# Chapitre 3

# Groupes symétriques et groupes linéaires

## 3.1 Groupes symétriques

**3.1.1.** Soit $n$ un entier $\geq 1$. Nous noterons $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $X = \{1, \ldots, n\}$. Il est bien connu que $|\mathfrak{S}_n| = n!$ (démonstration : pour définir une bijection $\sigma$ de $X$ vers lui-même, on peut choisir de $n$ façons distinctes l'image $\sigma(1)$ de 1, puis, pour chacun de ces choix de $\sigma(1)$, de $n-1$ façons distinctes l'image $\sigma(2)$ de 2 (la seule contrainte étant $\sigma(2) \neq \sigma(1)$), etc.) Pour tout $p$-uplet $i_0, \ldots, i_{p-1}$ d'éléments disincts de $X$, on note $[i_1, \ldots, i_p]$ l'élément $\sigma$ de $\mathfrak{S}_n$ défini par $\sigma(i_{j-1}) = i_j$ si $1 \leq j < p$, $\sigma(i_{p-1}) = i_0$, et $\sigma(k) = k$ si $k \notin \{i_0, \ldots, i_{p-1}\}$ ; on dit que $[i_0, \ldots, i_{p-1}]$ est le *cycle* défini par les éléments $i_0, \ldots, i_{p-1}$ donnés dans cet ordre. L'ensemble $\{i_0, \ldots, i_{p-1}\}$ est appelé *support* du cycle $[i_0, \ldots, i_{p-1}]$. On pourra noter qu'un cycle de longueur 1 est en fait l'identité ; leur considération n'a d'intérêt que pour des commodités de notation dans certains énoncés.

**3.1.2 Proposition.** — *(a) Deux $p$-uplets $i_0, \ldots, i_{p-1}$ et $j_0, \ldots, j_{p-1}$, où $p > 1$, définissent le même cycle si et seulement si ils se déduisent l'un de l'autre par permutation circulaire.*

*(b) Soit $\tau \in \mathfrak{S}_n$, $\gamma = [i_0, \ldots, i_{p-1}]$ ; alors $\tau\gamma\tau^{-1}$ est le cycle $[\tau(i_0), \ldots, \tau(i_{p-1})]$.*

*(c) Soient $\gamma, \gamma'$ deux cycles de longueurs respectives $p, p'$. Supposons que $\mathrm{supp}\,\gamma \cap \mathrm{supp}\,\gamma'$ soit réduit à un élément. Alors $\gamma\gamma'$ est un cycle de longueur $p + p' - 1$.*

*Démonstration.* — *(a)* et *(b)* : laissés au lecteur.

*(c)* Soient $\gamma = [i_0, \ldots, i_{p-1}]$, $\gamma' = [j_0, \ldots, j_{p'-1}]$. Quitte à faire des permutations circulaires, on peut supposer que $i_{p-1} = j_0$. Montrons alors que

$$\gamma\gamma' = [i_0, \ldots, i_{p-1} = j_0, j_1, \ldots, j_{p'-1}]$$

Il est clair que $\gamma\gamma'(x) = x$ si $x \notin \{i_0, \ldots, i_{p-1}, j_1, \ldots, j_{p'-1}\}$. De plus, $\gamma'(i_k) = i_k$ si $k < p-1$, donc $\gamma\gamma'(i_k) = \gamma(i_k) = i_{k+1}$ si $0 \leq k < p-1$. On a $\gamma(\gamma'(j_k)) = \gamma'(j_k)$ si

$0 \leq k < p' - 1$, d'où encore $\gamma\gamma'(j_k) = j_{k+1}$ (ceci couvre aussi le cas de $i_{p-1} = j_0$). Enfin, $\gamma\gamma'(j_{p'-1}) = \gamma(j_0) = \gamma(i_{p-1}) = i_0$.

**3.1.3 Proposition.** — *Soit $\sigma \in \mathfrak{S}_n$. Alors il existe des cycles $\gamma_1, \ldots, \gamma_s$ uniques dans $\mathfrak{S}_n$ tels que les supports des $\gamma_j$ forment une partition de $X$, et $\sigma = \gamma_1 \ldots \gamma_s$. On dit que les $\gamma_j$ sont les cycles de la permutation $\sigma$, et que l'écriture $\sigma = \gamma_1 \ldots \gamma_s$ est la décomposition de $\sigma$ en cycles (on remarquera que les $\gamma_j$ commutent entre eux).*

*Démonstration.* — Soit $H = \langle\sigma\rangle$ le sous-groupe de $G$ engendré par $\sigma$, et soient $C_1, \ldots, C_s$ les orbites de $H$ dans $X$ ; les $C_j$ forment donc une partition de $X$ en parties non-vides, stables par $\sigma$. Soit $d_j > 0$ le cardinal de $C_j$, et choisissons pour tout $j$ un élément $x_j \in C_j$. Alors les éléments $\sigma^k(x_j)$, $0 \leq k < d_j$, sont tous distincts. En effet, soit $l$ le plus grand entier $> 0$ tel que $\sigma^l(x_j) \in \{x_j, \ldots, \sigma^{l-1}(x_j)\}$ ; on a clairement $l \leq d_j$. Par définition, on doit alors avoir

$$\sigma(\sigma^{l-1}(x_j)) = \sigma^l(x_j) \in \{x_j, \ldots, s^{l-1}(x_j)\}$$

ce qui prouve que $\{x_j \ldots, \sigma^{l-1}(x_j)\}$ est $\sigma$-stable, donc $H$-stable ; mais comme l'action de $H$ sur $C_j$ est transitive, ceci n'est possible que si $l = d_j$, $\{x_j, \ldots, \sigma^{l-1}(x_j)\} = C_j$. On voit ainsi que la restriction de $\sigma$ à $C_j$ est le cycle $\gamma_j = [x_j, \sigma(x_j), \ldots, \sigma^{d_j-1}(x_j)]$, et on en déduit aussitôt, en restreignant les deux membres aux divers $C_j$, que $\sigma = \gamma_1 \ldots \gamma_s$. Par ailleurs, il est clair que deux cycles à supports disjoints commutent.

Pour l'unicité, considérons une deuxième décomposition $\sigma = \gamma'_1 \ldots \gamma'_t$, où les supports des $\gamma'_i$ forment une partition de $X$ ; en particulier, comme on vient de le voir, les $\gamma'_i$ commutent. Notons $C'_i$ le support de $\gamma'_i$. Alors $\sigma|_{C'_i} = \gamma'_i$, donc chaque $C'_i$ est stable sous $H$, et est donc une réunion de $H$-orbites ; mais clairement l'action de $H$ sur $C'_i$ est transitive (puisque c'est le cas pour le sous-groupe engendré par $\gamma'_i$), donc $C'_i$ *est* une $H$-orbite, et il existe un unique $j$ tel que $C'_i = C_j$. Comme toute $H$-orbite figure dans un $C'_i$, on voit qu'en fait $s = t$, et que quitte à renuméroter les $C'_i$ on peut supposer que $C'_j = C_j$ pour $1 \leq j \leq s$. Mais alors la restriction de $\sigma$ à $C_j$ est donnée à la fois par $\gamma_j$ et par $\gamma'_j$, ce qui prouve bien que $\gamma_j = \gamma'_j$ pour $1 \leq j \leq s$.

**3.1.4 Remarque.** — On peut bien sûr dans l'écriture $\sigma = \gamma_1 \ldots \gamma_s$ omettre ceux des $\gamma_j$ qui sont égaux à l'identité, *i.e.* ceux dont le support est réduit à un singleton. C'est ce que l'on fait en général en pratique. Dans ce cas on a une écriture de $\sigma$ comme produit de cycles non-triviaux de supports deux à deux disjoints.

**3.1.5 Proposition.** — *(classes de conjugaison dans $\mathfrak{S}_n$) Pour tout $\sigma \in \mathfrak{S}_n$, et $1 \leq j \leq n$, soit $a_j(\sigma)$ le nombre de cycles de longueur $n$ de $\sigma$ ; on a donc $n = \sum_{j=1}^{n} j a_j(\sigma)$. Alors $\sigma$ est conjugué à $\sigma'$ si et seulement si $a_j(\sigma) = a_j(\sigma')$ pour tout $1 \leq j \leq n$.*

*Démonstration.* — Soient $H$ et $H'$ les sous-groupes de $\mathfrak{S}_n$ engendrés par $\sigma$ et $\sigma'$ respectivement. Si $\tau \in \mathfrak{S}_n$ est tel que $\tau\sigma\tau^{-1} = \sigma'$, il est clair que $\tau H \tau^{-1} = H'$, et si $C = Hx$ est une $H$-orbite (*i.e.* un cycle de $\sigma$), $C' = \tau(C) = H'\tau(x)$ est un cycle de $\sigma'$. Donc $\tau$ définit une bijection de l'ensemble des cycles de $\sigma$ sur l'ensemble des cycles de $\sigma'$, qui respecte évidemment les longueurs, ce qui prouve que $a_j(\sigma) = a_j(\sigma')$ pour $1 \leq j \leq n$.

Réciproquement, supposons que $a_j(\sigma) = a_j(\sigma')$ pour $1 \leq j \leq n$. Rangeons les cycles $C_1, \ldots, C_s$ de $\sigma$ par ordre de longueurs décroissantes, et faisons de même pour les cycles $C'_1, \ldots, C'_s$ de $\sigma'$ (remarquons que l'hypothèse dit que $\sigma$ et $\sigma'$ ont même nombre de cycles en chaque longueur, donc aussi même nombre total de cycles). Alors on a $|C_j| = |C'_j|$ pour $1 \leq j \leq s$. Choisissons un élément $x_j$ dans chaque $C_j$, et de même un $x'_j$ dans chaque $C'_j$, et soit $d_j = |C_j| = |C'_j|$. Comme nous l'avons vu dans la démonstration de la prop. 3.1.3, on a alors $C_j = \{\sigma^i(x_j)\}_{0 \leq i < d_j}$, et $C'_j = \{\sigma'^i(x'_j)\}_{0 \leq i < d_j}$. Définissons maintenant une permutation $\tau$ de $X$ en posant $\tau(\sigma^i(x_j)) = \sigma'^i(x'_j)$. On a alors clairement $\tau\sigma(x) = \sigma'\tau(x)$ pour tout $x \in X$, donc $\tau\sigma\tau^{-1} = \sigma'$.

**3.1.6 Corollaire.** — *Le nombre de classes de conjugaison du groupe $\mathfrak{S}_n$ est égal au nombre $\pi(n)$ des partitions de l'entier $n$ (*i.e. *au nombre de façons d'écrire $n$ comme somme $n = \sum_{k=1}^{s} \lambda_k$ avec $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_s > 0$).*

**3.1.7 Proposition.** — *Soit $\lambda = (\lambda_1, \ldots, \lambda_s)$ une partition de $n$, et pour tout $1 \leq j \leq n$, soit $a_j(\lambda)$ le nombre de termes $\lambda_i$ égaux à $j$. Alors le cardinal de la classe de conjugaison correspondant à $\lambda$ est*

$$n!/\left(\prod_{j=1}^{n} a_j(\lambda)!j^{a_j(\lambda)}\right)$$

*Démonstration.* — Il s'agit de démontrer que le cardinal du stabilisateur d'un élément de la classe est $\left(\prod_{j=1}^{n} a_j(\lambda)!j^{a_j(\lambda)}\right)$. Soit donc $\sigma$ une permutation de la classe, $H = \langle\sigma\rangle$ le sous-groupe de $\mathfrak{S}_n$ engendré par $\sigma$, et soient $C_1, \ldots, C_s$ les supports des cycles de $\sigma$, rangés par ordre de cardinalité décroissante ; on a vu que les $C_j$ sont aussi les orbites de l'action de $H$ dans $X$. Pour $1 \leq j \leq n$, soit $X_j$ la réunion des $C_i$ de cardinal $j$ ; on a donc $|X_j| = ja_j(\lambda)$. Comme nous l'avons vu dans la démonstration de la prop. 3.1.5, si $\tau$ commute à $\sigma$, on a $\tau H\tau^{-1} = H$ et $\tau$ applique chaque $H$-orbite sur une $H$-orbite de même cardinal.

Choisissons un point $x_i$ dans chaque $C_i$. Toujours d'après la démonstration de la prop. 3.1.5, pour définir une permutation $\tau$ commutant à $\sigma$, on peut choisir arbitrairement une permutation des $C_i$ de cardinal $j$ donné, disons $\varphi$, puis un point $x'_i$ dans chaque $C_i$, et il y aura alors une unique $\tau$ commutant à $\sigma$ appliquant $x_i$ sur $x'_{\varphi(i)}$ ; cela donne $a_j(\lambda)!j^{a_j(\lambda)}$ choix pour la restriction de $\tau$ à $X_j$, et comme ces choix sont indépendants, on a bien la formule voulue (on notera que lorsque $a_j(\lambda) = 0$, $a_j(\lambda)!j^{a_j(\lambda)} = 1$, donc on peut faire porter le produit sur tous les indices $j$.)

**3.1.8 Exemple.** — Considérons le groupe $\mathfrak{S}_5$. Il existe 7 partitions de 5, à savoir (5), (4, 1), (3, 2), (3, 1, 1), (2, 2, 1), (2, 1, 1, 1), (1, 1, 1, 1, 1). D'après la formule précédente, les stabilisateurs ont respectivement pour cardinal 5, 4, 6, 6, 8, 12, 120, donc les classes de conjugaison ont pour cardinal 24, 30, 20, 20, 15, 10, 1. On vérifie que la somme de ces cardinalités est bien égale à 120.

**3.1.9 Exercice.** — En vous inspirant de la démonstration de la proposition précédente, pouvez-vous décrire la structure du centralisateur de $\sigma$ ? (On pourra commencer par décrire la structure du centralisateur pour les diverses classes de conjugaison de $\mathfrak{S}_5$.)

## 3.2 Engendrement par transpositions et signature

**3.2.1.** On appelle *transposition* dans $\mathfrak{S}_n$ toute permutation $\tau$ dont la partition associée est $2+1+\ldots+1$, *i.e.* pour laquelle il existe deux éléments $i \neq j$ dans $X$ tels que $\tau(i)=j$, $\tau(j)=i$, et $\tau(k)=k$ si $k \neq i,j$. Les transpositions forment donc une classe de conjugaison dans $\mathfrak{S}_n$. Nous noterons $\tau_{i,j}$ la transposition définie par $\{i,j\}$, et $\tau_i = \tau_{i,i+1}$ pour $1 \leq i < n$.

**3.2.2 Proposition.** — *Les transpositions, et même les $\tau_i$, $1 \leq i < n$, engendrent le groupe $\mathfrak{S}_n$.*

*Démonstration.* — On raisonne par récurrence sur $n$, le cas $n=1$ étant trivial. On identifie $\mathfrak{S}_{n-1}$ au stabilisateur de $n \in X$ dans $\mathfrak{S}_n$. Alors pour montrer que les transpositions engendrent $\mathfrak{S}_n$, suffit de prouver que pour toute $\sigma \in \mathfrak{S}_n$, $\sigma \notin \mathfrak{S}_{n-1}$, il existe $\sigma' \in \mathfrak{S}_{n-1}$ et $j < n$ tels que $\sigma = \tau_{jn}\sigma'$. Or c'est facile : il suffit de prendre $j = \sigma(n)$ ; alors $\tau_{jn}^{-1}\sigma = \tau_{jn}\sigma \in \mathfrak{S}_{n-1}$.

Pour passer de là au cas des $\tau_i$, il suffit de remarquer que si $j < n-1$, on a $\tau_j\tau_{jn}\tau_j = \tau_{j+1,n}$, ce qui prouve aussitôt que le sous-groupe engendré par les $\tau_i$ contient tous les $\tau_{i,j}$.

**3.2.3 Théorème.** — *Il existe un unique homomorphisme $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ tel que $\varepsilon(\tau) = -1$ pour toute transposition $\tau$. On dit que $\varepsilon$ est l'homomorphisme de* signature.

*Démonstration.* — L'unicité de $\varepsilon$ est claire, car les transpositions engendrent $\mathfrak{S}_n$ d'apres 3.2.2. Prouvons l'existence. Soit $Y = \mathcal{P}_2(X)$ l'ensemble des parties à deux éléments de $X$ ; alors $\mathfrak{S}_n$ agit (transitivement) sur $Y$ par permutation. Pour tous $\sigma \in \mathfrak{S}_n$, $A \in Y$, avec $A = \{i,j\}$, posons

$$I(\sigma, A) = \frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(i)-\sigma(j)}{i-j} \in \mathbf{Q}^\times$$

(on voit donc que $I(\sigma,A)$ est $>0$ si $\sigma$ préserve l'ordre des éléments de $A$, et $<0$ s'il le renverse.) On vérifie aisément la formule :

$$I(\sigma\sigma', A) = I(\sigma, \sigma' A) I(\sigma', A) \qquad \text{pour tous } \sigma, \sigma' \in \mathfrak{S}_n,\ A \in Y$$

Posons maintenant :

$$\varepsilon(\sigma) = \prod_{i<j} \operatorname{sgn} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{A \in Y} \operatorname{sgn}\big(I(\sigma, A)\big)$$

Clairement, $\varepsilon(\sigma) \in \{\pm 1\}$ pour tout $\sigma \in \mathfrak{S}_n$. De plus :

$$\varepsilon(\sigma\sigma') = \prod_{A \in Y} \operatorname{sgn}\big(I(\sigma\sigma', A)\big) = \prod_{A \in Y} \operatorname{sgn}\big(I(\sigma, \sigma' A)\big) \prod_{A \in Y} \operatorname{sgn}\big(I(\sigma', A)\big) \qquad (*)$$

et comme $\sigma' A$ parcourt $Y$ lorsque $A$ parcourt $Y$, le premier facteur du membre de droite de $(*)$ est encore égal à $\varepsilon(\sigma)$. Donc $\varepsilon$ est bien un homomorphisme.

Reste à prouver que $\varepsilon$ n'est pas trivial dès que $n \geq 2$ ; il suffira pour cela de prouver que $\varepsilon[1,2] = -1$. Or il est clair que si $\sigma = [1,2]$, on a $sgn(I(\sigma, A)) = -1$ si $A = 1, 2$, et 1 sinon, puisque si $A = \{1, j\}$, $j > 2$, on a $\sigma(j) - \sigma(1) = j - 2 > 0$, si $A = \{2, j\}$, $j > 2$, on a $\sigma(j) - \sigma(2) = j - 1 > 0$, et si $A = i, j$, $2 < i < j$, on a encore $\sigma(j) - \sigma(i) > 0$.

**3.2.4 Exercice.** — Montrer que $\varepsilon$ est le *seul* homomorphisme non trivial de $\mathfrak{S}_n$ vers $\{\pm 1\}$.

**3.2.5 Définition.** — Soit $\sigma \in \mathfrak{S}_n$. On dit que $\sigma$ est *paire* (resp. *impaire*) si $\varepsilon(\sigma) = 1$ (resp. $-1$). Les permutations paires forment pour $n \geq 2$ un sous-groupe distingué d'indice 2 dans $\mathfrak{S}_n$, noté $\mathfrak{A}_n$ et appelé *groupe alterné* d'indice $n$.

Une permutation est paire (resp. impaire) si et seulement si elle s'écrit comme produit d'un nombre pair (resp. impair) de transpositions ; ces deux cas sont donc mutuellement exclusifs.

**3.2.6 Proposition.** — *Un cycle $\gamma \in \mathfrak{S}_n$ est dans $\mathfrak{A}_n$ si et seulement si il est de longueur* impaire.

*Démonstration.* — Récurrence sur la longueur. Il est clair qu'un cycle de longueur 1 est dans $\mathfrak{A}_n$ (puisque c'est l'identité). Soit $\gamma = [i_1, \ldots, i_p]$, avec $p > 1$ ; alors d'après la prop. 3.1.2 *(c)*, $\gamma = [i_1, \ldots, i_{p-1}]\tau_{i_{p-1}, i_p}$. Donc, si par hypothèse de récurrence on a $\varepsilon[i_1, \ldots, i_{p-1}] = (-1)^{p-2}$, on a bien $\varepsilon(\gamma) = (-1)^{p-1}$.

**3.2.7 Théorème.** — *Soit $n$ un entier $\geq 2$.*

*(a) Les 3-cycles engendrent $\mathfrak{A}_n$.*
*(b) $\mathfrak{A}_n = D(\mathfrak{S}_n)$*
*(c) Si $\tau$ est une transposition quelconque, $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \{1, \tau\}$.*

*Démonstration.* — *(a)* On procède par récurrence sur $n$, exactement comme à la prop. 3.2.2 ; on remarque que les 3-cycles appartiennent à $\mathfrak{A}_n$ d'après 3.2.6. Si $n = 2$, $\mathfrak{A}_n = \{1\}$, et il n'y a rien à démontrer. Supposons $n > 2$ ; le stabilisateur de $n$ dans $\mathfrak{A}_n$ est alors égal à $\mathfrak{A}_{n-1}$. Il suffit de prouver que pour tout $\sigma \in \mathfrak{A}_n$ tel que $\sigma(n) \neq n$ il existe un 3-cycle $\gamma$ tel que $\gamma(n) = \sigma(n)$ ; mais cela est clair : il suffit de choisir $j$ distinct de $n, \sigma(n)$ et de prendre $\gamma = [n, \sigma(n), j]$.

*(b)* Il est clair que $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$, car $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$ est commutatif. Pour la réciproque, d'après *(a)*, il suffit de prouver que $D(\mathfrak{S}_n)$ contient un 3-cycle ; en effet les 3-cycles sont tous conjugués dans $\mathfrak{S}_n$ (prop. 3.1.5), donc $D(\mathfrak{S}_n)$ contiendra tous les 3-cycles, donc sera égal à $\mathfrak{A}_n$ d'après *(a)*. On peut supposer $n \geq 3$, le cas $n = 2$ étant trivial. Mais alors $\mathfrak{S}_3$ s'identifie à un sous-groupe de $\mathfrak{S}_n$, donc il suffira de traiter le cas $n = 3$ ; or si $\gamma = [1, 2, 3]$, $\tau = [1, 2]$, on a $[\tau, \gamma] = \gamma^{-2} = \gamma$, d'où le résultat.
*(c)* Il est clair que pour toute transposition $\tau$, le sous-groupe $\{1, \tau\}$ est un supplémentaire de $\mathfrak{A}_n$ dans $\mathfrak{S}_n$.

**3.2.8 Exercice.** — *(a)* Montrer que la signature de $\sigma \in \mathfrak{S}_n$ ne dépend que de la classe de conjugaison de $\sigma$. *(b)* Soit $\lambda$ une partition de $n$. Exprimer la signature des éléments de la classe de conjugaison associée à $\lambda$ à partir de $\lambda$. Caractériser les partitions associées aux permutations *paires*. *(c)* Vérifier que dans $\mathfrak{S}_5$ il y a autant de permutations paires que de permutations impaires.

## 3.3 Simplicité des groupes alternés

**3.3.1.** Nous allons maintenant rencontrer notre premier exemple de groupe simple non commutatif : il s'agit du groupe alterné $\mathfrak{A}_5$, d'ordre 60. Par une utilisation judicieuse des théorèmes de Sylow vus au chapitre 2, il n'est pas trop difficile de prouver que tout groupe d'ordre $< 60$ est résoluble ; ainsi, $\mathfrak{A}_5$ est le plus petit groupe simple non commutatif. De plus, on peut prouver qu'à isomorphisme près, $\mathfrak{A}_5$ est le *seul* groupe simple d'ordre 60. Le groupe simple suivant, par ordre croissant de cardinalité, n'est rencontré que pour l'ordre 168 (c'est le groupe $\mathbf{PSL}(2, \mathbf{F}_7) \simeq \mathbf{PSL}(3, \mathbf{F}_2)$, qui sera considéré dans la section suivante) ; cela donne une idée de la grande rareté des groupes simples.

La simplicité du groupe $\mathfrak{A}_5$ est la clef de voûte de la démonstration par Galois de l'impossibilité de la résolution par radicaux de l'équation générale de degré 5 ; mais ceci est une autre histoire.

Nous démontrerons en fait la simplicité du groupe $\mathfrak{A}_n$ pour tout $n \geq 5$ ; nous traiterons d'abord le cas $n = 5$, puis nous en déduirons le cas général par récurrence.

**3.3.2 Lemme.** — *Soit $Z$ un $\mathfrak{S}_n$-ensemble fini, $z \in Z$, et soit $H$ le stabilisateur de $z$ dans $\mathfrak{S}_n$. Alors deux cas peuvent se produire :*

*(a) $H \not\subset \mathfrak{A}_n$ ; alors $\mathfrak{A}_n z = \mathfrak{S}_n z$,* i.e. *les orbites de $z$ sous $\mathfrak{A}_n$ et $\mathfrak{S}_n$ sont les mêmes.*

*(b) $H \subset \mathfrak{A}_n$ ; alors $\mathfrak{S}_n z$ se décompose en deux orbites de même cardinal sous l'action de $\mathfrak{A}_n$.*

*Démonstration.* — Soit $\sigma \in \mathfrak{S}_n$, $\sigma \notin \mathfrak{A}_n$. Alors $\sigma$ est un représentant de la classe non triviale de $\mathfrak{A}_n$ dans $\mathfrak{S}_n$, d'où $\mathfrak{S}_n = \mathfrak{A}_n \coprod \mathfrak{A}_n\sigma$. Donc dans tous les cas, $\mathfrak{S}_n z = \mathfrak{A}_n z \cup \mathfrak{A}_n \sigma z$ (union non nécessairement disjointe), ce qui prouve que $\mathfrak{A}_n$ possède au plus deux orbites dans $\mathfrak{S}_n z$.

Si $H \not\subset \mathfrak{A}_n$, on peut prendre $\sigma \in H$ ; alors il est clair que $\mathfrak{S}_n z = \mathfrak{A}_n z$, et l'action de $\mathfrak{A}_n$ sur $\mathfrak{S}_n z$ est transitive. Si $H \subset \mathfrak{A}_n$, on ne peut pas avoir $\sigma z \in \mathfrak{A}_n z$ ; en effet si $\sigma z = \tau z$ avec $\tau \in \mathfrak{A}_n$, on aurait $\tau^{-1}\sigma \in H \subset \mathfrak{A}_n$, d'où $\sigma \in \mathfrak{A}_n$, contrairement à l'hypothèse. Donc il y a bien deux $\mathfrak{A}_n$-orbites distinctes, $Z' = \mathfrak{A}_n z$ et $Z'' = \mathfrak{A}_n \sigma z$. De plus, comme $\sigma$ normalise $\mathfrak{A}_n$ on voit aussitôt que l'action de $\sigma$ se restreint en une bijection de $Z'$ sur $Z''$ ; les deux orbites ont donc même cardinal.

**3.3.3 Lemme.** — *Si $n \geq 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

*Démonstration.* — D'après le lemme 3.3.2, il suffit de prouver que le centralisateur d'un 3-cycle $\gamma$ dans $\mathfrak{S}_n$ contient une permutation impaire. Or c'est évident : quitte à conjuguer $\gamma$ on peut supposer que $\gamma = [1, 2, 3]$, et alors la transposition $\tau = [4, 5]$ commute trivialement à $\gamma$, puisque les supports de $\tau$ et $\gamma$ sont disjoints.

**3.3.4 Remarque.** — Le résultat ci-dessus est *faux* si $n = 3$ ou $n = 4$ (exercice).

**3.3.5 Théorème.** — *Le groupe $\mathfrak{A}_5$ est simple.*

*Démonstration.* — Il y a dans $\mathfrak{S}_5$ quatre classes de conjugaison de permutations paires (cf. exercice 3.2.8) : la classe de l'identité, la classe des 3-cycles, la classe des 5-cycles et la classe associée à la partition $\lambda = (2, 2, 1)$ (produits de deux transpositions à supports disjoints). D'après le lemme 3.3.3 et le théorème 3.2.7 *(a)*, il suffit de prouver que tout sous-groupe distingué $N \neq \{1\}$ de $\mathfrak{A}_5$ contient un 3-cycle. Soit donc $N$ un tel groupe, $\sigma \neq 1 \in N$, et supposons que $\sigma$ ne soit pas un 3-cycle. Alors (quitte à conjuguer $N$ et $\sigma$ par un élément convenable de $\mathfrak{S}_5$, ce qui est loisible si l'on veut prouver que $N = \mathfrak{A}_5$), on peut supposer que l'on est dans l'un des deux cas suivants :

*(a)* $\sigma = [1, 2, 3, 4, 5]$ : alors en conjuguant par $\tau = [2, 3][4, 5]$ on voit que $N$ contient $\sigma' = \tau\sigma\tau^{-1} = [1, 3, 2, 5, 4]$, donc $\sigma\sigma' = [1, 4, 2][3][5]$, qui est un 3-cycle.

*(b)* $\sigma = [1, 2][3, 4][5]$ : alors en conjuguant par $\gamma = [3, 4, 5]$, on voit que $N$ contient $\sigma' = \tau\sigma\tau^{-1} = [1, 2][3][4, 5]$, donc $\sigma\sigma' = [1][2][3, 4, 5]$ qui est un 3-cycle.

(on a utilisé la prop. 3.1.2 *(b)*).

**3.3.6 Théorème.** — *Pour tout $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.*

*Démonstration.* — On procède par récurrence sur $n$, le cas $n = 5$ ayant déjà été vu au théorème 3.3.5. Supposons donc $n > 5$, et identifions $\mathfrak{A}_{n-1}$ au sous-groupe de $\mathfrak{A}_n$ stabilisant $n \in X$. Soit $N$ un sous-groupe distingué $\neq \{1\}$ de $\mathfrak{A}_n$ ; il suffira alors de prouver que $N \cap \mathfrak{A}_{n-1} \neq \{1\}$. En effet, on aura alors $N \cap \mathfrak{A}_{n-1} = \mathfrak{A}_{n-1}$ par hypothèse de récurrence ; en particulier, $N$ contient au moins un 3-cycle, mais alors il les contient tous d'après le lemme 3.3.3, et $N = \mathfrak{A}_n$ d'après le théorème 3.2.7 *(a)*.

En fait, il suffit de prouver qu'il existe $\sigma \neq 1$ dans $N$ possédant un point fixe dans $X$ ; en effet, quitte à conjuguer $\sigma$ par un élément de $\mathfrak{A}_n$, qui agit transitivement sur $X$, on pourra alors supposer $\sigma \in \mathfrak{A}_{n-1}$ et on aura gagné. Or, soit $\sigma \neq 1$ arbitraire dans $N$, et soit $\gamma$ un 3-cycle tel que le support de $\gamma$ ne soit pas $\sigma$-stable. Alors $[\sigma, \gamma] = \sigma.\gamma\sigma^{-1}\gamma^{-1} \in N$ ; mais en écrivant $[\sigma, \gamma] = \sigma\gamma\sigma^{-1}.\gamma^{-1}$ on voit que $[\sigma, \gamma] \neq 1$ est le produit de deux 3-cycles, et en particulier que son support contient au plus six éléments (et strictement moins de six si les supports de $\sigma\gamma\sigma^{-1}$ et $\gamma^{-1}$ ne sont pas disjoints). Ainsi, si $n > 6$ on est déjà certain que $[\sigma, \gamma]$ possède au moins un point fixe ; le seul cas un petit peu plus délicat est le cas $n = 6$, où l'on doit prouver que l'on peut choisir $\gamma$ pour que les supports de $\sigma\gamma\sigma^{-1}$ et $\gamma^{-1}$ (ou, ce qui revient au même, de $\sigma\gamma\sigma^{-1}$ et de $\gamma$), ne soient pas disjoints.

Or cela est facile. En effet, on peut supposer que $\sigma$ n'a pas de points fixes. Soit $\sigma = \gamma_1 \dots \gamma_s$ la décomposition en cycles de $\sigma$, et soit $C_j$ le support de $\gamma_j$ ; on a donc $|C_j| > 1$ pour $1 \leq j \leq s$. On ne peut pas avoir $s = 1$, car alors $\sigma$ serait un 6-cycle, et ne pourrait donc pas être pair. Soit alors $x \in C_1$, $y \in C_2$ ; les éléments $x, \sigma(x), y, \sigma(y)$ sont donc tous distincts dans $X$. Prenons maintenant $\gamma = [x, \sigma(x), y]$ ; si $\gamma' = \sigma\gamma\sigma^{-1}$, on a $\gamma' = [\sigma(x), \sigma^2(x), \sigma(y)]$, ce qui prouve que $\operatorname{supp}\gamma \cup \operatorname{supp}\gamma'$ a 4 ou 5 éléments, suivant que $\sigma^2(x)$ soit égal à $x$ ou non. Dans les deux cas, on a le résultat voulu.

## 3.4 Groupes linéaires

**3.4.1.** Fixons pour toute la suite du chapitre un corps commutatif $k$, de caractéristique arbitraire, et un entier $n \geq 1$. Nous nous intéressons à la structure du groupe $\mathbf{GL}(n,k)$ de toutes les matrices $n \times n$ inversibles à coefficients dans $k$. Nous noterons $\mathbf{F}_p$ le corps fini $\mathbf{Z}/p\mathbf{Z}$, $p$ premier.

**3.4.2 Définition.** — On note $\mathbf{SL}(n,k)$, et on appelle *groupe spécial linéaire* d'ordre $n$ sur $k$, le noyau de l'homomorphisme $u \to \det(u)$ de $\mathbf{GL}(n,k)$ vers le groupe multiplicatif $k^\times$. On note $\mathbf{PGL}(n,k)$ et l'on appelle *groupe projectif linéaire* d'ordre $n$ le quotient de $\mathbf{GL}(n,k)$ par le sous-groupe (isomorphe à $k^\times$) des matrices scalaires inversibles ; de même, on note $\mathbf{PSL}(n,k)$ le quotient de $\mathbf{SL}(n,k)$ par le sous-groupe des matrices scalaires inversibles de déterminant 1 (isomorphe au sous-groupe de $k^\times$ formé des racines $n^{\text{ièmes}}$ de l'unité dans $k$).

Pour tout espace vectoriel $V$ de dimension $n$ sur $k$, on note $\mathbf{GL}(V)$ le groupe des applications linéaires inversibles de $V$ vers lui-même ; alors en choisissant une base de $V$, on obtient un isomorphisme $\mathbf{GL}(V) \simeq \mathbf{GL}(n,k)$. On définit de même $\mathbf{SL}(V)$, $\mathbf{PGL}(V)$ et $\mathbf{PSL}(V)$, respectivement isomorphes à $\mathbf{SL}(n,k)$, $\mathbf{PGL}(n,k)$ et $\mathbf{PSL}(n,k)$.

**3.4.3 Proposition.** — *Supposons $k$ fini, et soit $q$ le cardinal de $k$. Alors le groupe $\mathbf{GL}(n,k)$ est fini, de cardinal $\prod_{j=0}^{n-1}(q^n - q^j)$. Les groupes $\mathbf{SL}(n,k)$ et $\mathbf{PGL}(n,k)$ ont tous deux pour cardinal $\dfrac{1}{q-1}|\mathbf{GL}(n,k)|$. Le groupe $\mathbf{PSL}(n,k)$ est distingué dans $\mathbf{PGL}(n,k)$, et $\mathbf{PGL}(n,k)/\mathbf{PSL}(n,k) \simeq k^\times/\mu_n(k^\times)$, en notant $\mu_n$ l'homomorphisme $\lambda \to \lambda^n$ de $k^\times$ vers lui-même.*

*Démonstration.* — Soit $(e_1, \ldots, e_n)$ la base canonique de $k^n$. Pour définir un élément $u \in \mathbf{GL}(n,k)$, on peut choisir arbitrairement $u(e_1)$ parmi les vecteurs non nuls de $k^n$, ce qui donne $q^n - 1$ choix, puis $u(e_2)$ dans le complémentaire du sous-espace vectoriel engendré par $u(e_1)$ ($q^n - q$ choix), etc. D'où la formule pour le cardinal de $\mathbf{GL}(n,k)$. On en déduit le cardinal de $\mathbf{PGL}(n,k)$, et aussi celui de $\mathbf{SL}(n,k)$ en remarquant que l'homomorphisme déterminant est surjectif : pour $a \in k^\times$, le déterminant de la matrice

$$\operatorname{diag}(a, 1, \ldots, 1) = \begin{pmatrix} a & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

est égal à $a$.

Il est clair que $\mathbf{PSL}(n,k)$ est distingué dans $\mathbf{PGL}(n,k)$, puisque c'est l'image du sous-groupe distingué $\mathbf{SL}(n,k) \subset \mathbf{GL}(n,k)$. Le quotient $\mathbf{PGL}(n,k)/\mathbf{PSL}(n,k)$ s'identifie au quotient de $\mathbf{GL}(n,k)$ par le sous-groupe distingué $N$ engendré par $\mathbf{SL}(n,k)$ et le groupe $D$ des matrices scalaires inversibles. En passant au quotient par $\mathbf{SL}(n,k)$, on voit que ce quotient s'identifie encore au quotient de $k^\times$ par l'image par le déterminant du groupe $N$, qui est précisément $\mu_n(k^\times)$.

**3.4.4 Exercice.** — Montrer que le groupe $\mathbf{GL}(2, \mathbf{F}_2)$ est isomorphe au groupe symétrique $\mathfrak{S}_3$. Exhiber les éléments d'ordre 3 de $\mathbf{GL}(2, \mathbf{F}_2)$.

**3.4.5 Exercice.** — *(a)* Montrer que $\mathfrak{S}_4$ possède un unique sous-groupe distingué d'ordre 4, isomorphe à $\mathbf{F}_2^2$. *(b)* Montrer que $\mathfrak{S}_4 \simeq \mathbf{F}_2^2 \rtimes \mathbf{GL}(2, \mathbf{F}_2)$.

**3.4.6 Exercice.** — Déterminer la structure du groupe $\mathbf{Q}^\times/\mu_2(\mathbf{Q}^\times)$ ; on pourra prouver que c'est un espace vectoriel de dimension infinie sur le corps $\mathbf{F}_2$, dont on donnera une base naturelle.

**3.4.7 Lemme.** — *Soit $V$ un $k$-espace vectoriel de dimension $n$, et soit $u$ un endomorphisme de $V$ tel que tout $x \neq 0$ dans $V$ soit vecteur propre de $u$, de valeur propre $\lambda_x$ (dépendant* a priori *de $x$). Alors en fait les $\lambda_x$ sont tous égaux, et $u$ est un edomorphisme scalaire.*

*Démonstration.* — C'est classique. Si $a \neq 0$ dans $k$ et $x \neq 0$ dans $V$, on a

$$u(ax) = \lambda_{ax} ax = au(x) = a\lambda_x x$$

donc $a\lambda_{ax} = a\lambda_x$ et $\lambda_{ax} = \lambda_x$. Si $x$ et $y$ sont non colinéaires :

$$u(x+y) = \lambda_{x+y}(x+y) = u(x) + u(y) = \lambda_x x + \lambda_y y$$

donc $\lambda_{x+y} = \lambda_x = \lambda_y$, puisque $(x, y)$ est une base du sous-espace vectoriel engendré par $x$ et $y$.

**3.4.8 Proposition.** — *Soit $V$ un $k$-espace vectoriel de dimension $n$. Le commutant de $\mathbf{SL}(V)$ dans $\mathbf{GL}(V)$ est égal à $k^\times$.*

*Démonstration.* — Il est clair que les matrices scalaires inversibles sont dans le commutant de $\mathbf{SL}(V)$. Réciproquement, soit $u \in \mathbf{GL}(n, k)$ commutant à $\mathbf{SL}(V)$, et soit $x \neq 0$ dans $V$. Soit $(e_1, \ldots, e_n)$ une base de $V$ telle que $e_1 = x$, et soit $g \in \mathbf{SL}(V)$ l'endomorphisme dont la matrice dans la base $(e_1, \ldots, e_n)$ est :

$$\begin{pmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$$

Alors le sous-espace propre de $V$ pour la valeur propre 1 est $ke_1 = kx$ ; or puisque $u$ commute à $g$, il préserve les sous-espaces propres de $g$, donc $u(x) = \lambda_x x \in kx$. Comme ceci est vrai pour tout $x \neq 0$ dans $V$, on peut appliquer le lemme 3.4.7, et conclure que $u \in k^\times$.

**3.4.9 Corollaire.** — *(a) Le centre de $\mathbf{GL}(V)$ est égal à $k^\times$.*

*(b) Le centre de $\mathbf{SL}(V)$ est égal à $k^\times \cap \mathbf{SL}(V)$.*

*Démonstration.* — Soit $Z$ le centre de $\mathbf{GL}(V)$. Alors il est clair que $k^\times \subset Z$ ; mais comme $Z$ est contenu dans le commutant de $\mathbf{SL}(V)$, on a $Z \subset k^\times$ d'après la proposition, d'où l'égalité. De même, le centre de $\mathbf{SL}(V)$ est l'intersection du commutant de $\mathbf{SL}(V)$ dans $\mathbf{GL}(V)$ avec $\mathbf{SL}(V)$, donc $k^\times \cap \mathbf{SL}(V)$ d'après la proposition.

**3.4.10.** Il découle du cor. 3.4.9 que les groupes $\mathbf{PGL}(V)$ et $\mathbf{PSL}(V)$ ne sont autres que les quotients de $\mathbf{GL}(V)$ et $\mathbf{SL}(V)$ par leurs centres respectifs, et sont donc intrinsèquement définis en termes de la seule structure de groupe (indépendamment de la réalisation matricielle.) Il y a encore un autre point de vue, plus géométrique, sur ces groupes, qui explique d'ailleurs les notations. Notons $\mathbf{P}(V)$, et appelons *espace projectif* associé à $V$, l'ensemble des droites vectorielles de $V$. Alors il est clair que $\mathbf{GL}(V)$ et $\mathbf{SL}(V)$ agissent (transitivement) sur $\mathbf{P}(V)$. Le noyau de cette action est formé de l'ensemble des $u$ tels que $u(D) = D$ pour *toute* droite vectorielle $D$, ou encore tels que $u(x)$ soit colinéaire à $x$ pour tout $x \neq 0$ dans $V$. D'après le lemme 3.4.7, un tel endomorphisme $u$ est scalaire. Donc $\mathbf{PGL}(V)$ et $\mathbf{PSL}(V)$ peuvent encore s'interpreter comme les images canoniques de $\mathbf{GL}(V)$ et $\mathbf{SL}(V)$ dans leur action sur $\mathbf{P}(V)$ ; d'où leurs noms de groupe linéaire projectif et groupe spécial linéaire projectif.

**3.4.11.** Comme pour le groupe symétrique, on peut trouver un ensemble de générateurs remarquables pour le groupe $\mathbf{SL}(V)$. Commençons par faire une remarque générale : si l'on se donne une décomposition $V = V_1 \oplus V_2$ de $V$ comme somme directe de deux sous-espaces vectoriels, tout endomorphisme $u$ de $V$ possède une décomposition en blocs :

$$u = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

avec $u_{ij} \in \mathrm{Hom}\,(V_j, V_i)$, et on peut calculer en termes de ces décompositions suivant les règles habituelles du calcul matriciel.

Soit $D$ une droite vectorielle de $V$, et soit $P_D$ le stabilisateur de $D$ dans $\mathbf{GL}(V)$ ; soit $W$ un supplémentaire de $D$ dans $V$. Alors, compte tenu du fait que l'algèbre $\mathrm{End}\,(D)$ s'identifie à $k$, la décomposition en blocs de $u \in P_D$ prend la forme :

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \qquad (*)$$

avec $a \in k^\times$, $b \in \mathrm{Hom}\,(W, D)$, $c \in \mathbf{GL}(W)$ ; pour avoir le stabilisateur dans $\mathbf{SL}(V)$ il faut rajouter la condition $a \det(c) = 1$. Le scalaire $a$ correspond simplement à l'action de $u$ dans $D$ ; l'endomorphisme $c$ a également un sens intrinsèque : moyennant l'identification canonique de $W$ avec l'espace quotient $V/D$, il donne l'action de $u$ dans $V/D$.

Nous noterons $U_D$ le sous-groupe de $P_D$ formé des $u$ tels que $u|_D = 1$ et $\mathrm{Im}\,(u - \mathrm{Id}) \subset D$ ; on voit aussitôt que ces conditions sont équivalentes au fait que dans la décomposition en blocs de $u$ associée à n'importe quelle écriture $V = D \oplus W$, l'on ait $a = 1$, $c = \mathrm{Id}_W$. Les éléments $u \neq \mathrm{Id}$ de $U_D$ sont appelés *transvections* de droite $D$.

**3.4.12 Lemme.** — *Si $g \in \mathbf{GL}(V)$ est tel que $g(D) = D'$, alors $gU_Dg^{-1} = U_{D'}$.*

*Démonstration.* — Clairement, si $g(D) = D'$ et $u \in U_D$, l'automorphisme $u' = gug^{-1}$ de $V$ vérifie $u'|_{D'} = 1$, et $\mathrm{Im}\,(u' - \mathrm{Id}) = \mathrm{Im}\,(g(u - \mathrm{Id})g^{-1}) = g\,\mathrm{Im}\,(u - 1) \subset D'$.

**3.4.13 Lemme.** — *Soit $V = V_1 \oplus V_2$ une décomposition de $V$ en somme directe de deux sous-espaces vectoriels, avec $\dim V_1 > 0$. Soit $u_1$ une transvection de $V_1$, de droite $D_1$. Alors $u \oplus \mathrm{Id}_{V_2}$ est une transvection de $V$, de droite $D_1$.*

*Démonstration.* — C'est évident : on a $u|_{D_1} = 1$, et $\mathrm{Im}\,(u - \mathrm{Id}_V) = \mathrm{Im}\,(u_1 - \mathrm{Id}_{V_1}) \subset D_1$.

**3.4.14 Théorème.** — *Les transvections engendrent* $\mathbf{SL}(V)$.

*Démonstration.* — Récurrence sur $n = \dim V$. Si $n = 1$, $\mathbf{SL}(V) = \{1\}$, et il n'y a rien à démontrer. Supposons donc $n > 1$. Soit $H$ le sous-groupe de $\mathbf{SL}(V)$ engendré par les transvections.

*Lemme. — Le groupe $H$ agit transitivement sur $V\backslash\{0\}$.*

*Démonstration.* — Soient $x$ et $y$ deux vecteurs non nuls de $V$ ; montrons que si $x$ et $y$ ne sont pas colinéaires, il existe une transvection $u$ telle que $u(x) = y$. En effet, soit $V_1 = kx \oplus ky$ le sous-espace vectoriel de dimension 2 de $V$ engendré par $x$ et $y$, et soit $z = y - x$. Soit $D$ la droite engendrée par $z$, et soit $u_1$ la transvection de $V_1$ dont la matrice dans la base $(z, x)$ est $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Choisissons un supplémentaire $V_2$ de $V_1$ dans $V$, et soit $u$ l'extension de $u_1$ à $V$ par l'identité sur $V_2$ (lemme 3.4.13). Alors $u(x) = y$.

Si $x$ et $y$ sont colinéaires et distincts, il est clair qu'aucune transvection ne peut appliquer $x$ sur $y$, car toutes les valeurs propres d'une transvection sont égales à 1. Mais si $z$ n'est pas colinéaire à $x$ et $y$, il existe d'après ce qui précède des transvections $u, v$ telles que $u(x) = z$, $v(z) = y$, donc $v \circ u(x) = y$.

Poursuivons maintenant la preuve du théorème 3.4.14. Soit $x$ un vecteur non nul dans $V$, $D = kx$. Si $g$ est un élément arbitraire de $\mathbf{SL}(V)$, il existe d'après le lemme un élément $h \in H$ tel que $h(x) = g(x)$, donc $h^{-1}g(x) = x$, ce qui prouve que l'élément $h^{-1}g$ a dans toute décomposition $V = D \oplus W$ une décomposition de la forme :

$$\begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix}$$

avec $\det(c) = \det(h^{-1}g) = 1$. Par hypothèse de récurrence, on peut écrire $c$ comme un produit fini de transvections dans $\mathbf{SL}(W)$. Si on étend ces transvections à $V$ tout entier comme dans le lemme 3.4.13, on obtient donc un élément $k \in H$, stabilisant $x$ et induisant $c$ sur $W$. Donc $u = k^{-1}h^{-1}g$ stabilise $x$ et vérifie $\mathrm{Im}\,(u - \mathrm{Id}) \subset D$ ; il appartient donc à $U_D$, d'où $g = hku \in H$.

**3.4.15 Exercice.** — Fixons une droite $D \in V$. Montrer que les orbites de $U_D$ dans $V$ sont les droites affines parallèles à $D$ et distinctes de $D$, et les points de $D$. En déduire que si $x$ et $y$ sont des vecteurs non colinéaires, il existe une *unique* droite $D$ telle que $y \in U_D x$ (cf. le lemme dans la démonstration du théorème 3.4.14).

**3.4.16 Exercice.** — En analysant la démonstration ci-dessus, donner un majorant du nombre de transvections nécessaires à l'écriture d'un élément quelconque de $\mathbf{SL}(V)$. Par exemple, si $\dim V = 2$, on montrera que tout $g \in \mathbf{SL}(V)$ est produit d'au plus *trois* transvections. Cette borne est-elle optimale ?

**3.4.17 Proposition.** — *(a) L'action de* $\mathbf{GL}(V)$ *sur les transvections de $V$ est transitive.*

*(ii)Si $n \geq 3$, l'action de* $\mathbf{SL}(V)$ *sur les transvections de $V$ est transitive.*

*Démonstration.* — *(a)* On peut supposer $n \geq 2$. On sait déjà que $\mathbf{GL}(V)$ permute transitivement les divers groupes $U_D$, $D \in \mathbf{P}(V)$. Il suffit donc de prouver que l'action de $P_D$ sur $U_D$ est transitive. Or, si $W$ est un supplémentaire de $D$ dans $V$, $b \in \mathrm{Hom}\,(W, D)$, et $c \in \mathbf{GL}(W)$ on a :

$$\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & \mathrm{Id}_W \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & bc^{-1} \\ 0 & \mathrm{Id}_W \end{pmatrix}$$

Or il est clair que l'action de $\mathbf{GL}(W)$ sur $\mathrm{Hom}\,(W, D)$ par $c.b = bc^{-1}$ est transitive sur les vecteurs non nuls de $\mathrm{Hom}\,(W, D)$, d'où le résultat.

*(b)* Si $n \geq 3$, on peut prendre $c \in \mathbf{SL}(W)$ dans ce qui précède : l'action de $\mathbf{SL}(W)$ sur les éléments non nuls de $\mathrm{Hom}\,(W, D)$ est encore transitive.

**3.4.18 Exercice.** — Montrer par un exemple que l'action de $\mathbf{SL}(V)$ sur les transvections peut ne pas être transitive si $\dim(V) = 2$.

**3.4.19 Théorème.** — *(a) On a* $D(\mathbf{GL}(V)) = \mathbf{SL}(V)$ *sauf si* $\dim V = 2$, $k = \mathbf{F}_2$.
*(b) On a* $D(\mathbf{SL}(V)) = \mathbf{SL}(V)$ *sauf si* $\dim V = 2$, $k = \mathbf{F}_2$ *ou* $\dim V = 2$, $k = \mathbf{F}_3$.

*Démonstration.* — On peut supposer $\dim V > 1$. Puisque $\mathbf{SL}(V)$ est le noyau d'un homomorphisme de $\mathbf{GL}(V)$ vers un groupe commutatif, l'inclusion $D(\mathbf{GL}(V)) \subset \mathbf{SL}(V)$ est claire dans tous les cas. On remarque que $\mathbf{SL}(V)$, $D(\mathbf{GL}(V))$ et $D(\mathbf{SL}(V))$ sont tous trois des sous-groupes distingués de $\mathbf{GL}(V)$. Donc pour prouver *(a)* ou *(b)* pour $k$ et $n = \dim(V)$ fixés, il suffit de prouver qu'*une* transvection est un commutateur : d'après la prop. 3.4.17, elles le seront alors toutes, et le résultat résultera du théorème 3.4.14.

Fixons une droite $D \in V$ et un supplémentaire $W$ de $D$. Soit $c \in \mathbf{GL}(W)$, et $b \neq 0$ dans $\mathrm{Hom}\,(W, D)$. On a :

$$\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & \mathrm{Id}_W \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & c^{-1} \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & \mathrm{Id}_W \end{pmatrix} = \begin{pmatrix} 1 & b(c^{-1} - 1) \\ 0 & \mathrm{Id}_W \end{pmatrix}$$

Mais si $c \neq \mathrm{Id}_W$, il existe des $b \in \mathrm{Hom}\,(W, D)$ tels que $b(c^{-1} - 1) \neq 0$ (il suffit de prendre $b$ non nul sur l'image de $c-$) ; donc il existe dans ce cas des transvections qui sont des commutateurs. Si $n > 2$, il existe toujours des $c \neq 1 \in \mathbf{SL}(W)$ ; cela montre *(b)*, et *a fortiori (a)*, si $n > 2$. Si $n = 2$, $\dim W = 1$, et $\mathbf{GL}(W) \simeq k^\times$, donc le seul cas où $\mathbf{GL}(W) = \{1\}$ est celui où $k = \mathbf{F}_2$ ; d'où *(a)*.

Reste à prouver *(b)* si $n = 2$. On calcule, pour $a \in k^\times$ :

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a^2 - 1 \\ 0 & 1 \end{pmatrix}$$

On obtient donc une transvection s'il est possible de choisir $a$ tel que $a^2 \neq 1$. Or les éléments de carré 1 dans $k$ sont $\pm 1$ ; on peut donc conclure sauf si $k^\times = \{\pm 1\}$, *i.e.* sauf si $k = \mathbf{F}_2$ (auquel cas on a même $+1 = -1$) ou $k = \mathbf{F}_3$.

On peut montrer (exercice) que les groupes $\mathbf{SL}(2, \mathbf{F}_2)$ et $\mathbf{SL}(2, \mathbf{F}_3)$ sont *résolubles* $\neq \{1\}$ ; ils ne peuvent donc pas être égaux à leur groupe dérivé.

**3.4.20 Exercice.** — On se propose d'étudier les groupes $\mathbf{SL}(2, \mathbf{F}_3)$ et $\mathbf{PGL}(2, \mathbf{F}_3)$.

*(a)* Calculer le cardinal de $\mathbf{SL}(2, \mathbf{F}_3)$ et $\mathbf{PGL}(2, \mathbf{F}_3)$.

*(b)* Montrer que $|\mathbf{P}(\mathbf{F}_3^2)| = 4$ ; en déduire que $\mathbf{PGL}(2, \mathbf{F}_3) \simeq \mathfrak{S}_4$.

*(c)* Déterminer le centre de $\mathbf{SL}(2, \mathbf{F}_3)$ ; en déduire que $\mathbf{SL}(2, \mathbf{F}_3)$ n'est *pas* isomorphe à $\mathfrak{S}_4$.

*(d)* Montrer que le quotient $\mathbf{PSL}(2, \mathbf{F}_3)$ de $\mathbf{SL}(2, \mathbf{F}_3)$ par son centre est isomorphe au groupe alterné $\mathfrak{A}_4$. En déduire que $\mathbf{SL}(2, \mathbf{F}_3)$ est résoluble.

*(e)* Montrer que $\mathbf{SL}(2, \mathbf{F}_3)$ possède un 2-sous-groupe de Sylow distingué.

## 3.5 Simplicité du groupe $\mathbf{PSL}(n, k)$

**3.5.1.** Les groupes linéaires vont nous fournir une grande quantité de nouveaux exemples de groupes simples (y compris de nombreux exemples de groupes simples *infinis*). Plus précisément, on a le théorème suivant :

**3.5.2 Théorème.** — *Le groupe $\mathbf{PSL}(n, k)$ est simple sauf dans les deux cas $n = 2$, $k = \mathbf{F}_2$ et $n = 2, k = \mathbf{F}_3$ (où il est résoluble).*

**3.5.3.** Soit $G = \mathbf{PSL}(V)$, $V = k^n$. Nous allons démontrer la simplicité de $G$ par une méthode due à Iwasawa, qui s'applique dans de nombreux autres cas. L'idée est d'utiliser les propriétés remarquables de l'action de $G$ sur l'espace projectif $X = \mathbf{P}(V)$.

**3.5.4 Définition.** — Soit $G$ un groupe, $X$ un $G$-ensemble homogène. On dit que l'action de $G$ sur $X$ est *doublement transitive*, si pour tout $x \in X$, l'action du stabilisateur $G_x$ est transitive sur $X \backslash \{x\}$ (il suffit pour cela que ce soit vrai pour *un* point $x$ particulier, pourquoi ?). En particulier, nos conventions sur les actions transitives entraînent que $X \backslash \{x\} \neq \emptyset$. Il revient au même (exercice) de demander que l'action de $G$ soit transitive sur les couples d'éléments distincts de $X$.

**3.5.5 Lemme.** — *L'action de $\mathbf{PSL}(V)$ sur $\mathbf{P}(V)$ est doublement transitive dès que* $\dim V \geq 2$.

*Démonstration.* — Il suffit de le prouver pour l'action de $\mathbf{SL}(V)$. Soient $(D_1, D_2)$, $(D_1', D_2')$ deux couples de droites distinctes. Choisissons deux bases $(e_j)_{1 \leq j \leq n}$, $(e_j')_{1 \leq j \leq n}$ de $V$ telles que $D_1 = k\, e_1$, $D_2 = k\, e_2$, $D_1' = k\, e_1'$, $D_2' = k\, e_2'$. Alors il existe $g \in \mathbf{GL}(V)$ unique telle que $g(e_j) = e_j'$, $1 \leq j \leq n$ ; clairement on a $g(D_1) = D_1'$, $g(D_2) = D_2'$. Pour avoir $\det(g) = 1$, il suffit au besoin de remplacer $g$ par $gh$, où $h(e_1) = \lambda e_1$, $h(e_j) = e_j$ si $j > 1$, avec $\lambda = \det(g)^{-1}$.

**3.5.6 Proposition.** — *Soit $G$ un groupe, $X$ un $G$-ensemble homogène. On suppose que l'action de $G$ sur $X$ est doublement transitive. Soit $x \in X$, $H = G_x$.*

*(a) Pour tout $g \notin H$, on a $G = H \coprod HgH$.*

*(b) Le groupe $H$ est un sous-groupe propre maximal de $G$.*

*(c) Tout sous-groupe distingué $N$ de $G$ opère transitivement ou trivialement sur $X$.*

*Démonstration. — (a)* Si $g \notin H$, on a $gx \neq x$. Mais alors, si $g' \neq H$, il existe $h \in H$ tel que $hgx = g'x$ ; donc $g^{-1}h^{-1}g' = k \in H$, et $g' = hgk \in HgH$.

*(b)* Si $K$ est un sous-groupe de $G$ contenant strictement $H$, on peut prendre $g \in K$ dans *(a)*, et alors $HgH \subset K$, d'où $K = G$.

*(c)* Soit $K = NH = \{xy\}_{x\in N, y\in H}$. Alors on voit tout de suite que $K$ est un sous-groupe de $G$. Donc d'après *(b)* on a $K = G$ ou $K = H$. Dans le premier cas on a $NHx = Nx = Gx = X$, donc l'action de $N$ sur $X$ est transitive. Dans le second, on a $N \subset H$ ; mais alors en conjuguant on voit que $N \subset G_y$ pour tout $y \in X$, donc l'action de $N$ sur $X$ est triviale.

**3.5.7.** *Démonstration du théorème 3.5.2.* Nous avons déjà vu que dans les deux cas exceptionnels $\mathbf{SL}(V)$, donc aussi $\mathbf{PSL}(V)$, est résoluble (non commutatif), donc ne peut pas être simple. Soit $N$ un sous-groupe distingué non trivial de $\mathbf{PSL}(V)$, et soit $D \in \mathbf{P}(V)$. Comme $U_D \cap Z(\mathbf{SL}(V)) = \{1\}$, on peut identifier $U_D$ à son image dans $\mathbf{PSL}(V)$. Comme $\mathbf{SL}(V)$ est engendré par les transvections (thm. 3.4.14), et que l'image d'un ensemble générateur par une surjection est encore un ensemble générateur (du groupe image), $\mathbf{PSL}(V)$ est engendré par l'ensemble des $U_{D'}$, $D' \in \mathbf{P}(V)$, qui, d'après le lemme 3.4.12, est aussi l'ensemble des $gU_Dg^{-1}$, $g \in \mathbf{PSL}(V)$. Comme par définition le noyau de l'action de $\mathbf{PSL}(V)$ sur $\mathbf{P}(V)$ est réduit à $\{1\}$, $N$ ne peut pas agir trivialement sur $\mathbf{P}(V)$. D'après la prop. 3.5.6 *(c)*, il agit donc transitivement, ce qui entraîne que l'ensemble des $nU_Dn^{-1}$, $n \in N$, engendre déjà $\mathbf{PSL}(V)$. Mais comme $NU_D$ est un sous-groupe de $\mathbf{PSL}(V)$, on a en fait $nU_Dn^{-1} \subset NU_D$ pour tout $n \in N$, donc on conclut que

$$NU_D = \mathbf{PSL}(V)$$

Il en résulte aussitôt que la surjection canonique $\pi : \mathbf{PSL}(V) \to \mathbf{PSL}(V)/N$ se restreint en une surjection $U_D \to \mathbf{PSL}(V)/N$. Comme $U_D$ est un groupe commutatif, on en déduit que $\mathbf{PSL}(V)/N$ l'est également. Mais alors la propriété universelle du groupe dérivé entraîne que $D(\mathbf{PSL}(V)) \subset N$. Or, d'après le théorème 3.4.19, $\mathbf{SL}(V)$ (et donc aussi $\mathbf{PSL}(V)$) est égal à son groupe dérivé sauf si $n = 2$, $k = \mathbf{F}_2$ ou $\mathbf{F}_3$, d'où le théorème.