UN THÉORÈME DE JORDAN REVISITÉ PAR SERRE

F. JOUVE

Introduction

L'objectif de cet exposé est de présenter une interprétation en théorie des nombres d'un théorème de Jordan portant sur les groupes de permutation. Cette transcription au cadre arithmétique, due à Serre, permet de répondre partiellement mais non trivialement à la question : si $f \in \mathbb{Z}[X]$ est irréductible, pour quelle proportion de nombres premiers p, le polynôme réduit $(f \bmod p)$ n'a t'il pas de zéro dans $\mathbb{Z}/p\mathbb{Z}$?

L'exposé suit de très près [Se]. Pour une approche élémentaire du théorème de Chebotarev (notamment concernant les substitutions de Frobenius) ainsi qu'une description du contexte historique autour de la découverte de ce résultat, on renvoie à [LS].

1. Le théorème de Jordan

Soit G un groupe agissant sur un ensemble fini X de cardianl n.

Théorème 1 (Jordan, 1872). *On suppose*

(1) $n \geqslant 2$,
(2) G *agit transitivement sur* X,

alors il existe un élément $g \in G$ *tel que* g *agisse sans point fixe sur* X.

On peut remarquer que l'on ne perd rien à supposer G fini puisque l'action $\Phi : G \to \mathrm{Sym}(X)$ induit un morphisme injectif

$$G/\ker\Phi \to \mathrm{Sym}(X)\,,$$

où $\mathrm{Sym}(X)$ désigne le groupe (fini, d'ordre $n!$) des permutations de l'ensemble X. Il suffit alors de noter qu'un élément de $G/\ker\phi$ agit sans point fixe si et seulement si un de ses relèvements agit sans point fixe.

On suppose désormais G *fini* et l'on note

$$G_0 = \{g \in G | g \text{ agit sans point fixe}\}\,.$$

On va donner la preuve d'une version "quantitative" du théorème de Jordan :

Théorème 2 (Cameron-Cohen, 1992). *Sous les mêmes hypothèses que dans le théorème 1, on a* $c_0 = |G_0|/|G| \geqslant 1/n$.

Pour prouver ce théorème, on va expoiter les 2 lemmes suivants

Lemme 1 (Burnside). *Si* G *est un groupe fini agissant sur un ensemble* X *fini alors, si l'on note* $|X^g|$ *le nombre de points fixes de* g *agissant sur* X, *on a*

$$\frac{1}{|G|}\sum_{g\in G}|X^g| = \textit{le nombre d'orbites de X sous G}$$

Démonstration. Quitte à décomposer X en réunion disjointe d'orbites, on peut supposer que G agit transitivement sur X. Le stabilisateur de tout élément de G a par conséquent même cardinalité qu'un sous groupe fixé H de G. On en déduit

$$\sum_{g\in G}|X^g| = \sum_{g\in G}\sum_{\substack{x\in X\\ g.x=x}} 1 = \sum_{x\in X}\sum_{\substack{g\in G\\ g.x=x}} 1 = \sum_{x\in X}|H| = |X||H| = |G|\,.$$

□

On en déduit facilement le

Date: 14/02/07. GdT doctorants en théorie des nombres, Bordeaux 1.

Lemme 2. *Si* $n \geqslant 2$,

$$\frac{1}{|G|}\sum_{g\in G}|X^g|^2 \geqslant 2\,.$$

Démonstration. On remarque que $|X^g|^2$ est le nombre de points fixes dans l'action diagonale de G sur $X\times X$. Ainsi, par le lemme 1, la quantité du membre de gauche est le nombre d'orbites de G agissant sur $X\times X$. Puisque $n \geqslant 2$ et que G laisse globalement invariante la diagonale de $X\times X$, il y a au moins 2 orbites dans l'action de G sur $X\times X$. □

On prouve maintenant le théorème de Cameron-Cohen :

On remarque que $G_0 = \{g\in G \,\|\, X^g| = 0\}$; ainsi, si $g\notin G_0$,

$$1 \leqslant |X^g| \leqslant n\,.$$

Donc, si $g \in G\setminus G_0$,

$$(|X^g|-1)(|X^g|-n) \leqslant 0\,;$$

puis, en sommant,

$$\sum_{g\in G\setminus G_0}(|X^g|-1)(|X^g|-n) \leqslant 0\,.$$

Autrement dit

$$\sum_{g\in G}(|X^g|-1)(|X^g|-n) \leqslant \sum_{g\in G_0}(|X^g|-1)(|X^g|-n)\,.$$

Par définition de G_0, le membre de droite vaut $n|G_0|$. Divisant les 2 membres par $|G|$, on obtient

$$\frac{1}{|G|}\sum_{g\in G}|X^g|^2-(n+1)\frac{1}{|G|}\sum_{g\in G}|X^g|+n \leqslant nc_0\,.$$

Par le lemme 2, le 1er sommant du membre de gauche est supérieur ou égal à 2 et, par le lemme 1, le second sommant est égal à $-(n+1)\times 1$ (l'action de G étant transitive). Finalement

$$2-(n+1)+n \leqslant nc_0\,,$$

d'où $c_0 \geqslant 1/n$.

Un utilisation immédiate que l'on peut faire du théorème 2 est la suivante : si G est un groupe fini et H est un sous groupe propre de G, alors G agit transitivement par multiplication à gauche sur G/H qui est de cardinalité supérieure à 2. Ainsi, par Jordan-Cameron-Cohen, il existe un élément $g \in G$ agissant sans point fixe sur G/H ; autrement dit, aucun G-conjugué de g n'est élément de H. On en déduit donc qu'il existe une classe de conjugaison de G n'intersectant pas H.

On va s'intéresser maintenant à une application plus sophistiquée due à Serre du théorème 2.

2. Une incarnation arithmétique du théorème de Jordan

2.1. **Énoncé du résultat.** Soit $f(x)=\sum_{m=0}^{n} a_m x^m \in \mathbb{Z}[x]$ un polynôme de degré n.

Théorème 3 (Serre, 2003)**.** *Supposons*

(1) $n \geqslant 2$,

(2) f *est irréductible sur* $\mathbb{Q}$,

alors, si l'on note, pour p *premier,* $N_p(f)$ *le nombre de zéros de la réduction* f_p *de* f *modulo* p *dans* $\mathbb{Z}/p\mathbb{Z}$, *l'ensemble des nombres premiers* p *tels que* $N_p(f)=0$ *admet une densité* $c_0(f)$ *supérieure à* $1/n$.

Remarque : (1) On rappelle qu'un ensemble P de nombres premiers admet une densité si le rapport

$$\frac{|\{p \text{ premier} \,|\, p\in P,\ p\leqslant X\}|}{|\{p \text{ premier} \,|\, p\leqslant X\}|}$$

admet une limite lorsque $X\to\infty$.

(2) On montre en fait (voir [Se]) que l'inégalité large $c_0(f) \geqslant 1/n$ (resp. $c_0 \geqslant 1/n$) dans le théorème de Serre (resp. dans le théorème de Cameron-Cohen) est stricte si n n'est pas une puissance d'un nombre premier.

Vue l'analogie évidente entre les hypothèses nécessaires à l'énonciation des théorèmes 2 et 3, on peut d'ores et déjà entamer la preuve du théorème 3 :

Notons $X = \{x_1, \dots, x_n\}$ l'ensemble des racines de f dans $\mathbb{C}$. Par hypothèse $|X| \geqslant 2$. Par ailleurs, le corps de décomposition $K = \mathbb{Q}(x_1, \dots, x_n)$ est galoisien sur $\mathbb{Q}$ et, si l'on note G le groupe de Galois de l'extension correspondante, alors G agit transitivement sur X, car f est irréductible sur $\mathbb{Q}$. On a alors, d'après le théorème 2 :

$$\frac{|G_0|}{|G|} \geqslant \frac{1}{n},$$

où $G_0 = \{g \in G | g \text{ agit sans point fixe sur } X\}$.

Remarquons par ailleurs que si l'on note X_p l'ensemble des réductions modulo p des éléments de X, alors X_p est l'ensemble des racines de $f_p = f \bmod p$ et le morphisme de Frobenius Fr_p agit sur cet ensemble. On sait que $N_p(f) = 0$ si et seulement si Fr_p agit sans point fixe sur X_p. Le problème consiste donc en relier l'information que l'on vient d'obtenir sur $|G_0|$ au fait que Fr_p agit ou non sans point fixe sur X_p. On veut donc construire, pour chaque p (sauf peut être un nombre fini), un élément de G qui permute les éléments de X de la même manière (au sens de la décomposition en produit de cycles disjoints) que Fr_p permute X_p.

2.2. **Substitutions de Frobenius.** On considère tout d'abord l'ensemble de "mauvais" nombres premiers

$$S = \{p \text{ premier} \,|\, p \mid a_n \text{ ou } p \mid \Delta_K\},$$

où Δ_K désigne le discriminant du corps K. *On suppose dorénavant que* $p \notin S$.

Dans l'anneau $\mathbb{Z}_K$ des entiers de K, p de décompose en produits d'idéaux premiers *distincts* :

$$p = \mathfrak{p}_1 \dots \mathfrak{p}_r .$$

On sait, d'après les résultats généraux sur les extensions galoisiennes de corps de nombres, que le groupe de Galois G agit simplement transitivement sur $\{\mathfrak{p}_i\}_i$, i.e., pour tout couple (i, j), il existe un unique élément $g \in G$ tel que

$$g.\mathfrak{p}_i = \mathfrak{p}_j .$$

Les premiers $\mathfrak{p}_i$ sont les places finies au-dessus de p ; pour conserver un sytle d'exposition élémentaire (on n'invoquera pas, par exemple, les propriétés du symbole d'Artin), on va tout d'abord donner une autre construction des places au-dessus de p. cette construction va fournir le cadre recherché pour définir ce qu'est une substitution de Frobenius.

Proposition 1. *Pour une fonction* $\psi : K \to \overline{\mathbb{F}_p} \cup \{\infty\}$, *on considère les propriétés suivantes*

- $(\dagger)$ $\widetilde{\psi} : \psi^{-1}\overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ *est un morphisme d'anneaux,*
- $(\ddagger)$ *Pour* $x \in K$, *on a* $\psi(x) = \infty$ *ssi* $\psi(x^{-1}) = 0$.

On a alors une correspondance bijective

$$\{\psi : K \to \overline{\mathbb{F}_p} \cup \{\infty\} \mid \psi \textit{ vérifie } (\dagger) \textit{ et } (\ddagger)\} \leftrightarrow \{\mathfrak{p} \subset \mathbb{Z}_K \textit{ premier} \mid \mathfrak{p}|p\}$$

Démonstration. Soit $\mathfrak{p}$ un premier de$K$ au dessus de p. On a la surjection canonique

$$(\mathbb{Z}_K)_\mathfrak{p} \to (\mathbb{Z}_K)_\mathfrak{p}/\mathfrak{p}(\mathbb{Z}_K)_\mathfrak{p}$$

et ce morphisme est à valeurs dans le corps résiduel de $\mathbb{Z}_K$ en $\mathfrak{p}$. Ce corps est isomorphe à une extension finie $\mathbb{F}_q$ de $\mathbb{F}_p$, puisque $\mathfrak{p}|p$. D'où un morphisme

$$\Theta : (\mathbb{Z}_K)_\mathfrak{p} \to \overline{\mathbb{F}_p} .$$

On définit alors une application $\psi : K \to \overline{\mathbb{F}_p} \cup \{\infty\}$, par $\psi(a/b) = \infty$ si $a/b \notin (\mathbb{Z}_K)_\mathfrak{p}$ et $\psi(x) = \Theta(x)$ sinon. L'application ainsi définie vérifie bien $(\dagger)$ et $(\ddagger)$.

Réciproquement, soit $\psi : K \to \overline{\mathbb{F}_p} \cup \{\infty\}$ une application vérifiant $(\dagger)$ et $(\ddagger)$. Le noyau $\ker \widetilde{\psi}$ du morphisme donné par $(\dagger)$ est un idéal premier de $\psi^{-1}\overline{\mathbb{F}_p}$ (en effet, $\psi^{-1}\overline{\mathbb{F}_p}/\ker\widetilde{\psi}$ s'injecte dans $\overline{\mathbb{F}_p}$). Notons $\mathfrak{p}$ l'idéal $\ker\widetilde{\psi} \cap \mathbb{Z}_K$ de $\mathbb{Z}_K$. C'est un idéal premier de $\mathbb{Z}_K$. En effet, si $x, y \in \mathbb{Z}_K$ sont tels que $\widetilde{\psi}(xy) = 0$, alors, si $x, y \in \psi^{-1}\overline{\mathbb{F}_p}$, on en déduit $\widetilde{\psi}(x) = 0$ ou $\widetilde{\psi}(y) = 0$. Si x ou y (disons x) n'est pas élément de $\psi^{-1}\overline{\mathbb{F}_p}$, alors $\psi(x) = \infty$ et, par $(\ddagger)$, on déduit $\psi(x^{-1}) = 0$. Ainsi

$$\psi((xy) \times x^{-1}) = \widetilde{\psi}(xy)\widetilde{\psi}(x^{-1}) = 0 ,$$

d'où $\psi(y) = \widetilde{\psi}(y) = 0$.

Il suffit alors de montrer que $\mathfrak{p}$ est au-dessus de p. Considérons pour cela $\mathfrak{p} \cap \mathbb{Z} = \ker\widetilde{\psi} \cap \mathbb{Z}$, c'est un idéal de $\mathbb{Z}$ contenant $p\mathbb{Z}$ car $\psi(p) = 0$. Mais $\ker\widetilde{\psi} \cap \mathbb{Z}$ est inclus dans $p\mathbb{Z}$ car l'image par ψ de $\ker\widetilde{\psi} \cap \mathbb{Z}$ est nulle dans $\overline{\mathbb{F}_p}$. Ainsi $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Le fait que les 2 applications ainsi définies soient réciproques l'une de l'autre permet de conclure la preuve de la proposition. $\square$

Puisque G agit simplement transitivement sur $\{\mathfrak{p}_i\}_i$, la correspondance donnée par la proposition précédente permet de définir une action (elle aussi simplement transitive) de G sur l'ensemble des fonctions vérifiant (†) et (‡) : pour ψ une telle fonction et $g \in G$,

$$g.\psi = \psi \circ g\,.$$

Soit maintenant $\mathfrak{p}|p$ un idéal premier de $\mathbb{Z}_K$ au-dessus de p. Par la proposition précédente, cela équivaut à la donnée d'une fonction $\psi : K \to \overline{\mathbb{F}_p} \cup \{\infty\}$ vérifiant (†) et (‡). L'application $\mathrm{Fr}_p \circ \psi$ est également définie sur K, à valeurs dans $\overline{\mathbb{F}_p} \cup \{\infty\}$ et vérifie (†) et (‡) (en posant $\mathrm{Fr}_p(\infty) = \infty$). Ainsi, par simple transitivité de l'action de G sur l'ensemble formé de telles fonctions, *il existe un unique* $g_\psi \in G$ tel que

$$\mathrm{Fr}_p \circ \psi = \psi \circ g_\psi\,. \tag{1}$$

L'élément g_ψ dépend a priori du choix d'une place ψ au-dessus de p. Explicitons cette dépendance : si $\psi' = \psi \circ \tau$ est une autre place au-dessus de p, on a pour tout $x \in K$,

$$\mathrm{Fr}_p(\psi \circ \tau(x)) = \psi \circ \tau \circ g_{\psi\circ\tau}(x)\,.$$

Appliquant cette formule en $\tau^{-1}(x)$, on obtient

$$\mathrm{Fr}_p(\psi(x)) = \psi \circ \tau \circ g_{\psi\circ\tau} \circ \tau^{-1}(x)\,.$$

D'où $\mathrm{Fr}_p(\psi(x)) = \psi \circ \tau \circ g_{\psi\circ\tau} \circ \tau^{-1}(x)$, puis

$$\psi \circ g_\psi = \psi \circ \tau \circ g_{\psi\circ\tau} \circ \tau^{-1}\,.$$

L'action de G sur les places au-dessus de p étant simple, on en déduit $g_\psi = \tau \circ g_{\psi\circ\tau} \circ \tau^{-1}$; ainsi, si un élément g_ψ dépend du choix de ψ, la classe de G-conjugaison σ_p de g_ψ ne dépend elle que du nombre premier p.

Définition 1. *La classe de conjugaison σ_p est appelée substitution de Frobenius en p.*

2.3. **Fin de la preuve du théorème 3.** La propriété (1) nous permet d'affirmer que tout représentant de la classe de conjugaison σ_p permute X "de la même façon" (au sens de la longueur des cycles composant ces permutations) que Fr_p permute X_p. Or le fait que Fr_p agit sans point fixe sur X_p (i.e. f_p n'admet pas de racine dans $\mathbb{Z}/p\mathbb{Z}$) peut se lire sur la décomposition en produit de cycles disjoints de Fr_p agissant sur X_p. La prtie G_0 de G étant stable par conjugaison, on peut en conclure que

$$f_p \text{ n'a pas de racine dans } \mathbb{Z}/p\mathbb{Z} \text{ ssi } \sigma_p \in G_0\,.$$

Pour terminer la preuve du théorème 3, il nous suffit d'utiliser le merveilleux

Théorème 4 (Chebotarev)**.** *Soient* C *une partie de* G *stable par conjugaison et* S *un ensemble fini de nombres premiers. Si l'on note* $P_{C,S} = \{p \text{ premier} \mid p \notin S \text{ et } \sigma_p \in C\}$*, alors* $P_{C,S}$ *admet une densité égale à* $|G_0|/|G|$.

D'après ce qui précède et la fin de la section 2.1, l'ensemble $\{p \notin S \mid N_p(f) = 0\}$ admet, par le théorème de Chebotarev, une densité égale à $|G_0|/|G| \geqslant 1/n$; ce qui achève la preuve du théorème 3.

On trouvera dans [LS] l'essentiel des idées de la preuve du théorème de Chebotarev (voir [M], page 126, pour un exposé plus complet de la preuve). Pour conclure sur l'importance et la beauté de ce dernier théorème, on ne résiste pas à l'envie d'en donner une autre application, très classique cette fois.

Soit $K = \mathbb{Q}(\zeta_m)$ le corps cyclotomique pour un entier $m \geqslant 1$. On sait que $K/\mathbb{Q}$ est une extension galoisienne de groupe $G = (\mathbb{Z}/m\mathbb{Z})^*$. L'extension $K/\mathbb{Q}$ est donc abélienne ce qui permet de parler de σ_p comme d'un *élément* de G. Soit a l'entier premier à m tel que

$$\sigma_p(\zeta_m) = \zeta_m^a\,.$$

Soit p premier ne divisant pas m (et donc, ne divisant pas Δ_K).D'après (1), on a, en notant $\eta =$ "$\zeta_m \bmod p$" la racine primitive m-ième de 1 dans $\overline{\mathbb{F}_p}$ image de ζ_m par une place ψ au-dessus de p,

$$\mathrm{Fr}_p(\eta) = \eta^a\,,$$

puis $\eta^p = \eta^a$ d'où $p \equiv a \bmod m$. Donc, d'après le théorème de Chebotarev, $\{p \text{ premier} \mid p \nmid m, p \equiv a \bmod m\}$ admet une densité égale à $1/\phi(m)$. On a ainsi déduit le théorème de la progression arithmétique de Dirichlet du théorème de Chebotarev.

Références

[M] Milne, J. : *Algebraic number theory*, `http://www.jmilne.org/math/`

[LS] Stevenhagen, P., Lenstra, H. W., Jr. : *Chebotarev and his density theorem*, Math. Intelligencer 18 (1996), no. 2, 26-37. `http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf`

[Se] Serre, J. P. : *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) 40 (2003), no. 4, 429-440. `http://www.math.mcgill.ca/goren/SeminarOnCohomology/Serre.pdf`