation $hn = (h.n)h$. Notons aussi que $N \rtimes H$ est abélien si et seulement si l'opération est triviale, avec N et H tous deux abéliens.

On a une sorte de réciproque de la proposition précédente pour savoir quand un groupe se décompose en produit semi-direct.

Proposition 1.5 *1. (Caractérisation "interne") Soit G un groupe contenant deux sous-groupes N et H avec*

i) $N \lhd G$.

ii) $N \cap H = \{1\}$.

iii) $G = NH$.

Alors $G \simeq N \rtimes H$ pour l'opération $h.n = hnh^{-1}$.

2. (Caractérisation "externe") Soit

$$1 \to N \to G \to H \to 1$$

une suite exacte admettant une section $s : H \to G$. Alors $G \simeq N \rtimes H$ pour l'opération $h.n = s(h)ns(h)^{-1}$.

Démonstration : 1. Soit φ l'opération de H sur N définie par $\varphi(h)(n) = hnh^{-1}$. Alors l'application $\Phi : N \rtimes_\varphi H \to G$ qui associe à (n,h) le produit nh (dans G) est un morphisme car $\Phi((n,h)(n',h')) = \Phi(n(hn'h^{-1}),hh') = nhn'h'$. L'injectivité de Φ résulte de ii) et sa surjectivité de iii).

2. Posons $H_1 = s(H)$. Comme s est injective vu que $p \circ s = \mathrm{id}_H$, H_1 est un sous-groupe de G isomorphe à H et via 1., il suffit de montrer : $N \cap H_1 = \{1\}$ et $NH_1 = G$ (on a identifié N à son image dans G). Si $h_1 \in N \cap H_1$, alors $p(h_1) = 1$ mais $h_1 = s(h)$ avec $h \in H$, d'où $1 = p(s(h)) = h$ et $h_1 = 1$. Si maintenant $g \in G$, alors g et $s(p(g))$ ont même image par p, donc ils diffèrent d'un élément du noyau N, i.e. $g = nh_1$ avec $h_1 := s(p(g))$, et $g \in NH_1$.

□

C'est en général le deuxième critère qui est le plus utile pour obtenir des décompositions en produit semi-direct, mais on gardera bien à l'esprit la façon de déterminer l'opération de H sur N associée en fonction de la suite exacte et de la section.

Exercice 1.6 a) Soit $G = N \rtimes H$, alors l'opération de H sur N est triviale (i.e. le produit est direct) si et seulement si le sous-groupe H de G est distingué.

b) Soient N et H deux groupes, φ et ψ deux morphismes $H \to \mathtt{Aut}\, N$. S'il existe $u \in \mathtt{Aut}\, N$ tel que $\psi(h) = u \circ \varphi(h) \circ u^{-1}$ ("actions conjuguées"), alors $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.

c) Soient N et H deux groupes, φ et ψ deux morphismes $H \to \mathtt{Aut}\, N$. S'il existe $\alpha \in \mathtt{Aut}\, H$ tel que $\varphi = \psi \circ \alpha$, alors $N \rtimes_\varphi H \simeq N \rtimes_\psi H$ (envoyer $nh \in N \rtimes_\varphi H$ sur $n\alpha(h) \in N \rtimes_\psi H$).

Exemple 1.7

1. Pour $n \geq 2$, la suite exacte
$$1 \to \mathcal{A}_n \to \mathcal{S}_n \xrightarrow{\varepsilon} \mathbf{Z}/2\mathbf{Z} \to 1$$
est scindée via la section s qui envoie $\bar{0}$ sur Id et $\bar{1}$ sur une transposition (arbitraire) τ. On en déduit une décomposition $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.
2. Soient K un corps et $n \in \mathbf{N}^*$. La suite exacte
$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^* \to 1$$
est scindée (envoyer $\lambda \in K^*$ sur la matrice $\mathrm{Diag}(\lambda, 1, ..., 1)$). Ainsi $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$.
3. Le groupe $\mathbf{Z}/4\mathbf{Z}$ n'est *pas* produit semi-direct de $\mathbf{Z}/2\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$. En effet le seul automorphisme de $\mathbf{Z}/2\mathbf{Z}$ est l'identité, donc l'action serait triviale ; or $\mathbf{Z}/4\mathbf{Z}$ n'est pas isomorphe au produit direct $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (le premier groupe a des éléments d'ordre 4 et pas le deuxième). En particulier la suite exacte
$$0 \to \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$$
(obtenue en envoyant x (mod. 4) sur x (mod.2), le noyau est $\{\bar{0}, \bar{2}\}$ qui est isomorphe à $\mathbf{Z}/2\mathbf{Z}$) n'est pas scindée. [3]

3. On voit donc que même dans des cas très élémentaires, on ne peut pas toujours "reconstituer" un groupe à partir de ses sous-groupes. En particulier, la connaissance des groupes finis simples ne suffit absolument pas à connaître tous les groupes finis, contrairement à une croyance populaire assez répandue (notamment chez les agrégatifs !).

4. Soit $n \geq 3$, on note D_n le *groupe diédral* des isométries du plan conservant un polygone régulier convexe à n côtés. Il contient les n rotations de centre O (le centre du polygone) et d'angle $2k\pi/n$ ($0 \leq k \leq n-1$) et les n réflexions par rapport aux droites passant par O et les sommets (si n est impair) ou les milieux des côtés (si n est pair). On a une suite exacte
$$1 \to \mathbf{Z}/n\mathbf{Z} \to D_n \to \mathbf{Z}/2\mathbf{Z} \to 1$$
obtenue en prenant le déterminant d'une isométrie, qui est à valeurs dans $\{\pm 1\}$. Elle est scindée (on envoie l'élément non trivial ε de $\mathbf{Z}/2\mathbf{Z}$ sur une réflexion), d'où une décomposition $D_n \simeq \mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$. Notons que l'action correspondante de $\mathbf{Z}/2\mathbf{Z}$ sur $\mathbf{Z}/n\mathbf{Z}$ consiste à poser $\varepsilon.x = -x$ pour $x \in \mathbf{Z}/n\mathbf{Z}$.
5. Si p et q sont des nombres premiers avec $p < q$, les groupes d'ordre pq sont tous cycliques si p ne divise pas $q-1$ (c'est une application classique des théorèmes de Sylow, cf. [3]). Si par contre p divise $q-1$, on a de plus un produit semi-direct non commutatif $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$, via le fait qu'il y a des morphismes non triviaux $\mathbf{Z}/p\mathbf{Z} \to \mathtt{Aut}\,(\mathbf{Z}/q\mathbf{Z}) \simeq \mathbf{Z}/(q-1)\mathbf{Z}$.
6. Si p est un nombre premier impair, il y a deux groupes non commutatifs d'ordre p^3, qui sont des produits semi-directs de groupes plus petits. Le cas $p = 2$ est exceptionnel : le groupe diédral est le seul produit semi-direct non trivial d'ordre 8, et on a de plus le groupe des quaternions, qui ne se décompose pas en produit semi-direct de groupes plus petits ([3]).

2. Groupes résolubles et nilpotents

On se contentera ici des définitions et des premières propriétés. On pourra se reporter aux chapitres 9 et 10 du livre de Hall [2] pour plus de détails.

Définition 2.1 Soit G un groupe.[4] On dit que G est *résoluble* s'il existe une suite finie
$$\{1\} = G_0 \subset G_1 \subset ... \subset G_n = G$$
avec pour tout $i \in [1, n]$, $G_{i-1} \lhd G_i$ et G_i/G_{i-1} abélien.

Remarque 2.2 a) Comme la proposition 2.5 le montrera, on peut demander en plus que chaque G_i soit distingué dans G tout entier. Alors G résoluble

4. La notion est surtout intéressante pour les groupes finis, mais ce n'est pas indispensable de le supposer.

signifie que G se déduit de $\{1\}$ par une suite finie d'*extensions à noyaux abéliens* (en effet chaque G/G_{i-1} est extension de G/G_i par G_i/G_{i-1}).

b) Si G est fini et qu'on n'impose pas $G_i \lhd G$, on peut demander G_i/G_{i-1} cyclique d'ordre premier au lieu d'abélien (car tout groupe abélien fini H admet une suite $H \supset ... \supset \{1\}$ avec tous les H_i/H_{i-1} simple, par récurrence sur $\#H$; or les groupes simples abéliens sont les $\mathbf{Z}/p\mathbf{Z}$ avec p premier). Par contre demander G_i/G_{i-1} cyclique et $G_i \lhd G$ pour tout i est plus fort (on parle de groupe *hyper-résoluble*).

c) Le terme résoluble vient de la théorie des équations algébriques. Si P est un polynôme irréductible à coefficients dans $\mathbf{Q}$, et $K \subset \mathbf{C}$ son *corps de décomposition* (c'est le plus petit corps contenant toutes ses racines), on définit le *groupe de Galois* G de P comme le groupe des automorphismes du corps K. La théorie de Galois dit qu'une équation est résoluble par radicaux si et seulement si G est résoluble.[5] Le fait que $\mathcal{S}_n$ ne soit pas résoluble pour $n \geq 5$ entraîne l'impossiblité de résoudre par radicaux l'équation générale de degré 5.

Une notion plus forte que résoluble (et même qu'hyper-résoluble pour les groupes finis) est celle de groupe nilpotent :

Définition 2.3 On dit qu'un groupe G est *nilpotent* s'il existe une suite finie

$$\{1\} = G_0 \subset G_1 \subset ... \subset G_n = G$$

avec pour tout $i \in [1, n]$, $G_i \lhd G$ et G_i/G_{i-1} inclus dans le centre de G/G_{i-1}.

Cela signifie donc que G se déduit de $\{1\}$ par une suite finie d'*extensions centrales* (une extension $1 \to N \to G \to H \to 1$ est dite centrale si N est inclus dans le centre de G).

Exemple 2.4

1. Un groupe abélien est nilpotent.
2. Un p-groupe est nilpotent : c'est immédiat par récurrence sur son cardinal, vu que son centre est non trivial, et le quotient par son centre est encore un p-groupe.
3. $\mathcal{S}_n$ et $\mathcal{A}_n$ ne sont pas résolubles pour $n \geq 5$. Cela résulte de ce que $D(\mathcal{S}_n) = D(\mathcal{A}_n) = \mathcal{A}_n$, et de la proposition ci-dessous.

5. Sans rentrer dans les détails, rajouter une racine n-ième à un corps qui contient les racines n-ièmes de l'unité donne un groupe de Galois cyclique, et ajouter les racines n-ièmes de l'unité à $\mathbf{Q}$ donne un groupe de Galois abélien. Ainsi obtenir K en extrayant des racines correspond à une suite d'extensions de groupe de Galois abélien.

4. $\mathcal{S}_4$ est résoluble, via la suite

$$\mathcal{S}_4 \supset \mathcal{A}_4 \supset V_4 \supset \{1\}$$

où V_4 est le sous-groupe constitué de l'identité et des doubles transpositions, mais il ne peut pas être nilpotent car son centre est trivial. Les mêmes conclusions valent pour $\mathcal{A}_4$ et $\mathcal{S}_3$

La proposition suivante donne la caractérisation la plus canonique d'un groupe résoluble. En particulier, c'est la plus commode pour montrer qu'un groupe n'est *pas* résoluble.

Proposition 2.5 *Soit G un groupe, on pose $D^0(G) = G$, $D^1(G) = D(G)$, et $D^i(G) = D(D^{i-1}(G))$ pour tout $i \geq 2$. Alors G est résoluble si et seulement s'il existe un entier n tel que $D^n(G) = \{1\}$.*

Démonstration : S'il existe un entier n tel que $D^n(G) = \{1\}$, alors chaque $D^i(G)/D^{i-1}(G)$ est un groupe abélien par définition du sous-groupe dérivé donc G est résoluble via la suite des $D^i(G)$. Notons que chaque $D^i(G)$ est distingué dans G tout entier parce que le sous-groupe dérivé d'un groupe H est caractéristique dans H, et cette propriété est transitive.

En sens inverse si G est résoluble, soit $(G_i)_{1\leq i\leq n}$ une suite comme dans la définition 2.1. Alors G/G_{n-1} est abélien donc $G_{n-1} \supset D(G)$. Par récurrence sur i, on a $G_{n-i} \supset D^i(G)$ (si $G_{n-i+1} \supset D^{i-1}(G)$, alors comme G_{n-i+1}/G_{n-i} est abélien, on a $G_{n-i} \supset D(G_{n-i+1}) \supset D(D^{i-1}(G)) = D^i(G)$). Pour $i = n$ cela donne $D^n(G) = \{1\}$.

□

Exercice 2.6 a) Montrer que $\mathcal{S}_3$ est hyper-résoluble mais pas $\mathcal{A}_4$.

b) Un sous-groupe et un quotient d'un groupe résoluble sont résolubles, ainsi qu'une extension d'un groupe résoluble par un groupe résoluble.

3. Les isomorphismes exceptionnels

Rappelons que si K est un corps, on note respectivement $\mathrm{GL}_n(K)$ le groupe multiplicatif des matrices (n, n) inversibles à coefficients dans K, et $\mathrm{SL}_n(K)$ le sous-groupe de $\mathrm{GL}_n(K)$ constitué des matrices de déterminant 1. On note aussi $\mathrm{PGL}_n(K)$ le quotient de $\mathrm{GL}_n(K)$ par son centre (i.e. par le sous-groupe des λI_n, $\lambda \in K^*$), et $\mathrm{PSL}_n(K)$ le quotient de $\mathrm{SL}_n(K)$ par son centre, lequel est constitué des λI_n avec $\lambda \in K^*$ et $\lambda^n = 1$.

On va ici s'intéresser plus particulièrement à $\mathrm{PSL}_2(K)$ quand K est fini. On commence par une proposition donnant le cardinal des groupes $\mathrm{PSL}_n(K)$.

Proposition 3.1 *Soient K un corps fini*[6] *de cardinal q et $n \in \mathbf{N}^*$. Alors :*

$$\#\mathrm{GL}_n(K) = (q^n - 1)(q^n - q)...(q^n - q^{n-1})$$
$$\#\mathrm{SL}_n(K) = \#\mathrm{PGL}_n(K) = (q^n - 1)(q^n - q)...(q^n - q^{n-2})q^{n-1}$$
$$\#\mathrm{PSL}_n(K) = \#\mathrm{SL}_n(K)/d$$

où $d = (n, q-1)$ est le pgcd de n et $q-1$.

Démonstration : Le résultat sur le cardinal de $\mathrm{GL}_n(K)$ est classique, on le montre en comptant les bases de K^n. Le deuxième résultat vient de ce que $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^*$ et $\mathrm{SL}_n(K)$ est le noyau du morphisme surjectif det : $\mathrm{GL}_n(K) \to K^*$. Pour montrer le troisième point, il suffit de vérifier que le cardinal de l'ensemble $\mu_n(K)$ des racines n-ièmes de l'unité de K est d, vu que $\mathrm{PSL}_n(K) = \mathrm{SL}_n(K)/\mu_n(K)$. Déjà on a $\mu_n(K) = \mu_d(K)$ car si $x \in K^*$, on a $x^{q-1} = 1$ vu que le groupe multiplicatif K^* est d'ordre $q-1$, donc l'ordre d'une racine n-ième de l'unité divise n et $q-1$, donc divise d.

Il y a au plus d racines de l'unité dans K car le polynôme $X^d - 1$ a au plus d racines. D'autre part le polynôme $X^{q-1} - 1$ est scindé sur K (il a $q-1$ racines distinctes qui sont les éléments de K^*), donc aussi $X^d - 1$ qui le divise puisque d divise $q-1$ (si $q - 1 = md$, on a $X^{q-1} - 1 = (X^d - 1)(1 + X^d + ... + X^{d(m-1)})$. Finalement il y a bien exactement d racines d-ièmes de l'unité dans K.

□

Theorème 3.2 *Soit $\mathbf{F}_q$ le corps fini à q éléments. On a les isomorphismes (dits exceptionnels) :*

$$\mathrm{GL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) = \mathrm{PGL}_2(\mathbf{F}_2) = \mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathcal{S}_3$$

$$\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathcal{S}_4 \quad \mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathcal{A}_4$$
$$\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4) \simeq \mathcal{A}_5$$
$$\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathcal{S}_5 \quad \mathrm{PSL}_2(\mathbf{F}_5) \simeq \mathcal{A}_5$$

En particulier $\mathrm{PSL}_2(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_3)$ ne sont pas simples, tandis que $\mathrm{PSL}_2(\mathbf{F}_4)$ et $\mathrm{PSL}_2(\mathbf{F}_5)$ le sont.

Remarque 3.3 On a $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$, $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$, $\mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$, mais $\mathbf{F}_4$ n'est ni l'anneau $\mathbf{Z}/4\mathbf{Z}$, ni $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (qui ne sont pas des corps !). Une définition correcte de $\mathbf{F}_4$ est de le voir comme l'anneau quotient de $\mathbf{Z}/2\mathbf{Z}[X]$ par l'idéal engendré par $X^2 + X + 1$ (qui est un polynôme irréductible de $\mathbf{Z}/2\mathbf{Z}[X]$).

6. On note souvent $\mathbf{F}_q$ *le* corps fini de cardinal q, car on sait que si q est une puissance d'un nombre premier p, il existe un et un seul corps fini de cardinal q à isomorphisme près.

Démonstration : Soient K un corps fini, E le K-espace vectoriel K^n. On note $\mathbf{P}(E) = \mathbf{P}_K^{n-1}$ (noter le décalage d'indice) l'ensemble des droites vectorielles de K^n, appelé *espace projectif de dimension* $n-1$. C'est aussi l'ensemble quotient de $K^n - \{0\}$ par la relation d'équivalence $x \sim y$ si et seulement si x et y sont colinéaires. Le groupe $\mathrm{GL}(E)$ opère sur $\mathbf{P}(E)$ via $g.D = g(D)$, et comme le centre opère trivialement on obtient un morphisme $\Phi : \mathrm{PGL}(E) \to \mathcal{S}(\mathbf{P}(E))$ qui est injectif, vu que les seuls $g \in \mathrm{GL}(E)$ qui stabilisent toutes les droites sont les homothéties.

Prenons maintenant $n = 2$ et K de cardinal q, alors comme le cardinal de $\mathbf{P}_K^1$ est $q+1$ (il y a $q+1$ droites dans le plan sur $\mathbf{F}_q$), on obtient un plongement

$$\Phi : \mathrm{PGL}_2(\mathbf{F}_q) \to \mathcal{S}_{q+1}$$

On passe alors en revue tous les cas en calculant les cardinaux avec la proposition 3.1.

a) Si $q = 2$, tous les groupes considérés sont de cardinal 6 car $\mathbf{F}_q^*$ est trivial. En particulier Φ est un isomorphisme de but $\mathcal{S}_3$.

b) Ici $\mathrm{PGL}_2(\mathbf{F}_3)$ est de cardinal 24, donc Φ est un isomorphisme. Comme $\mathrm{PSL}_2(\mathbf{F}_3)$ est de cardinal 12, il est d'indice 2 dans $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathcal{S}_4$, donc isomorphe à $\mathcal{A}_4$.

c) D'après la proposition 3.1, on a $\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4)$ et ces groupes sont de cardinal 60, donc d'indice 2 (via Φ) dans $\mathcal{S}_5$, donc isomorphes à $\mathcal{A}_5$.

d) Le groupe $\mathrm{PGL}_2(\mathbf{F}_5)$ est d'ordre 120, il peut être vu via Φ comme un sous-groupe d'indice 6 de $\mathcal{S}_6$, donc il est isomorphe à $\mathcal{S}_5$ d'après un corollaire (non immédiat !) de la simplicité des groupes alternés (cf. [3]). Comme $\mathrm{PSL}_2(\mathbf{F}_5)$ est de cardinal 60, il est d'indice 2 dans $\mathcal{S}_5$, donc isomorphe à $\mathcal{A}_5$. □

Remarque 3.4 a) On obtient que le groupe $\mathrm{GL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) \simeq \mathcal{S}_3$ n'est pas parfait. Le groupe $\mathrm{SL}_2(\mathbf{F}_3)$ ne l'est pas non plus car $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathcal{A}_4$ a un quotient isomorphe à $\mathbf{Z}/3\mathbf{Z}$ (le quotient par le groupe V_4 constitué de l'identité et des doubles transpositions), donc également $\mathrm{SL}_2(\mathbf{F}_3)$ (en prenant l'image réciproque de V_4 par la surjection canonique). Au passage on voit que $\mathrm{SL}_2(\mathbf{F}_3)$ n'est pas isomorphe à $\mathrm{PGL}_2(\mathbf{F}_3)$, bien que ces deux groupes aient même cardinal (le premier a un quotient d'ordre 3 et pas le second).

b) Le plongement $\Phi : \mathrm{PGL}_2(\mathbf{F}_5) \to \mathcal{S}_6$ donne un sous-groupe d'indice 6 de $\mathcal{S}_6$ qui opère transitivement sur $\{1, ..., 6\}$, donc n'est pas conjugué du stabilisateur d'un point. Cela permet de construire un automorphisme de $\mathcal{S}_6$ qui n'est pas intérieur (ce phénomène ne se produit pour $\mathcal{S}_n$ que quand $n = 6$).

c) Il y a des isomorphismes exceptionnels plus compliqués, par exemple $\mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{PSL}_3(\mathbf{F}_2)$ (l'unique groupe simple d'ordre 168, voir [1]...).

Références

[1] J. Dieudonné : *La géométrie des groupes classiques* (seconde éd.), Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[2] M. Hall Jr : *The theory of groups*, The Macmillan Co., New York, N.Y. 1959.

[3] D. Perrin : *Cours d'algèbre*, Ellipses 1996.