École Normale Supérieure, Année 2019-2020

1^{e} année, Algèbre 1

TD n° 6 : La méthode d'Iwasawa

Le but de cette note est de montrer un critère dû à Iwasawa qui permet d'établir la simplicité de certains groupes et d'en déduire le théorème suivant :

Théorème 1. *Les deux familles infinies de groupes finis suivants sont simples :*
- *les groupes* $\mathrm{PSL}_n(K)$*, sauf pour l'entier* $n = 2$ *et les corps* $K = \mathbb{F}_2$ *et* $K = \mathbb{F}_3$*,*
- *les groupes* $\mathfrak{A}_n$ *pour* $n \geqslant 5$*.*

Les deux premiers paragraphes sont essentiellement tirés du polycopié de O. Debarre, utilisé pour le cours d'Algèbre 1 à l'ENS.

0.1 Le critère d'Iwasawa

Le critère utilise la notion *d'action primitive* dont la définition est la suivante :

Définition 2. *Soit* G *un groupe agissant sur un ensemble* X*. On dit que l'action est* primitive *si elle est transitive et si pour tout* $x \in X$ *le stabilisateur* G_x *est un sous-groupe maximal de* G*, i.e. tout sous-groupe strict de* G *contenant* G_x *est égal à* G_x*.*

En pratique, on rencontrera des actions 2-transitives. On rappelle que l'action d'un groupe G sur un ensemble X est 2 transitive si pour tout $x_1, x_2, y_1, y_2 \in X$ tel que $x_1 \neq x_2$ et $y_1 \neq y_2$ il existe $g \in G$ tel que $g \cdot x_1 = y_1$ et $g \cdot x_2 = y_2$. De manière équivalente si on pose

$$X^2_{\mathrm{reg}} = \{(x_1, x_2) \in X^2 \mid x_1 \neq x_2\},$$

l'ensemble des *paires régulières* de X, l'action de G sur X est 2-transitive si et seulement si l'action diagonale de G sur X^2_{reg} est transitive. Le lemme suivant assure que les actions 2-transitives sont primitives :

Lemme 3. *Soit* G *un groupe qui agit* 2*-transitivement sur un ensemble* X*. Alors cette action est primitive.*

Démonstration. Par définition l'action est transitive, il suffit donc de montrer que les stabilisateurs sont maximaux. Soit $x \in X$ et G_x son stabilisateur. Soit $g \in G \backslash G_x$, montrons que le sous-groupe engendré par G_x et g contient G, ce qui montrera que G_x est maximal.

Soit $h \in G \backslash G_x$. On note $y = g \cdot x$ et $z = h \cdot x$. Alors par définition $z, y \neq x$, donc comme l'action est 2-transitive il existe $k \in G$ tel que $k \cdot (x, z) = (k \cdot x, k \cdot z) = (x, y)$. Comme $k \cdot x = x$ on a $k \in G_x$ et comme $k \cdot z = k \cdot (h \cdot x) = (kh) \cdot x = g \cdot x$ on en déduit que $g^{-1}kh \in G_x$. Ainsi

$$h = \underbrace{k^{-1}}_{\in G_x} g \underbrace{g^{-1}kh}_{\in G_x} \in \langle g, G_x \rangle.$$

Ainsi le sous-groupe engendré par G_x et g contient $G \backslash G_x$ et donc contient G tout entier. □

La réciproque est fausse : considérer l'action naturelle de $\mathfrak{S}_n$ sur les sous-ensembles à 2-éléments de $\{1, \dots, n\}$. On montre maintenant le *critère d'Iwasawa* :

Proposition 4. *Soit* G *un groupe qui agit primitivement sur un ensemble* X*. On se donne pour tout* $x \in X$ *un sous-groupe abélien* T_x *de* G *tel que*
- *pour tout* $g \in G$*,* $T_{g \cdot x} = g T_x g^{-1}$*,*
- *la réunion* $\bigcup_{x \in X} T_x$ *engendre* G*.*

Alors tout sous-groupe distingué de G *qui agit non-trivialement sur* X *contient* $D(G)$*, le sous-groupe dérivé de* G

Démonstration. Soit H un sous-groupe distingué de G agissant non-trivialement sur X. On veut montrer que G/H est abélien car alors par la propriété universelle du sous-groupe dérivé $D(G)$ on aura $D(G) \subset H$.

Soit $x \in X$, comme l'action est primitive $G_x \subset G$ est un sous-groupe maximal et donc $HG_x = G$ ou $HG_x = G_x$. Montrons que $HG_x = G$ par l'absurde, supposons que $HG_x = G_x$. Alors $H \subset G_x$ et donc pour tout $g \in G$ comme H est distingué on a

$$H = gHg^{-1} \subset gG_xg^{-1} = G_{g\cdot x}.$$

Comme l'action de G sur X est transitive on en déduit que H est contient tous les stabilisateurs de X et donc que H agit trivialement sur X ce qui est une contradiction. Ainsi $HG_x = G$.

On en déduit que l'action de H sur X est en faite transitive. En effet soit $x \in X$ alors comme l'action de G sur X est transitive

$$X = G \cdot x = HG_x \cdot x = H \cdot x.$$

ce qui montre bien que l'action de H sur X est transitive.

Soit $x \in X$ montrons que $G = HT_x$. En effet pour tout $h \in H$ on a

$$T_{h\cdot x} = hT_xh^{-1} \subset HT_xH = HT_x$$

où la dernière égalité s'obtient en utilisant que H est distingué dans G. Comme l'action de H sur X est transitive on en déduit que HT_x contient tout les T_y pour $y \in X$. Or comme l'ensemble des T_y engendre G et que HT_x est un groupe car H est distingué on en déduit que $G = HT_x$.

Pour conclure il suffit de montrer que G/H est abélien. En effet

$$G/H = HT_x/H \cong T_x/(H \cap T_x).$$

Or T_x est abélien donc G/H aussi, ce qui montre bien le critère. □

0.2 Simplicité des $\mathrm{PSL}_n(K)$

On applique maintenant ce critère pour montrer la première partie du théorème 1. Les deux cas exceptionnels sont les suivants :

$$\mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3,\ \mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4.$$

Or $\mathfrak{S}_3$ n'est pas simple car les 3-cycles forment un sous-groupe distingué non trivial et $\mathfrak{A}_4$ n'est pas simple car les doubles transpositions forment un sous-groupe distingué non-trivial. La conclusion repose sur le critère d'Iwasawa et le lemme suivant :

Lemme 5. *On a*

$$D(\mathrm{PSL}_n(K)) = \mathrm{PSL}_n(K),$$

sauf si $n = 2$ et $K = \mathbb{F}_2$ ou $\mathbb{F}_3$.

Démonstration. Il suffit de prouver le résultat analogue pour $\mathrm{SL}_n(K)$. Soit i, j deux entiers distincts tels que $1 \leqslant i, j \leqslant n$. On note $E_{i,j}$ la matrice élémentaire usuelle, alors les *matrices de transvection* $\mathrm{Id}_n + \alpha E_{i,j}$ pour $\alpha \in K$ engendrent $\mathrm{SL}_n(K)$; c'est essentiellement le pivot de Gauss. Il suffit donc d'écrire une matrice de transvection comme un commutateur.

On suppose que $n \geqslant 3$. Alors pour trois indices distincts i, j, k et $\alpha, \beta \in K$ on a la relation des commutateurs suivante

$$(\mathrm{Id}_n + \alpha\beta E_{i,k}) = [\mathrm{Id}_n + \alpha E_{i,j}, \mathrm{Id}_n + \beta E_{j,k}]$$

qui se vérifie par le calcul en utilisant que $(\mathrm{Id}_n + \alpha E_{i,j})^{-1} = \mathrm{Id}_n - \alpha E_{i,j}$. Ceci prouve le lemme pour $n \geqslant 3$.

On suppose $n = 2$ et que K n'est ni $\mathbb{F}_2$ ni $\mathbb{F}_3$. Ceci nous permet de choisir $\beta \in K$ tel que $\beta \neq 0, 1, -1$. Soit $\alpha \in K$, La relation des commutateurs que l'on veut est alors

$$\mathrm{Id}_2 + \alpha E_{1,2} = \left[\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \frac{\alpha}{\beta^2 - 1} \\ 0 & 1 \end{pmatrix}\right].$$

Ceci permet de conclure dans le cas $n = 2$. □

On cherche maintenant à appliquer le critère d'Iwasawa : on pose $X = \mathbb{P}^{n-1}(K)$ l'espace projectif sur K. On rappelle que l'action de $\mathrm{PSL}_n(K)$ sur $X = \mathbb{P}^{n-1}(K)$ est bien 2-transitive et donc primitive par le lemme 3. Pour $x \in \mathbb{P}^{n-1}(K)$ une droite de K^n on définit T_x comme l'ensemble des transvections de droite directrice x. Plus précisément, pour a un vecteur non-nul de la droite x, $l\colon K^n \to K$ une forme linéaire qui s'annule sur x on pose $t_{a,l}\colon v \to v + l(v)a$ comme automorphisme de K^n. Il définit donc un élément de $\mathrm{PSL}_n(K)$ que l'on note de la même façon. Alors on pose

$$T_x = \{t_{a,l} \in \mathrm{PSL}_n(K); a \in x, l\colon K^n \to K\}.$$

Montrons que ces ensembles vérifies les hypothèses du critère :

- Soit $g \in \mathrm{PSL}_n(K)$. Alors on vérifie par le calcul que pour $x \in \mathbb{P}^{n-1}(K)$, $a \in x$ et $l\colon K^n \to K$ tel que $l(a) = 0$ on a
$$g \circ t_{a,l} \circ g^{-1} = t_{l \circ g^{-1}, g \cdot a} \in T_{g \cdot x},$$
ce qui montre bien que $gT_x g^{-1} = T_{g \cdot x}$.
- On a déjà utilisé que les transvections engendrent $\mathrm{SL}_n(K)$ dans la preuve du lemme 5, qui, on le rappelle, provient essentiellement du pivot de Gauss. Ainsi, la réunion des T_x pour x parcourant $\mathbb{P}^{n-1}(K)$ engendre bien $\mathrm{PSL}_n(K)$ ce qui vérifie la deuxième hypothèse.

On est maintenant en mesure de conclure sur la simplicité de $\mathrm{PSL}_n(K)$. On se place dans les hypothèses du lemme 5. Soit H un sous-groupe distingué non-trivial de $\mathrm{PSL}_n(K)$. Alors H agit non-trivialement sur $\mathbb{P}^{n-1}(K)$ car l'action de $\mathrm{PSL}_n(K)$ sur l'espace projectif est fidèle. Ainsi le critère d'Iwasawa assure que $D(\mathrm{PSL}_n(K)) \subset H$ et donc le lemme 5 assure que $H = \mathrm{PSL}_n(K)$, ce qui termine la preuve de la simplicité.

0.3 Simplicité des $\mathfrak{A}_n$

On applique maintenant le critère pour montrer la deuxième partie du théorème 1, la simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$. Dans les autres cas on a

$$\mathfrak{A}_2 \cong \{e\},\ \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z},\ \mathfrak{A}_4 \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z},$$

donc seulement $\mathfrak{A}_3$ est simple mais commutatif. Il est intéressant de voir que le même critère va fonctionner, essentiellement en remplaçant les transvections par les 3-cycles. Dans toute la suite on supposera un entier fixé $n \geqslant 5$.

Lemme 6. *Le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles.*

Démonstration. On sait que $\mathfrak{S}_n$ est engendré par les transpositions. Or un produit de transposition est contenu dans $\mathfrak{A}_n$ si et seulement si c'est un produit d'un nombre paire de transposition, i.e. d'un produit de double transpositions. Ainsi $\mathfrak{A}_n$ est engendré par les paires de transpositions. Soit $a, b, c, d \in \{1, \dots, n\}$ tous distincts (ce qui est possible car $n \geqslant 5$), alors on a les relations de produit de transpositions à 3-cycles suivantes

$$(a\ b)(b\ c) = (a\ b\ c),\ (a\ b)(c\ d) = (a\ b\ c)(b\ c\ d),$$

Ce qui permet d'écrire tout produit d'un nombre paire de transposition comme un produit de 3-cycles, donc $\mathfrak{A}_n$ est engendré par les 3-cycles □

On doit maintenant montrer que $\mathfrak{A}_n$ est égal à son commutateur :

Lemme 7. *Soit $n \geqslant 5$, alors*

$$D(\mathfrak{A}_n) = \mathfrak{A}_n.$$

Démonstration. Par le lemme précédent il suffit de montrer que $D(\mathfrak{A}_n)$ contient tous les 3-cycles. Or $D(\mathfrak{A}_n)$ est un sous-groupe distingué de $\mathfrak{A}_n$ et tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$ (car comme $n \geqslant 5$, il commute à une transposition dans $\mathfrak{S}_n$), donc pour qu'il contienne tous les 3-cycles il suffit de montrer qu'il contient un 3-cycle disons $(1\ 2\ 4)$. Or on a la relation de commutateurs suivante

$$(1\ 2\ 4) = [(1\ 2\ 3), (1\ 2\ 3\ 4\ 5)]\,,$$

ce qui conclut la preuve. □

On cherche maintenant à appliquer le critère. Soit $X = \{1, 2 \ldots, n\}^3_{\text{reg}}$ l'ensemble des triplets d'entiers distincts entre 1 et n. L'action diagonale de $\mathfrak{A}_n$ sur X est 2-transitive et donc primitive par le lemme 3. Pour $x = (a, b, c) \in X$ on pose T_x le sous-groupe de $\mathfrak{A}_n$ engendré par le 3-cycle $(a\ b\ c)$. Ces ensembles vérifient les hypothèses du critères :

- Soit $\sigma \in \mathfrak{A}_n$ et $x = (a, b, c) \in X$. On a la relation usuelle de commutation $\sigma(a\ b\ c)\sigma^{-1} = (\sigma(a)\ \sigma(b)\ \sigma(c))$, ce qui assure que $\sigma T_x \sigma^{-1} = T_{\sigma \cdot x}$.
- On a montré au lemme 6 que $\mathfrak{A}_n$ est engendré par les 3-cycles et donc engendré par la réunion des T_x quand x parcourt X.

On est maintenant en mesure de conclure sur la simplicité de $\mathfrak{A}_n$. L'action de $\mathfrak{A}_n$ sur X est fidèle, donc pour H un sous-groupe distingué non-trivial de $\mathfrak{A}_n$, il agit non-trivialement sur X. Donc $D(\mathfrak{A}_n) \subset H$ et par le lemme 7 on conclut que $H = \mathfrak{A}_n$, ce qui termine la preuve de la simplicité de $\mathfrak{A}_n$.