Proséminaire SA-2016
Le groupe $PSL_2(q)$

Magali Frontini

Bachelor en Mathématiques

Contents

1 Quelque groupe fini

Dans cette première section du chapitre on va identifier les groupes finis $PGL_2(q)$ et $PSL_2(q)$.
Soit K un corps, une première définition sera donnée à l'aide des groupes $GL_2(K)$ et $SL_2(K)$; alors qu'on se servira de la transformation de Möbius définie sur la droite projective $P^1(K)$ pour en donner une définition plus concrète.

Définition 1.1. Soit K un corps:

1. On note avec $GL_2(K)$ le groupe des matrices 2×2 inversibles (c.à.d. avec déterminant différent de zéro) à coéfficients dans K; ce groupe s'appelle groupe général linéaire.
   $\Rightarrow GL_2(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K : ab - cd \neq 0 \right\}$
2. On note avec $SL_2(K) \subseteq GL_2(K)$ le sous groupe des matrices 2×2 avec déterminant égale à 1; ce groupe s'appelle groupe spécial linéaire.
   $\Rightarrow SL_2(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K) : ab - cd = 1 \right\}$

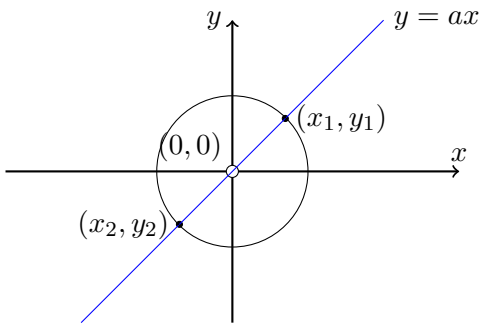
Remarque. Le groupe spécial linéaire $SL_2(K)$ forme le noyeau de l'application déterminant $det : GL_2(K) \to K^*$.

Définition 1.2. Soit K un corps:

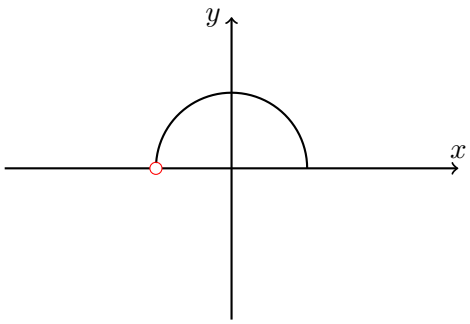
1. $PGL_2(K)$, le groupe projectif linéaire sur K, corréspond au groupe quotient $GL_2(K)/\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in K^* \right\}$.
2. $PSL_2(K)$, le groupe projectif spécial linéaire sur K, corréspond au groupe quotient $SL_2(K)/\left\{ \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix} : \epsilon = \pm 1 \right\}$.

On veut construire ces deux groupes de façon plus concrète. Soit donc $P^1(K) := K \cup \{\infty\}$ la droite projective sur K, c'est à dire un éspace projectif sur K de dimension 1.

Exemple 1.3. Si on considère $K = \mathbb{R}$ alors $P^1(\mathbb{R}) = \mathbb{R}^2 \setminus \{(0,0)\}/\backsim$,
où $(x_1, y_1) \backsim (x_2, y_2) \Leftrightarrow$ la droite qui passe par (x_1, y_1) et (x_2, y_2) contient le point $(0, 0)$.
Illustration:



$\Rightarrow (x_1, y_1) \backsim (x_2, y_2)$ et tout point sur la droite $y = ax$ sont équivalents entre eux; i.e. dans $P^1(\mathbb{R})$ la droite $y = ax$ est un point.
On peut donc représenter $P^1(\mathbb{R})$ comme le demi-cercle suivant, où $(-1, 0) \sim (1, 0)$.



Définition 1.4. Soient K un corps et $Sym(P^1(K))$ le groupe des permutations de l'ensemble fini $P^1(K)$.
Pour tout matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ on associe la Trasformation de Möbius

$$\varphi_A : P^1(K) \to P^1(K)$$

définie par

$$\varphi_A(z) = \tfrac{az+b}{cz+d},$$

avec $\varphi(\infty) = \begin{cases} \frac{a}{c} & , c \neq 0 \\ \infty & , c = 0 \end{cases}$ et $\varphi_A(\frac{-d}{c}) = \infty$, si $c \neq 0$.
On obtient alors un homomorphisme $\varphi : GL_2(K) \to Sym(P^1(K))$ tel que $\varphi(A) = \varphi_A$.
On définit $PGL_2(K) := \varphi(GL_2(K))$ et $PSL_2(K) := \varphi(SL_2(K))$.

Justification. Montrons que $\varphi : GL_2(K) \to Sym(P^1(K))$ est effectivement un homomorphisme. A voir que $\varphi_{AB} = \varphi_A \circ \varphi_B$.
Soient $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in GL_2(K)$. Alors $AB = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$ et

$$\begin{aligned} \varphi_{AB}(z) &= \frac{(aa'+bc')z + ab' + bd'}{(ca'+dc')z + cb' + dd'} \\ &= \frac{a(a'z+b') + b(c'z+d')}{c(a'z+b') + d(c'z+d')} \\ si\ c'z + d' \neq 0 \Rightarrow \varphi_{AB}(z) &= \frac{(c'z+d')\left(\frac{a(a'z+b')}{(c'z+d)} + b\right)}{(c'z+d')\left(\frac{c(a'z+b')}{(c'z+d')} + d\right)} \quad . \qquad (1) \\ &= \frac{a\frac{(a'z+b')}{(c'z+d')} + b}{c\frac{(a'z+b')}{(c'z+d')} + d} = \varphi_A \circ \varphi_B(z) \ . \end{aligned}$$

$$
\begin{aligned}
Si\ c'z+d'=0 \Rightarrow z &= \frac{-d'}{c'},\ (si\ c'\neq 0)\\
&\Rightarrow \varphi_B(\frac{-d'}{c'})=\infty\\
\Rightarrow \varphi_{AB}(\frac{-d'}{c'}) &= \frac{aa'(\frac{-d'}{c'})+bc'(\frac{-d'}{c'})+ab'+bd'}{ca'(\frac{-d'}{c'})+dc'(\frac{-d'}{c'})+cb'+dd'}\\
&= \frac{aa'(\frac{-d'}{c'})-bd'+ab'+bd'}{ca'(\frac{-d'}{c'})-dd'+cb'+dd'} \qquad (2)\\
&= \frac{a(a'(\frac{-d'}{c'})+b')}{c(a'(\frac{-d'}{c'})+b')}\\
&= \frac{a}{c}\\
&= \varphi_A(\infty)\ (si\ c\neq 0)\\
&= \varphi_A\circ\varphi_B(\frac{-d'}{c'})\ .\ \square
\end{aligned}
$$

Notation. Si K est un corps fini à q éléments, on écrit $GL_2(q)$, $SL_2(q)$, $PGL_2(q)$ et $PSL_2(q)$ pour les groupes qu'on vient de définir.

Proposition 1.5. *Soit K un corps d'ordre q, alors:*

a) $|GL_2(q)| = q(q-1)(q^2-1)$

b) $|SL_2(q)| = |PGL_2(q)| = q(q^2-1)$

c) $|PSL_2(q)| = \begin{cases} q(q^2-1) & si\ q\ est\ pair \\ \frac{q(q^2-1)}{2} & si\ q\ est\ impair\ . \end{cases}$

Preuve.

a) Soit $v=\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in \mathbb{F}_q^2 \setminus \{(0,0)\}$ le premier vecteur colonne d'une matrice $A = GL_2(q)$; comme $|\mathbb{F}_q^2 \setminus \{(0,0)\}| = q^2-1$, v peut être choisit entre q^2-1 vecteurs différents.
Le deuxiem vecteur colonne d'une même matrice doit être linéairement indépendant de v, c.à.d un vecteur $w=\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \in \mathbb{F}_q^2 \setminus \{\lambda(v_1,v_2)\}, \lambda \in \mathbb{F}_q$; comme $|\mathbb{F}_q^2 \setminus \{\lambda(v_1,v_2)\}| = q^2-q$, on $q^2-q = q(q-1)$ vecteurs entre lesquels choisir. En conclusion on a $q(q-1)(q^2-1)$ choix possilbes pour construire une matrice $A \in GL_2(q)$.

$$\Rightarrow |GL_2(q)| = q(q-1)(q^2-1)$$

b) Montrons d'abord que $|PGL_2(q)| = q(q^2-1)$.
On a $PGL_2(q) = GL_2(q)/\left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} : \lambda\in\mathbb{F}_q^*\right\}$, et le groupe $\left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} : \lambda\in\mathbb{F}_q^*\right\}$ est d'orde $q-1$ car, en construisant une telle matrice, on a $q-1$ possibilitées pour choisir le premier vecteur colonne, et il nous reste donc une seule possibilité pour choisir le deuxiem $\Rightarrow |PGL_2(q)| = \frac{q(q-1)(q^2-1)}{(q-1)} = q(q^2-1)$.
Maintenant considérons l'application $det : GL_2(q) \to \mathbb{F}_q^*$, dont le noyau corréspond au sous groupe normal $SL_2(q) \triangleleft GL_2(q)$.
Par le premier théorème d'isomorphismes on obtient que $GL_2(q)/SL_2(q) \cong \mathbb{F}_q^*$ d'où on voit facilement que $|SL_2(q)| = \frac{|GL_2(q)|}{(q-1)} = q(q^2-1)$.

$$\Rightarrow |SL_2(q)| = |PGL_2(q)| = q(q^2-1).$$

c) On a que $PSL_2(q) = SL_2(q)/\left\{A = \begin{pmatrix}\epsilon & 0\\ 0 & \epsilon\end{pmatrix} : \epsilon = \pm 1\right\}$.
Pour chaque corps fini K il existe p premier et $k \in \mathbb{N}$ tels que K est isomorphe à $\mathbb{F}_{p^k}$, où $\mathbb{F}_{p^k}$ est une extention de degré k de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
La charactérisrique de $\mathbb{F}_{p^k}$ est p, c.à.d. $\underbrace{1+...+1}_{p\ fois} = 0$.
On distingue deux cas.
Si $q = 2^k \Rightarrow q$ est pair et la charactéristique de $\mathbb{F}_q$ est 2, c.à.d.

$$1+1 = 0 \Leftrightarrow 1 = -1 \text{ et } A = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}.$$

Alors si q est pair $|PSL_2(q)| = \frac{|SL_2(q)|}{1} = |SL_2(q)| = q(q^2-1)$.
Si $q = p^k$, $p \neq 2$, $\Rightarrow q$ est impair et la charactéristique de $\mathbb{F}_q$ est p, c.à.d.

$$1 \cdot p = 0 \Leftrightarrow 1 \neq p-1 = -1$$

et

$$A \in \left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}; \begin{pmatrix}p-1 & 0\\ 0 & p-1\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}.$$

Alors si q est impair $|PSL_2(q)| = \frac{|SL_2(q)|}{2} = \frac{q(q^2-1)}{2}$

$$\Rightarrow |PSL_2(q)| = \begin{cases} q(q^2-1) & si\ q\ est\ pair \\ \frac{q(q^2-1)}{2} & si\ q\ est\ impair. \end{cases} \square$$

Exercice.

1) Montrer que $Ker\varphi$ est exactement le sous-groupe $\left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} : \lambda \in K^*\right\}$.

   Soit $\lambda \in K^* \Rightarrow \lambda Id = \begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} \in GL_2(K)$ et $\varphi(\lambda Id) = \varphi_{\lambda Id}(z) = \frac{\lambda z+0}{0z+\lambda} = z = Id$.

   Conversement, soit $z \in P^1(K)$

$$\begin{aligned}\frac{az+b}{cz+d} = Id &\Leftrightarrow az+b = z(cz+d)\\ &\Leftrightarrow az+b = cz^2+dz\\ &\Leftrightarrow az+b-cz^2-dz = 0\\ &\Leftrightarrow b+(a-d)z-cz^2 = 0\\ &\Leftrightarrow a = d \ \ et \ \ b = c = 0\end{aligned} \tag{3}$$

   On peut alors conclure que $\varphi(A) = Id \Leftrightarrow A = \begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$ telle que $\lambda \in K^*$.

2) Soit K un corps, calculer les matrices $A \in SL_2(K)$ telles que $\varphi_B(\infty) = \infty$.

   Soit $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(K)$. Par Définition 1.4 on a que $\varphi(\infty) = \infty$ si $c = 0$ ce qui implique que $det(A) = ad - bc = ad = 1$, donc $d = a^{-1}$, $a \neq 0$.

   $\Rightarrow$ pour toure matrice $A \in \left\{\begin{pmatrix}a & b\\ 0 & a^{-1}\end{pmatrix} : b \in K \text{ et } a \in K^*\right\}$, $\varphi_A(\infty) = \infty$.

2 Simplicité

Dans cette section, on va principalement étudier la simplicité du groupe $PSL_2(K)$ à l'aide d'une propriété structurelle de $SL_2(K)$, ce qui aidra dans le chapitre 4 à déterminer quel graphe de Ramanujan est biparti.

Lemme 2.1. *Pour tout corps K le groupe $SL_2(K)$ est engendré par l'union des deux sous-groups*

$$\left\{\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in K\right\} \text{ et } \left\{\begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in K\right\}.$$

C.à.d. que tout matrice dans $SL_2(K)$ c'est le produit fini de matrices $\Delta - infrieures$ et $\Delta - suprieures$ qui ont des 1 le long de la diagonale.

Preuve. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(K)$. On distingue deux cas différents:

cas 1: $c \neq 0$. On a

$$\begin{pmatrix} 1 & \frac{a-1}{c} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \frac{a(d-1)+(a-1)}{c} \\ c & d \end{pmatrix}.$$

Mais $\frac{a(d-1)+(a-1)}{c} = \frac{ad-1}{c} = \frac{ad-(ad-bc)}{c} = \frac{bc}{c} = b.$

cas 2: $c = 0$. Alors $d \neq 0$ et donc on peut traiter la matrice

$$\begin{pmatrix} a+b & b \\ d & d \end{pmatrix} \in SL_2(K)$$

comme dans le premier cas et on obtient

$$\begin{pmatrix} a+b & b \\ d & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \Leftrightarrow \begin{pmatrix} a+b & b \\ d & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \quad \square$$

Rappel. Un groupe G est dit simple si les uniques sous-groupes normales qu'il possède sont triviaux; c.à.d. G ou $\{1\}$. Par coséquence si G est simple tout homomorphisme de groupe $\pi : G \to H$, où $H \lhd G$, est constante ou injectif (conserve les distinctions).

Exemple 2.2.

- Le groupe cyclique fini $\mathbb{Z}/5\mathbb{Z}$ est simple, car tout groupe cyclique est abélien et un groupe cyclique abélien est simple $\Leftrightarrow$ il est d'ordre premier.
- Le groupe fini $G = \mathbb{Z}/12\mathbb{Z}$ n'est pas simple; en effet $H = \mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$ car l'indice $[G : H] = 2$ (Rappel: tout sous groupe d'indice 2 est normale).

Theorème 2.3. *Soit K un corps tel que $|K| \geq 4$. Alors le groupe projéctif spécial linéaire de diménsion 2 à coéfficients dans K, $PSL_2(K)$, est simple.*

Lemme 2.4. *Soit $\varphi : G \to G'$ un homomorphisme.*
Si $H \lhd G'$, $H \neq G'$ et $H \neq \{1\}$, alors $\varphi^{-1}(H) \lhd G$.

Preuve. Soit $H \lhd G'$, $H \neq G'$ et $H \neq \{1\}$.
$\varphi^{-1}(H) \lhd G \Leftrightarrow \forall g \in G\ g\varphi^{-1}(H)g^{-1} = \varphi^{-1}(H)$. $\varphi^{-1}(H) \subseteq G$ est un sous-groupe.
Soient $h \in \varphi^{-1}(H)$ et $g \in G$, alors:
$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) \in H \Rightarrow ghg^{-1} \in \varphi^{-1}(H) \Rightarrow \varphi^{-1}(H) \lhd G$. □

Preuve (Théorème 2.3)**.** (*Jordan* 1861)
Considérons l'homomorphisme de la Définition 1.4 réstreint à $SL_2(K)$,
$\varphi : SL_2(K) \to PSL_2(K)$. Il suffit de montrer qu'un sous groupe normal $N \lhd SL_2(K)$, qui n'est pas contenu dans le noyau $ker(\varphi) = \left\{ \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix} : \varepsilon = \pm 1 \right\}$, est égale à $SL_2(K)$ (voir Lemme 2.4) .

Soit donc $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N$ une matrice non-scalaire.

Rappel. Une matrice scalaire est une matrice diagonale dont tout élément de sa diagonale contiennent le même scalaire. Ex: $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$.

Comme A est non-scalaire il existe un vecteur $v \in K^2$ qui n'est pas un vecteur propre de A.

Justification. Supposons que pour tout $v \in K^2\ \exists\ \lambda \in K$ tq $Av = \lambda v$.
On cosidère les vecteurs $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. e_1 et e_2 sont des vecteurs propres de $A \Leftrightarrow \exists\ \lambda_1, \lambda_2 \in K$ tq:

$$A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} a = \lambda_1 \\ c = 0 \end{cases}$$

et

$$A \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Leftrightarrow \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ \lambda_2 \end{pmatrix} \Leftrightarrow \begin{cases} b = 0 \\ d = \lambda_2 \end{cases} \Leftrightarrow A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

Maintenant, soit $v = \lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$:

$$\begin{aligned} \Rightarrow Av &= A\lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + A\lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ 0 \end{pmatrix} + \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} 0 \\ \lambda_2 \end{pmatrix} \\ &= \lambda_1^2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_2^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \end{aligned} \tag{4}$$

Alors, $Av = \lambda v \Leftrightarrow \lambda_1^2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_2^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \lambda\lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda\lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Leftrightarrow \lambda = \lambda_1 = \lambda_2$,
ce qui contraidit le fait que A est non scalaire.

Donc v et Av sont linéairement indépendants sur K et $\{v, Av\}$ est une base de K^2.
Réécrivons A dans cette base.
Soit $A = (a_{ij})_{i,j\in\{0,1\}}$, où $a_{ij} = \langle Ae_j, e_i\rangle$.
Soient $e_1 = v$ et $e_2 = Av$, on définit:
$\langle v, v\rangle = \langle Av \text{ et } Av\rangle = 1$, $\langle Av, v\rangle = \langle v, Av\rangle = 0$.
$\Rightarrow a_{11} = a = \langle Av, v\rangle = 0$
$\Rightarrow a_{12} = b$
$\Rightarrow a_{21} = c = \langle Av, Av\rangle = 1$
$\Rightarrow a_{22} = d$.
Alors on peut écrire $A = \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix}$ dans la base $\{v, Av\}$, et vu que $A \in SL_2(K) \Rightarrow b = -1$.
Maintenant, soient $B \in N$ et $C \in SL_2(K)$; vu que $C^{-1}B^{-1}C \in N$ alors le commutateur $C^{-1}B^{-1}CB \in N$ aussi.
Appliquons ceci à $B = A$ et $C = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$, où $\alpha \in K^*$:

$$C^{-1}B^{-1}CB = \begin{pmatrix} \alpha^{-2} & d\left(\alpha^{-2} - 1\right) \\ 0 & \alpha^2 \end{pmatrix} \in N.$$

On repète le même calcul avec $B' = \begin{pmatrix} \alpha^{-2} & d\left(\alpha^{-2} - 1\right) \\ 0 & \alpha^2 \end{pmatrix}$ *et* $C' = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$, $\mu \in K$.
Alors,

$$C'^{-1}B'^{-1}C'B' = \begin{pmatrix} 1 & \mu\left(\alpha^4 - 1\right) \\ 0 & 1 \end{pmatrix} \in N.$$

Si $|K| \geq 4$ et $|K| \neq 5$ il existe $\alpha \in K^*$ telle que $\alpha^4 \neq 1$ et $\beta = \alpha^4 - 1 \neq 0$ ($\mathbb{F}_5^*$ est un groupe cyclique d'ordre 4 $\Rightarrow$ pour tout $\alpha \in \mathbb{F}_5^* :\ \alpha^4 = 1$).
β est inversible. Soit $\mu = k\beta^{-1}$, $k \in K$, alors $\mu(\alpha^4 - 1) = k\beta^{-1}\beta = k \in K$ et $\left\{\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in K\right\} \subseteq N$.

En plus

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} \in N,$$

alors on a aussi que $\left\{\begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in K\right\} \subseteq N$; et donc chaque élément de N est le produit fini de matrices $\Delta - infrieures$ et $\Delta - suprieures$ qui ont des 1 le long de la diagonale. Par le Lemme 2.1 on peut conclure que $N = SL_2(K)$. $\square_{K\neq\mathbb{F}_5}$

Maintenant on donne la preuve pour $|K| = 5$. Soit alors $K = \mathbb{F}_5$. Pour la première partie de la preuve on a que $\begin{pmatrix} \alpha^{-2} & d\left(\alpha^{-2} - 1\right) \\ 0 & \alpha^2 \end{pmatrix} \in N$, pour n'importe quel $\alpha \in \mathbb{F}_5^*$.

Soit $\alpha = 2$ (et $\alpha^{-1} = -2$), alors $\begin{pmatrix} -1 & -2d \\ 0 & -1 \end{pmatrix} \in N$, et $\begin{pmatrix} -1 & -2d \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix} \in N$.
On distingue deux cas différents:

cas 1: $d \neq 0$. Donc $\begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n(-d) \\ 0 & 1 \end{pmatrix} \forall n \in \mathbb{N}$, c.à.d. toute puissance de $\begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix}$ appartient à $\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{F}_5 \right\}$. En plus

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix},$$

donc $\left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{F}_5 \right\} \subseteq N$ et par Lemme 2.1 $N = SL_2(5)$.

cas 2: $d = 0$. Donc $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Calculons alors le commutateur $C''^{-1}A^{-1}C''A$ où $C'' = \begin{pmatrix} \delta & 1 \\ -1 & 0 \end{pmatrix}$, $\delta \in \mathbb{F}_5^*$:

$$A' = C''^{-1}A^{-1}C''A = \begin{pmatrix} 1 & -\delta \\ -\delta & \delta^2 + 1 \end{pmatrix} \in N.$$

Comme A' est non-scalaire, dans une certaine base $\{w, A'w\}$ de $\mathbb{F}_5^2$, on peut écrire $A' = \begin{pmatrix} 0 & -1 \\ 1 & d' \end{pmatrix}$ et $d' = TrA' = 1 + \delta^2 + 1 = \delta^2 + 2 \neq 0$, car $\delta^2 = \pm 1$ dans $\mathbb{F}_5^*$.
Alors

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & d' \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d' & -1 \\ 1 & 0 \end{pmatrix} \in N.$$

et

$$\begin{pmatrix} d' & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & d' \end{pmatrix} = \begin{pmatrix} -1 & -2d' \\ 0 & -1 \end{pmatrix} \in N \Rightarrow \begin{pmatrix} -1 & -2d' \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & -d' \\ 0 & 1 \end{pmatrix} \in N.$$

On peut donc se reconduire au cas 1 et conclure que $N = SL_2(5)$. $\square_{K=\mathbb{F}_5}$ $\square$

Exercice. Montrer que:

1) $PSL_2(2)$ est isomorphe à $Sym(3)$.
Considérons l'homomorphisme

$$\varphi : SL_2(2) \to Sym(3).$$

Par Définition 1.4 on a que $\varphi(SL_2(2)) = PSL_2(2) \subseteq Sym(3)$ mais $|PSL_2(2)| = 2(2^2 - 1) = 6 = 3! = |Sym(3)|$ (voir proposition 1.5), alors on peut conclure

$$PSL_2(2) \cong Sym(3).$$

2) $PSL_2(3)$ est isomorphe à Alt_4.
Considérons l'homomorphisme

$$\varphi : SL_2(3) \to Sym(4).$$

On a que $\varphi(SL_2(3)) = PSL_2(3)$. En plus $|PSL_3(3)| = \frac{3(3^2-1)}{2} = 12$ et $|Sym(4)| = 4! = 24$.

Alors, vu que l'indice $[Sym(4) : PSL_2(3)] = 2$ on peut affirmer que $PSL_2(3) \triangleleft Sym(4)$ est un sous-groupe normale, mais $A_4 \triangleleft Sym(4)$ est l'unique sous-groupe normale de $Sym(4)$ d'ordre 12, donc on peut conclure que

$$PSL_2(3) \simeq Alt_4.$$

3) $PSL_2(4)$ et $PSL_2(5)$ sont isomorphes à $Alt(5)$.
Considérons les homomorphismes

$$\varphi : SL_2(4) \to Sym(5) \text{ et } \varphi_1 : SL_2(5) \to Sym(5).$$

On fait le même raisonnement que dans exercice 2):
$\varphi(SL_2(4)) = PSL_2(4)$ qui a ordre $4(4^2 - 1) = 60 \Rightarrow [Sym(5) : PSL_2(4)] = 2$
$\Rightarrow PSL_2(4) \triangleleft Sym(5)$.
$\varphi_1(SL_2(5)) = PSL_2(5)$ qui a ordre $\frac{5(5^2-1)}{2} = 60 \Rightarrow [Sym(5) : PSL_2(5)] = 2$
$\Rightarrow PSL_2(4) \triangleleft Sym(5)$.
Mais Alt_5 est l'unique sous-groupe normale de $Sym(5)$, alors on peut conclure que

$$PSL_2(4) \simeq PSL_2(5) \simeq Alt_5.$$