Groupes linéaires

Mahmoud Goual Abderrafie Mounadim

23 mai 2017

Le but de ce projet est de montrer que *les groupes linéaires de type fini* (groupes engendrés par un ensemble fini de matrices inversibles, que l'on prendra à coefficients dans $\mathbb{C}$) sont*résiduellement finis*. Pour celà on commencera par voir si $\mathrm{GL}_d(R)$ est résiduellement fini (avec $R = \mathbb{Z}, \mathbb{Z}[\frac{1}{r}], \mathbb{Z}[X_1, \ldots, X_n], \mathbb{Z}[X_1, \ldots, X_n, \frac{1}{f}]$). Dans la deuxième partie on utlisera les proprités des extensions des corps pour montrer la finitude résiduelle des groupes linéaires de type fini.

Définition :
Un groupe G est dit résiduellement fini si pour tout $g \in G$ tel que $g \neq 1_G$ il existe un groupe fini F et un homomorphisme $\Phi : G \to F$ tel que $\Phi(g) \neq 1_F$.

1 Finitude résiduelle des groupes $\mathrm{GL}_d(R)$

Soit $d \geq 2$;

Théorème 1 :
Si $\varphi : R \to S$ est un morphisme d'anneaux unitaires alors l'application $\Phi : \mathrm{GL}_d(R) \to \mathrm{GL}_d(S)$ définie par $\Phi((a_{ij})_{1\leq i,j\leq d}) = (\varphi(a_{ij}))_{1\leq i,j\leq d}$ est un morphisme de groupe.

Preuve :
Soient $A, B \in \mathrm{GL}_d(R)$ avec $A = (a_{ij})_{i,j}$ et $B = (b_{ij})_{i,j}$
Posons $C = A \times B$ donc $C = (c_{ij})_{i,j}$ avec $c_{ij} = \sum_{k=1}^{d} a_{ik}b_{kj}$.
On a $\Phi(A \times B) = \Phi(C) = \varphi((c_{ij}))_{i,j} = (\varphi(\sum_{k=1}^{d} a_{ik}b_{kj}))_{i,j}$. Or on sait que φ est un morphisme d'anneau de R dans S donc :

$$\varphi(\sum_{k=1}^{d} a_{ik}b_{kj}) = \sum_{k=1}^{d} \varphi(a_{ik})\varphi(b_{kj}), \forall i, j \in \{1, ..., d\} \qquad (*)$$

On pose $D = (d_{ij})_{i,j}$ avec $d_{ij} = \varphi(\sum_{k=1}^{d} a_{ik}b_{kj}), \forall i, j \in \{1, ..., d\}$ et $e_{ik} = \varphi(a_{ik})$ et $f_{kj} = \varphi(b_{kj})$ $\forall i, k, j \in \{1, ..., d\}$ donc $E = (e_{ij})_{i,j} = (\varphi(a_{ij})_{i,j})$ et $F = (f_{ij})_{i,j} = (\varphi(b_{ij})_{i,j})$ et d'après $(*)$ $D = E \times F$ d'où

$$\Phi(A \times B) = \Phi(A) \times \Phi(B).$$

Donc Φ est un morphisme de groupe de $\mathrm{GL}_d(R)$ dans $\mathrm{GL}_d(S)$.

1.1 $\mathbb{Z}$ est résiduellement fini.

Soit $n \in \mathbb{Z}$ tel que $n \neq 0$ et p ne divise pas n. On pose :
$\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ (c'est un morphisme de groupe)
$k \mapsto \bar{k}$
et on a $\varphi(n) \neq \bar{0}$ car p ne divise pas n. Donc $\mathbb{Z}$ est résiduellement fini.

1.2 $\mathrm{GL}_d(\mathbb{Z})$ est résiduellement fini.

Soit $A \in \mathrm{GL}_d(\mathbb{Z})$ tel que $A \neq Id$. En posant $A = (a_{ij})_{i,j}$ on a :

$$\exists (i,j) \in (\{1,...,d\})^2 \text{ tels que } i \neq j \text{ et } a_{ij} \neq 0.$$

$$A = \begin{pmatrix} a_{1,1} & \cdots & \cdots & a_{1,n} \\ \vdots & \ddots & a_{i,j_{i\neq j}} & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n} \end{pmatrix}$$

Soit $p \in \mathbb{Z}$ tel que p ne divise pas a_{ij} donc $a_{ij} \neq 0[p]$ et soit $\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ un morphisme d'anneau $k \mapsto k \pmod p$.

Par le théorème précédent $\Phi : \mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$ définie par $\Phi(A) = \Phi((a_{ij})_{i,j}) \mapsto (\varphi(a_{ij}))_{i,j}$ est un morphisme de groupe.

Donc pour le a_{ij} que l'on a choisit on $\varphi(a_{ij}) \neq 0$

$$\Phi(A) = \begin{pmatrix} \bar{a_{1,1}} & \cdots & \cdots & \bar{a_{1,n}} \\ \vdots & \ddots & \bar{a_{i,j}} \neq 0 & \vdots \\ \vdots & \cdots & \ddots & \vdots \\ \bar{a_{n,1}} & \cdots & \cdots & \bar{a_{n,n}} \end{pmatrix}$$

D'où $\Phi(A) \neq Id$, d'où $\mathrm{GL}_d(\mathbb{Z})$ est résiduellement fini.

1.3 $\mathbb{Z}[\frac{1}{r}]$ est résiduellement fini.

On pose $\varphi : \mathbb{Z}[\frac{1}{r}] \to \mathbb{Z}/p\mathbb{Z}$ tel que $x \times r^k = a[p]$
$\alpha = \frac{a}{r^k} \mapsto \bar{x}$

On prend p premier qui ne divise pas r. Soit $\alpha \in \mathbb{Z}[\frac{1}{r}]$ tel que $\alpha \neq 0$ c'est à dire $a \neq 0$.

On sait que p premier et ne divise pas r donc $p \wedge r = 1$ et donc par récurrence immédiate et par le théorème de Gauss on a $\forall k \in \mathbb{N}^*$, $p \wedge r^k = 1$ en appliquant le théorème de Bezout il vient $\exists u, v \in \mathbb{Z}$ tel que :
$pu + r^k v = 1$

d'où $pua + r^k va = a$ en posant $x = va$ il vient donc :

$$\begin{aligned} pua + xr^k = a &\Rightarrow xr^k = -pua + a \\ &\Rightarrow x \times \frac{r^k}{a} = -pu + 1 \\ &\Rightarrow x \times \frac{1}{\alpha} = -pu + 1 \\ &\Rightarrow x = \alpha - pu\alpha \\ &\Rightarrow x = \alpha[p] \end{aligned}$$

Mais $x = va$ et on a $v \neq 0$ et $a \neq 0$ sinon $pu = 1 \Rightarrow p = \pm 1$ absurde car p premier donc $\bar{x} = \bar{\alpha}$ donc $\mathbb{Z}[\frac{1}{r}]$ est résiduellement fini.

On a donc montré que $\mathbb{Z}[\frac{1}{r}]$ est résiduellement fini.

1.4 $\mathrm{GL}_d(\mathbb{Z}[\frac{1}{r}])$ est résiduellement fini.

Soit $\Phi : \mathrm{GL}_d(\mathbb{Z}[\frac{1}{r}]) \to \mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$ définie par $\Phi(A) = \Phi((a_{ij})_{i,j}) \mapsto (\varphi(a_{ij}))_{i,j}$ qui est un morphisme de groupe d'après le théorème précédent.

Soit $A \neq Id$ et soit $a_{ij} \neq 0$ tq $i \neq j$ on pose $a_{ij} = \alpha = \frac{a}{r^k}$ et pour $p \wedge r = 1$ on trouve $\bar{a_{ij}} = \bar{\alpha} \neq \bar{0}$ comme pour $\mathbb{Z}[\frac{1}{r}]$ donc $\Phi(A) \neq Id$ donc $\mathrm{GL}_d(\mathbb{Z}[\frac{1}{r}])$ est résiduellement fini.

1.5 $\mathbb{Z}[X_1, ..., X_n]$ est résiduellement fini.

1.5.1 Exemple : $\mathbb{Z}[X]$.

Soit $P = \sum_k a_k X^k \in \mathbb{Z}[X]$ non nulle c'est à dire $\exists k$ tel que $a_k \neq 0$ et soit p un nombre premier tel que $p > max_k(|a_k|)$.

On a donc $Q = \sum_k \bar{a_k} X^k \in \mathbb{F}_p[X]$ non nul car pour tout $a_k \neq 0$, $\bar{a_k}$ est non nul. On prend le morphisme $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ definie par $\varphi : P = \sum_k a_k X^k \mapsto Q = \sum_k \bar{a_k} X^k$

Maintenant supposons que le degré de P est $m \in \mathbb{N}$, soit $q = p^n$ avec $m \in \mathbb{N}$ tel que $q > m$.

On sait que $Card(\mathbb{F}_q) = q > m$, donc on peut trouver un élément a de $\mathbb{F}_q = \mathbb{F}_p[a]$ tel que $Q(a) = \sum_k \bar{a_k} a^k \neq 0$, car Q admet au plus, m racines. Donc on considère le morphisme :

$\Psi : \mathbb{F}_p[X] \to \mathbb{F}_q = \mathbb{F}_p[a]$

$Q = \sum_k \bar{a_k} X^k \mapsto \sum_k \bar{a_k} a^k$

et on a $\Phi = \Psi \circ \varphi$ on a donc

$\Phi : \mathbb{Z}[X] \to \mathbb{F}_q$ définie par $\Phi : P = \sum_k a_k X^k \neq 0 \mapsto \sum_k \bar{a_k} a^k \neq 0$

donc on a construit un morphisme d'anneau qui va de $\mathbb{Z}[X]$ dans $\mathbb{F}_q$ qui est un corps fini tel que pour le polynome P en question l'image par Φ n'est pas l'identité dans $\mathbb{F}_q$. Finalement $\mathbb{Z}[X]$ est résiduellement fini.

Montrons que $\mathrm{GL}_n(\mathbb{Z}[X])$ est résiduellement fini :

Soit $f : \mathrm{GL}_n(\mathbb{Z}[X]) \to \mathrm{GL}_n(\mathbb{F}_q)$

$A = (p_{ij})_{i,j} \mapsto B = (\Phi(p_{ij}))_{i,j}$

Si $A = (p_{ij})_{i,j} \in \mathrm{GL}_n(\mathbb{Z}[X])$ différent de l'identité dans $\mathrm{GL}_n(\mathbb{Z}[X])$ alors $\exists$ au moins un polynome $p_{ij} \neq 0$ tel que $i \neq j$

donc $B = (\Phi(p_{ij}))_{i,j} \neq 0$ d'où $\mathrm{GL}_n(\mathbb{Z}[X])$ est résiduellement fini.

1.5.2 $A[X]$ est résiduellement fini

Lemme :

Soit A un anneau résiduellement fini. Alors $A[X]$ est aussi résiduellement fini.

Preuve :

A est un anneau résudiellement fini admettant donc des morphismes d'anneaux unitaires $\varphi_n : A \to R_n$ avec R_n des anneaux finis, et tels que pour tout $g \in A$, $g \neq 0_A$ on a $\varphi_n(g) \neq 0_{R_n}$ pour n assez grand). En plus de celà R_n sont des corps finis.
Soit $P \in A[X]$ c'est à dire $P = \sum_k a_k X^k$ avec $a_k \in A$, pour tout k, tel que $P \neq 0$, c'est à dire $\exists k \in \mathbb{N}$ tel que $a_k \neq 0$.
On considère le morphisme d'anneau :

$\Psi : A[X] \to R_n[X]$
$P = \sum_k a_k X^k \mapsto Q = \sum_k \varphi(a_k) X^k$
En effet :(explication de l'existence de φ)

Puisque $P \neq 0$, donc $\exists k \in \mathbb{N}$ tel que $a_k \neq 0$ et donc il existe forcement un morphisme $\varphi : A \to R_n$ qui à $g \mapsto \varphi_n(g)$ tel que $\varphi_n(a_k) \neq 0$ donc $Q \neq 0$.

Maintenant supposons que le degré du polynome Q est $m \in \mathbb{N}$.
Soit $\mathbb{F}_q$ un corps fini de cardinal q tel que $m < q$. Q est de degré m, donc admet au plus m racines, et donc il existe bien un élément $a \in \mathbb{F}_q$ tel que $Q(a) \neq 0$.
Donc on considère le morphisme :
$\delta : R_n[X] \to \mathbb{F}_q$
$Q = \sum_k \varphi(a_k) X^k \mapsto Q(a) = \sum_k \varphi(a_k) a^k \neq 0$

Finalement on considère le morphisme $\Phi = \delta \circ \Psi$

$\Phi : A[X] \to \mathbb{F}_q$
$P = \sum_k a_k X^k \mapsto Q(a) = \sum_k \varphi(a_k) a^k$

Donc pour le $P \in A[X]$ fixé non nul, il existe un corps fini $R_n$un morphisme Φ qui va de $A[X] \mapsto \mathbb{F}_q$ tel que $\Phi(P)$ n'est pas l'identité.

Donc $A[X]$ est résiduellement fini.

1.5.3 $\mathbb{Z}[X_1, ..., X_k]$ est résiduellement fini

Montrons qu'il est résiduellement fini par récurrence sur n.

Pour $n = 1$, d'après l'exemple précédent $\mathbb{Z}[X_1]$ est résiduellement fini.

Supposons que $\mathbb{Z}[X_1, ..., X_k]$ est résiduellement fini pour k allant de 1 jusqu'à $n - 1$.

Montrons que $\mathbb{Z}[X_1, ..., X_n]$ est résiduellement fini pour tout n entier.

Soit $n \in \mathbb{N}$

On sait que $\mathbb{Z}[X_1, ..., X_n] = (\mathbb{Z}[X_1, ..., X_{n-1}])[X_n]$ et d'après l'hypothèse de récurrence $\mathbb{Z}[X_1, ..., X_{n-1}]$ est résiduellement fini, donc par le lemme déjà montrer $A[X_n]$ est résiduellement fini. Finalement par récurrence $\mathbb{Z}[X_1, ..., X_n]$ est résiduellement fni.

1.6 $\mathrm{GL}_d(\mathbb{Z}[X_1, ..., X_n])$ est résiduellement fini.

Soit $P \in \mathbb{Z}[X_1, ..., X_n])$ différent de l'identité, et notons $\mathbb{F}_q$ le corps fini tel qu'il existe

$\Phi : \mathbb{Z}[X_1, ..., X_n] \to \mathbb{F}_q$
tel que $P \xrightarrow{\Phi} \Phi(P) \neq 0$

Soit $\Pi \in \mathrm{GL}_d(\mathbb{Z}[X_1, ..., X_n])$ différent de l'identité c'est à dire $\exists P_{ij} \in \mathbb{Z}[X_1, ..., X_n]$ tel que $P_{ij} \neq 0$

Soit $f : \mathrm{GL}_d(\mathbb{Z}[X_1, ..., X_n]) \to \mathrm{GL}_d(\mathbb{F}_q)$

$\Pi = (P_{ij})_{1 \leq i,j \leq d} \mapsto (\Phi(P_{ij}))_{1 \leq i,j \leq d}$

On a $\Phi(P_{ij}) \neq 0$ par ce qui précéde. Donc $\mathrm{GL}_d(\mathbb{Z}[X_1, ..., X_n])$ est résiduellement fini.

1.7 $\mathbb{Z}[X_1, ..., X_n][1/f]$ est résiduellement fini

De la même manière on peut montrer que $\mathbb{Z}[X_1, ..., X_n][1/f]$ est résiduellement fini. En effet de la même manière que pour $\mathbb{Z}[\frac{1}{r}]$ et en utilisant le fait que $\mathbb{Z}[X_1, \ldots, X_n]$ est résiduellement fini, on montre que $\mathbb{Z}[X_1, ..., X_n][1/f]$ est résiduellement fini.

2 Extension finie

2.1 Définition et Lemme

Définition :

L'extension L/K est *finie* si L est de dimension finie en tant que K-espace vectoriel.

Lemme :

Si L/K est une extension finie alors il existe un morphisme injectif $\mathrm{GL}_d(L) \to \mathrm{GL}_{rd}(K)$.

Preuve :

Soient α fixé et $\varphi_\alpha : L \to L$ qui à $l \xrightarrow{\varphi_\alpha} \alpha l$ une application linéaire bijective.

Soit $\beta = (b_1, ..., b_r)$ une base de L, $Mat_\beta(\varphi_\alpha) \in \mathrm{GL}_r(K)$. Soit $\Phi : \mathrm{GL}_d(L) \to \mathrm{GL}_{rd}(K)$ tel que $(l_{ij})_{i,j} \xrightarrow{\Phi} (\varphi_{l_{ij}})_{1 \leq i,j \leq d}$ car pour chaque $\varphi_{l_{ij}}$; $Mat_\beta(\varphi_{l_{ij}}) \in \mathrm{GL}_r(K)$.

Montrons que Φ est un morphisme c'est à dire :

Soient $A = l_{ij}$ et $B = l'_{ij}$ montrons que $\Phi(A \times B) = \Phi(A) \times \Phi(B)$.

On pose $C = A \times B$, $C = (c_{ij})_{i,j}$ tel que $c_{ij} = \sum_{k=1}^{d} l_{ik} l'_{kj}$. On a $\Phi((c_{ij})_{i,j}) = \Phi(\sum_{k=1}^{d} l_{ik} l'_{kj})_{1 \leq i,j \leq d} = (\varphi_{\sum_{k=1}^{d} l_{ik} l'_{kj}})_{1 \leq i,j \leq d}$.

$$\begin{aligned} \varphi_{\sum_{k=1}^{d} l_{ik} l'_{kj}}(\alpha) &= (\sum_{k=1}^{d} l_{ik} l'_{kj})\alpha \\ &= \sum_{k=1}^{d} l_{ik} l'_{kj} \alpha \\ &= \sum_{k=1}^{d} \varphi_{l_{ik}}(l' kj\alpha \qquad\qquad = \sum_{k=1}^{d} \varphi_{l_{ik}} \circ \varphi_{l'_{kj}}(\alpha) \end{aligned}$$

$\forall \alpha \in L$ et $\forall i, j \in 1, ..., d$.

Donc $\Phi(A \times B) = \Phi(A) \times \Phi(B)$.

Le morphisme est injectif car si on a $\Phi(a) = \Phi(B)$ donc $(\varphi_{l_{ij}})_{i,j} = (\varphi_{l'_{ij}})_{i,j}$. On a donc $\varphi_{l_{ij}}(l) = \varphi_{l'_{ij}}(l)$

$\Rightarrow l_{ij} l = l'_{ij} l$

$\Rightarrow l_{ij} = l'_{ij}$ car $l \in L$ avec L un corps donc on a bien l'injectivité.

2.2

Définition :

L'extension L/K est *purement transcendante* s'il existe des éléments $a_1, \ldots, a_k \in L$ tels que $L = K[a_1, \ldots, a_k]$ et pour tout polynôme $f \in K[T_1, \ldots, T_k]$ on a $f(a_1, \ldots, a_k) \neq 0$. Autrement dit L est isomorphe comme corps au corps des fractions rationelles à coefficients dans K en k variables, $K(T_1, \ldots, T_k)$.

Théorème : *Soit L un sous-corps de $\mathbb{C}$ engendré (comme corps) par un nombre fini d'éléments. Alors il existe une extension purement transcendente $\mathbb{Q}(t_1, \ldots, t_k)/Q$ telle que $\mathbb{Q}(t_1, \ldots, t_k) \subset L$ et $L/\mathbb{Q}(t_1, \ldots, t_k)$ est une extension finie.*

Montrons que pour tout sous-groupe de type fini G de $\mathrm{GL}_d(\mathbb{C})$ il existe un homomorphisme injectif $G \to \mathrm{GL}_{rd}(\mathbb{Q}(t_1, \ldots, t_k))$ pour des $r, k \geq 1$, où $\mathbb{Q}(t_1, \ldots, t_k)/\mathbb{Q}$ est une extension purement transcendante.

Soit G un groupe de type fini de $\mathrm{GL}_d(\mathbb{C})$. G est donc engendré par un nombre fini d'éléments de $\mathrm{GL}_d(\mathbb{C})$.

On note $A_1, \ldots, A_r$ les matrices qui engendrent G. $c_1, \ldots, c_n$ tous les coefficients de ces matrices et $L = \mathbb{Q}(c_1, \ldots, c_n)$ le sous corps de $\mathbb{C}$ engendré comme corps par un nombre fini d'éléments $(c_1, \ldots, c_n) \in (\mathbb{C})^n$.

Par le théorème précédent qui nous dit que par un processus de récurence, on peut extraire une extension purement transcendante $\mathbb{Q}(c_{k_1}, \ldots, c_{k_l})/\mathbb{Q}$ tel

que $\mathbb{Q}(c_{k_1}, \ldots, c_{k_l}) \subset L$ et $L/\mathbb{Q}(c_{k_1}, \ldots, c_{k_l})$ est une extension finie (on pose $dim(L) = r$).
Par le lemme du 2.1, on a donc qu'il existe un morphisme injectif $\Phi : \mathrm{GL}_d(L) \to \mathrm{GL}_d(\mathbb{Q}(c_{k_1}, \ldots, c_{k_l})$ car $G \subset \mathrm{GL}_d(L)$. On a alors $\Phi_G : G \to \mathrm{GL}_{rd}(\mathbb{Q}(c_{k_1}, \ldots, c_{k_l}))$ un morphisme injectif tel que $\mathbb{Q}(c_{k_1}, \ldots, c_{k_l})/\mathbb{Q}$ est une extension purement transcendante.

2.3

Montrons qu'il existe $f \in \mathbb{Z}[T_1, \ldots, T_n]$ tel que $G \subset \mathrm{GL}_d(\mathbb{Z}[T_1, ..., T_k, \frac{1}{f}])$.

De même que précédemment G est un groupe de type fini de $\mathrm{GL}_d(\mathbb{C})$. G est donc engendré par un nombre fini d'éléments de $\mathrm{GL}_d(\mathbb{C})$.

On note $A_1, \ldots, A_r$ les matrices qui engendrent G. $c_1, \ldots, c_n$ tous les coefficients de ces matrices et $L = \mathbb{Q}(c_1, \ldots, c_n)$ le sous corps de $\mathbb{C}$ engendré comme corps par un nombre fini d'éléments $(c_1, \ldots, c_n) \in (\mathbb{C})^n$.
Montrons tout d'abord qu'il existe $f \in \mathbb{Z}[T_1, ..., T_k]$ tel que $L \in \mathbb{Z}[T_1, ...T_k, \frac{1}{r}]$.
Il suffit de prendre $f \in \mathbb{Z}[T_a, ..., T_k]$ tel que $\forall i \in 1, ..., n : f \times C_i^l \in \mathbb{Z}(c_1, \ldots, c_n)$.
Donc par consequent $G \subset \mathrm{GL}_d(L) \subset \mathrm{GL}_d(\mathbb{Z}[T_1, \ldots, T_k, \frac{1}{f}$.
D'après la section 1, $\mathrm{GL}_d(\mathbb{Z}[T_1, ..., T_k, \frac{1}{f}])$ est résiduellement fini donc pour chaque élément de G, il suffit de prendre le même morphisme qu'on a pris pour $\mathrm{GL}_d(\mathbb{Z}[T_1, ..., T_k, \frac{1}{f}])$ restreint à G.

3 Conclusion

On peut finalement conclure en ayant montré que tout sous groupe de type fini de $\mathrm{GL}_d(\mathbb{C})$ est résiduellement fini.