Concours Agrégation, Mathématiques générales

Leçon 08- Exemples de parties génératrices d'un groupe. Applications.

Commentaires du jury 2015 : C'est une leçon qui demande un minimum de culture mathématique. Peu de candidats voient l'utilité des parties génératrices dans l'analyse des morphismes de groupes ou pour montrer la connexité de certains groupes. Tout comme dans la leçon 106, la présentation du pivot de Gauss et de ses applications est envisageable.
Commentaires du jury 2016 : C'est une leçon qui doit être illustrée par des exemples très variés en relation avec les groupes de permutations et les groupes linéaires ou de leurs sous-groupes. La connaissance de parties génératrices s'avère très utile dans l'analyse des morphismes de groupes ou pour montrer la connexité de certains groupes. Tout comme dans la leçon 106, la présentation du pivot de Gauss et de ses applications est envisageable.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. B.C.D] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)
[Fr. E] Fresnel J. *Groupes* (Hermann 2001)
[Fr. MMG] Fresnel J. *Méthodes modernes en géométrie* (Hermann 1996, 2010)
et
[Se.] Serre J.P. *Cours d'arithmétique* (PUF 1970)

Développements conseillés :

(1) Nombre minimal de transpositions pour engendrer S_n (3 preuves : représentations linéaires, [Fr. E.] p.28 ; combinatoire des supports, [F. M. 1] $n°62$ et avec les graphes, [F. M. 2] p.114 et Compléments et errata.

(2) Engendrement de $SL_n(K)$ (resp. $SL_n(E)$) par les matrices élémentaires de transvections (resp. par les transvections) avec applications à la connexité des matrices de rang r dans le cas $\mathbb{R}$ ou $\mathbb{C}$ (Fresnel alg matrices p. 121 et ex. 2.3.16 p. 130) ou dans le cas $K = \mathbb{F}_p$, application à l'engendrement de $SL_n(\frac{\mathbb{Z}}{p^a\mathbb{Z}})$ par les transvections élémentaires, [Fr. A.] ex. 2.3.19 et 20 p. 136.

(3) Sur le nombre minimum de générateurs d'un groupe de type fini, [F. M. 2] Compléments-Errata, le compléments à la page 130 étudie la variation de ce nombre par inclusion. Il y a matière à plusieurs développements. Voir aussi Sous-groupe de Frattini et nombre minimal de générateurs d'un p-groupe fini, [F. M. 1] $n°76$, cas des groupes non abéliens d'ordre p^3, [F. M. 1] cor. p. 194.

(4) Groupe dérivé, existence d'un plus petit sous-groupe distingué H de G avec G/H abélien. Engendrement par les commutateurs, [Fr. E] p. 37 et [F. M. 1] $n°80$.

Plan.
A. Groupes finis (abstraits).

1. Groupes abéliens et nombre minimal de générateurs, [Fr. E] p. 100 et [F. M. 2] p. 130 et complément dans Compléments-Errata

Exercice 1

(1) Soit G un sous-groupe abélien fini de $\mathrm{GL}_n(\mathbb{C})$, alors G admet une famille génératrice de cardinal $\leq n$. C'est [F. M. 2] p. 100.

(2) En déduire que $GL_n(\mathbb{C})$ isomorphe à $GL_m(\mathbb{C})$ ssi $n = m$. Voir [F. M. 2] p. 63 pour des généralisations.

Exercice 2 Soit $H \neq \{0\}$ un sous-groupe d'un groupe abélien fini G alors le nombre minimal de générateurs de H est $\leq$ celui de G, [F. M. 2] Compléments-Errata, prop. 5 du complément à la page 130.

2. Groupe dérivé, existence d'un plus petit sous-groupe distingué H de G avec G/H abélien. Engendrement par les commutateurs, [Fr. E] p. 37 et [F. M. 1] $n°80$.

3. Sous-groupe de Frattini et nombre minimal de générateurs d'un p-groupe fini [F. M. 1] $n°76$, cas des groupes non abéliens d'ordre p^3, [F. M. 1] cor. p. 194.

Exercice 3 Variation du nombre minimal $r(G)$ de générateurs pour les groupes finis non nécessairement commutatifs, partie 3. du compléments à la page 130 dans [F. M. 2] Compléments-Errata.

Soient $H \subset G$ deux groupes finis avec $r(H) > r(G)$. On suppose que G est d'ordre minimum avec la propriété précédente. Alors G est isomorphe au groupe d'ordre 16 engendré par a, b, c et soumis aux relations $o(a) = 4$, $o(b) = o(c) = 2$, $ab = ba$, $bc = cb$ et $cac^{-1} = ab$.

4. Les groupes S_n, A_n, [Fr. E.] corollaire 2.2.1.3.5. p. 30 et [F. M. 1] $n°64$ partie 3.2. p. 155.

Exercice 4 Engendrement de S_n par les transpositions, application aux caractères de degré 1.

Exercice 5 Nombre minimal de transpositions pour engendrer S_n (3 preuves : représentations linéaires, [Fr. E.] p.28 ; combinatoire des supports, [F. M. 1] $n°62$ et avec les graphes, [F. M. 2] p.114 et Compléments et errata.

Exercice 6 Parties génératrices de S_n à 2 éléments [Fr. E] p. 30.

Exercice 7 Engendrement de A_n par les 3-cycles et application à la simplicité de A_n, [F. M. 2] p. 137.

B. Groupes issus de la géométrie.

1. Les groupes $SL_n(K)$, $GL_n(K)$, engendrement par les matrices élémentaires de transvection et les dilatations, [Fr. A] p. 113. Exercices applicatifs corrigés ci-dessous -Composantes connexes dans le cas $\mathbb{R}$ ou $\mathbb{C}$, [Fr. A.] p. 130, et à la résolution des systèmes linéaires -Application multiplicative sur les matrices, [Fr. A.] p. 93.

Exercice 8 Sur la connexité des matrices de rang r, [Fr. A.] p. 130. Exercice corrigé.

On munit $M_n(\mathbb{C})$ de sa topologie de $\mathbb{C}$-espace vectoriel de dimension finie.

(1) Montrer que $GL_n(\mathbb{C})$ est un ouvert dense dans $M_n(\mathbb{C})$.

Preuve. $\mathrm{GL}_n(\mathbb{C})$ *est l'image réciproque par l'application déterminant* $\det : M_n(\mathbb{C}) \to \mathbb{C}$ *de l'ouvert* $\mathbb{C} - \{0\}$ *de* $\mathbb{C}$. *Puisque* det *est une fonction polynôme sur* $M_n(\mathbb{C})$ *donc continue, il suit que* $\mathrm{GL}_n(\mathbb{C})$ *est ouvert dans* $M_n(\mathbb{C})$. *Enfin si* $M \in M_n(\mathbb{C})$ *le polynôme caractéristique* $\chi_M(X) := \det(XI_n - M)$ *est un polynôme unitaire de degré n, ainsi pour* $k \in \mathbb{N}$ *suffisament grand* $\chi_M(1/k) \neq 0$ *ainsi M est limite de la suite* $M - \frac{1}{k}I_n \in \mathrm{GL}_n(K)$. ///

(2) Montrer que $GL_n(\mathbb{C})$ est connexe.

Preuve. Soit $A \in \mathrm{GL}_n(\mathbb{C})$, *on va construire un chemin (continu) dans* $\mathrm{GL}_n(\mathbb{C})$ *de* I_n *à* A *ce qui montrera que la composante connexe de l'identité dans* $\mathrm{GL}_n(\mathbb{C})$ *est* $\mathrm{GL}_n(\mathbb{C})$. *Pour cela on écrit* $A = \prod_{k\in I} T_k D(\det A)$ *avec* $T_k = B_{i_k,j_k}(\lambda_k)$. *L'application* $t \in [0,1] \to \prod_{k\in I} B_{i_k,j_k}(t\lambda_k)$ *fournit un chemin continu dans* $\mathrm{GL}_n(K)$ *de* $D(\det A)$ *à* A. *Ensuite on écrit* $\det A = \rho e^{i\theta}$ *avec* $\rho \in \mathbb{R}^{>0}$ *et*

$\theta \in [0, 2\pi[$, *alors l'application* $t \in [0,1] \to D((1-t+t\rho)e^{it\theta})$ *fournit un chemin continu dans* $\mathrm{GL}_n(\mathbb{C})$ *de* I_n *à* $D(\det A)$. ///

(3) Soit $r < n$ et N_r le sous-ensemble de $M_n(\mathbb{C})$ des matrices de rang $\leq r$.

(a) Montrer que N_r est fermé dans $M_n(\mathbb{C})$.

Preuve. Une matrice $A \in N_r$ *si et seulement si ses mineurs de taille* $> r$ *sont nuls, c'est une condition fermée sur* $M_n(\mathbb{C})$ *puisque* det *est une fonction polynôme.* ///

(b) Montrer que $N_r - N_{r-1}$ est un ouvert connexe de N_r.

Preuve. D'abord $N_r - N_{r-1}$ *est un ouvert par la question précédente. Soit* $J_r := \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in N_r - N_{r-1}$ *alors* $N_r - N_{r-1}$ *est l'image continue du connexe* $\mathrm{GL}_n(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})$ *par l'application* $(P,Q) \to PJ_rQ$. ///

Exercice 9 Applications multiplicatives sur les matrices, [Fr. A.] p. 93. Exercice corrigé.

Soit K un corps commutatif et $f : M_n(K) \to K$, une application non constante avec $f(AB) = f(A)f(B)$ pour tout $A, B \in M_n(K)$. On suppose $n > 1$.

(1) Montrer que $f(I_n) = 0$ ou 1, conclure que $f(I_n) = 1$ et que $f(M) \neq 0$ pour tout $M \in \mathrm{GL}_n(K)$.

Preuve. On a $f(I_nI_n) = f(I_n)f(I_n)$, *ainsi* $f(I_n) = 0$ *ou* 1. *Si* $f(I_n) = 0$, *il suit que* $f(A) = f(AI_n) = 0$ *et donc* f *est une application constante (contradiction). Si* $M \in \mathrm{GL}_n(K)$, *alors* $1 = f(I_n) = f(M)f(M^{-1})$ *ainsi* $f(M) \neq 0$. ///

(2) Montrer que $f(0) = 0$ ou 1. En supposant que $f(0) = 1$ montrer que $f(M) = 1$ pour tout $M \in M_n(K)$. En déduire que $f(0) = 0$.

Preuve. On a $f(0) = f(0)f(0)$, *ainsi* $f(0) = 0$ *ou* 1. *On suppose que* $f(0) = 1$, *alors* $1 = f(0) = f(0M) = f(0)f(M) = f(M)$ *et* f *est une application constante (contradiction).* ///

(3) Soit $M \in M_n(K)$ avec rang de M égal $r < n$. Montrer que M est équivalente modulo $\mathrm{GL}_n(K)$ à une matrice nilpotente. Conclure que $f(M) = 0$.

Preuve. Les matrices équivalentes sont caractérisées par leur rang. Puisque $r < n$ *on peut considérer la matrice* $J_r := \sum_{1 \leq i \leq r} E_{i,i+1}$, *son image est de dimension* r *et un calcul immédiat donne* $J_r^n = 0$ *(on peut aussi utiliser Cayley-Hamilton ...). Ainsi* $M = PJ_rQ$ *avec* $P, Q \in GL_n(K)$ *et donc* $f(M) = f(P)f(J_r)f(Q) = f(J_r)$. *Mais* $f(J_r)^n = f(J_r^n) = 0$ *et donc* $f(M) = 0$. ///

(4) On veut montrer que $f(\mathrm{SL}_n(K)) = \{1\}$.

(a) Pour $\lambda \in K - \{0\}$ et $i \neq j$, on note $B_{i,j}(\lambda) := Id + \lambda E_{i,j}$. Pour σ une permutation de $\{1, ..., n\}$ on note $Q(\sigma) \in M_n(K)$ telle que $Q(\sigma)(e_i) = e_{\sigma(i)}$ où $(e_i)_i$ est la base canonique de K^n. Enfin si $\mu \in K - \{0\}$, on note $D(\mu)$ la matrice avec $D(\mu)(e_2) = \mu e_2$ et $D(\mu)(e_i) = e_i$ pour $i \neq 2$. Montrer que $Q(\sigma)E_{i,j}Q(\sigma)^{-1} = E_{\sigma(i),\sigma(j)}$ et que $D(\mu)E_{2,1}D(\mu)^{-1} = \mu E_{2,1}$. En déduire qu'il existe $P \in \mathrm{GL}_n(K)$ avec $B_{i,j}(\lambda) = PB_{2,1}(1)P^{-1}$.

Preuve. On évalue $Q(\sigma)E_{i,j}Q(\sigma)^{-1}(e_{\sigma(k)}) = Q(\sigma)E_{i,j}(e_k) = \delta_{k,j}e_{\sigma(i)}$ *et donc* $Q(\sigma)E_{i,j}Q(\sigma)^{-1} = E_{\sigma(i),\sigma(j)}$. *L'égalité* $D(\mu)E_{2,1}D(\mu)^{-1} = \mu E_{2,1}$ *est immédiate. Soit* σ *une permutation de* $\{1, ..., n\}$ *avec* $\sigma(1) = i$ *et* $\sigma(2) = j$ *(on complète par une bijection entre les complémentaires), alors* $Q(\sigma)E_{i,j}Q(\sigma)^{-1} = E_{1,2}$ *et pour* $\mu := 1/\lambda$, *on a* $D(\mu)Q(\sigma)(\lambda E_{i,j})Q(\sigma)^{-1}D(\mu)^{-1} = E_{1,2}$, *ainsi* $P = D(\mu)Q(\sigma)$ *convient. On vient ainsi de vérifier que la réduction de Jordan de* $B_{i,j}(\lambda)$ *est* $B_{2,1}(1)$. *Il suit que* $f(B_{i,j}(\lambda) = f(B_{2,1}(1))$. ///

(b) On suppose que $K \neq \mathbb{F}_2$. Montrer qu'il existe $a \in K - \{0,1\}$ avec $B_{2,1}(1) = B_{2,1}(a)B_{2,1}(1-a)$. En déduire que $f(B_{2,1}(1)) = 1$ puis que $f(\mathrm{SL}_n(K)) = \{1\}$.

Preuve. Soit $a \in K - \{0,1\}$, *alors* $B_{2,1}(a)B_{2,1}(1-a) = B_{2,1}(a+1-a) = B_{2,1}(1)$. *Ainsi avec la question précédente on déduit que* $f(B_{2,1}(1)) = f(B_{2,1}(1))^2$ *et donc* $f(B_{2,1}(1)) = 1$ *(*$B_{2,1}(1)$ *est inversible). Puisque* $\mathrm{SL}_n(K)$ *est engendré par les matrices élémentaires de transvection il suit que* $f(\mathrm{SL}_n(K)) = \{1\}$. ///

(c) On suppose que $K = \mathbb{F}_2$. Montrer que $f(B_{i,j}(\lambda)) = Id$ pour $\lambda \in K$. En déduire que $f(\mathrm{SL}_n(K)) = \{1\}$.

Preuve. Si $K = \mathbb{F}_2$, $f(B_{i,j}(\lambda)^2) = f(B_{i,j}(2\lambda)) = f(I_n) = 1$ (on utilise que la caractéristique est 2) et on conclut comme précédemment. ///

(5) Montrer qu'il existe $\rho : K^\times \to K^\times$, un homomorphisme avec $f(A) = \rho(\det(A))$ pour tout $A \in \mathrm{GL}_n(K)$.

Preuve. f induit un homomorphisme de groupes $GL_n(K) \to K^\times$, et $f(\ker \det) = f(\mathrm{SL}_n(K)) = \{1\}$, ainsi le théorème de factorisation fournit un unique homomorphisme de groupes avec $f = \rho \circ \det$. ///

Exercice 10 Application de l'engendrement de $\mathrm{SL}_n(\mathbb{F}_p)$ par les transvections élémentaires à l'engendrement de $SL_n(\frac{\mathbb{Z}}{p^a\mathbb{Z}})$ par les transvections élémentaires, [Fr. A.] ex. 2.3.19 et 20 p. 136.

2. Engendrement de $O(E)$ (E espace euclidien) par les réflexions (avec minimalité) et de $SO(E)$ par les renversements, simplicité en dimension impaire ≥ 3, [Fr. B.C.D.] p. 74.

Exercice 11 Une application d'un espace euclidien qui conserve les distances est affine car produit de réflexions, [Fr. MMG] prop. 1.4.5 p. 157

Soit E un espace affine euclidien de dimension n et f une application de E dans E qui conserve les distances. Soient $(x_0, x_1, ..., x_n)$ un repère affine de E et $y_i := f(x_i)$ pour $0 \leq i \leq n$. On veut montrer que f est un produit de réflexions (i.e. symétries orthogonales hyperplanes), en particulier $f \in Is(E)$, le groupe des isométries affines de E.

(1) Montrer par récurrence sur k l'existence de $g \in Is(E)$ qui est produit de réflexions et telle que $g(x_i) = y_i$ pour $0 \leq i \leq k$.

Preuve. Montrons cela pour $k = 0$. Si $y_0 = g(x_0)$, $g := Id_E$ convient (produit vide de réflexions) et si $y_0 \neq x_0$ soit H_0 l'hyperplan médiateur de x_0, y_0 et r_{H_0} la réflexion par rapport à H_0, alors $g := r_{H_0}$ convient.

On suppose le résultat satisfait pour $k-1$ i.e; il existe $g \in Is(E)$ avec $g(x_i) = y_i$ pour $0 \leq i \leq k-1$. On suppose que $z_k := g(x_k) \neq y_k$, Soit H_k l'hyperplan médiateur de y_k, z_k. Puisque $\|x_i - x_j\| = \|y_i - y_j\|$ pour tout i, j, il suit que $\|g(x_i) - g(x_k)\| = \|y_i - y_k\|$ pour tout $0 \leq i \leq k-1$ et donc par hypothèse de récurrence que $\|y_i - g(x_k)\| = \|y_i - y_k\|$ pour tout $0 \leq i \leq k-1$. Ainsi y_i, $0 \leq i \leq k-1$ appartient à l'hyperplan médiateur H_k de $g(y_k)$ et y_k. Soit r_{H_k} la réflexion d'hyperplan H_k alors $r_{H_k} \circ g$ convient. ///

(2) On suppose que $y_i = x_i$ pour $0 \leq i \leq n$. Montrer que $f = Id_E$.

Preuve. Soit $x \in E$ avec $y := f(x) \neq x$. Soit H l'hyperplan médiateur de x, y, alors $x_i \in H$ pour $0 \leq i \leq n$ et donc $H = E$, ce qui est une contradiction. ///

(3) Conclure.

Preuve. On a construit dans la question 2, $g \in Is(E)$ qui coïncide avec f sur le repère affine $(x_0, x_1, ..., x_n)$, alors $h := g^{-1} \circ f$ est une application qui conserve les distances et qui est l'identité sur un repère affine; c'est donc l'identité par la question précédente et donc $f = g$ est produit d'au plus n réflexions. ///

3. Réduction des endomorphismes orthogonaux et composantes connexes de $O_n(R)$, [Fr. B.C.D] p. 93.

4. Le groupe $PSL_2(\mathbb{Z}) := \frac{\mathrm{SL}_2(\mathbb{Z})}{\{\pm I_2\}}$ est engendré par $\pi(\rho), \pi(\tau)$ d'ordre respectifs 2 et 3, avec $\rho := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\tau := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et $\pi : \mathrm{SL}_2(\mathbb{Z}) \to \frac{\mathrm{SL}_2(\mathbb{Z})}{\{\pm I_2\}}$, la surjection canonique, [Se.] p.12.