

SUR LES SOUS-GROUPES NORMAUX DE SL_2 SUR UN ANNEAU LOCAL

PAR

N. H. J. LACROIX ET C. LEVESQUE

RESUME. Soit $GL_n(\mathfrak{o})$ le groupe des matrices inversibles $n \times n$ sur \mathfrak{o} et soit $SL_n(\mathfrak{o})$ le groupe des matrices $n \times n$ de déterminant 1 sur \mathfrak{o} . Lorsque \mathfrak{o} est un anneau local avec idéal maximal \mathfrak{p} , W. Klingenberg (Amer. J. Math. 1961) a classifié les sous-groupes normaux de $GL_n(\mathfrak{o})$ et de $SL_n(\mathfrak{o})$ au moyen de certains groupes de congruences déterminés par les idéaux de \mathfrak{o} , sauf lorsque $n=2$ et $2 \in \mathfrak{p}$ ou $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_3$. Ces cas furent étudiés par N. H. J. Lacroix (Can. J. Math. 1969) qui trouva (lorsque $\mathfrak{o}/\mathfrak{p} \neq \mathbb{F}_2$) la même classification pour les sous-groupes normaux de $GL_2(\mathfrak{o})$; sa méthode donne simultanément la même classification également pour les sous-groupes normaux de $SL_2(\mathfrak{o})$ si l'anneau \mathfrak{o} satisfait à une forte condition appelée Propriété T.

Au cours de cette note, nous précisons que les sous-groupes normaux de $SL_2(\mathfrak{o})$ obéissent à la classification de Klingenberg si et seulement si \mathfrak{o} a la Propriété T. Par la suite nous montrons qu'en l'absence de cette condition, l'on n'a pas de vraie classification basée sur les transvections. Divers résultats sur les sous-groupes normaux illustrent ce qu'on peut attendre d'une entreprise visant à décrire les sous-groupes normaux de $SL_2(\mathfrak{o})$ en l'absence de la Propriété T.

1. Introduction. Soit $GL_n(\mathfrak{o})$ le groupe des matrices inversibles $n \times n$ sur \mathfrak{o} et soit $SL_n(\mathfrak{o})$ le groupe des matrices $n \times n$ de déterminant 1 sur \mathfrak{o} . Lorsque \mathfrak{o} est un anneau local avec idéal maximal \mathfrak{p} , W. Klingenberg [1] a classifié les sous-groupes normaux de $GL_n(\mathfrak{o})$ et de $SL_n(\mathfrak{o})$ au moyen de certains groupes de congruences déterminés par les idéaux de \mathfrak{o} , sauf lorsque $n=2$ et $2 \in \mathfrak{p}$ ou $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_3$. Ces cas furent étudiés par N. H. J. Lacroix [2], avec les résultats suivants: (a) lorsque $\mathfrak{o}/\mathfrak{p}$ a plus de 2 éléments, les sous-groupes normaux de $GL_2(\mathfrak{o})$ obéissent à la classification de Klingenberg, à une seule exception près; (b) lorsque $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_3$, le même énoncé est vrai pour les sous-groupes normaux de $SL_2(\mathfrak{o})$ (à la même exception près); (c) lorsque $2 \in \mathfrak{p}$ et $\mathfrak{o}/\mathfrak{p}$ a plus de 2 éléments, les sous-groupes normaux de $SL_2(\mathfrak{o})$ obéissent à la classification de Klingenberg si l'anneau \mathfrak{o} satisfait à une forte condition appelée "Propriété T"; (d) lorsque

Reçu par la rédaction le 13 novembre 1981 et, sous une forme révisée, le 2 juin 1982.

1980 AMS Subject Classification Number: 20 H 05

© 1983 Société Mathématique du Canada.

$\mathfrak{o}/\mathfrak{p} = \mathbb{F}_2$, beaucoup d'aberrations surgissent et on ne fournit que des résultats partiels.

Le premier but atteint par le présent article est le remplacement de l'énoncé (c) ci-dessus par celui-ci: (c') lorsque $2 \in \mathfrak{p}$ et $\mathfrak{o}/\mathfrak{p}$ a plus de 2 éléments, les sous-groupes normaux de $SL_2(\mathfrak{o})$ obéissent à la classification de Klingenberg si et seulement si l'anneau \mathfrak{o} satisfait à la Propriété T . (Voir les théorèmes 4.3 et 4.4).

Le deuxième objectif de cet article est l'étude de la question suivante reliée aux énoncés (c) et (c') ci-dessus: y a-t-il une classification ou au moins une description assez systématique des sous-groupes normaux de $SL_2(\mathfrak{o})$ lorsque \mathfrak{o} n'a pas la Propriété T ?

Pour résumer la portée de nos résultats à ce sujet, rappelons d'abord en ces termes ce qu'est la classification de Klingenberg: elle repose essentiellement sur l'inclusion des groupes de congruences spéciaux, le reste des détails allant de soi; en gros, G est normal si et seulement si $G \geq SC_2$, où SC_2 représente un des groupes de congruences spéciaux (ceux-ci étant engendrés par des transvections). (Pour plus de détails, voir Klingenberg [1], ou Lacroix [2] p. 108 et p. 114).

Dans la situation où $2 \in \mathfrak{p}$ et $\mathfrak{o}/\mathfrak{p} \neq \mathbb{F}_2$ (i.e. caractéristique $(\mathfrak{o}/\mathfrak{p}) = 2$ et $\mathfrak{o}/\mathfrak{p}$ possède au moins 4 éléments), nous montrons tout d'abord que tout sous-groupe normal de $SL_2(\mathfrak{o})$, rattaché à un idéal principal, contient au moins une transvection, c'est-à-dire, au moins un sous-groupe A d'un groupe de congruences spécial SC_2 , alors que la réciproque est fautive, à savoir: un groupe qui contient une transvection, c'est-à-dire, qui contient un sous-groupe A , n'est pas toujours normal. (Voir Théorème 5.1 et Exemple 5.2).

On n'aboutit donc pas à une classification, ni à la Klingenberg, ni basée sur les transvections.

On donne alors une description assez systématique des groupes A engendrés chacun par une transvection:

(1) on compte le nombre l de groupes A distincts par un même idéal principal (Proposition 6.1), ce qui dépend de l'anneau \mathfrak{o} et mesure en un certain sens combien loin l'on est d'une vraie classification, soit selon les SC_2 , soit basée sur les transvections;

(2) en spécifiant que l'anneau est principal et que $\mathfrak{o}/\mathfrak{p}$ est fini, on peut fournir une valeur précise pour l (Proposition 8.2);

(3) dans ces mêmes dernières conditions, on évalue précisément à l^2 l'écart entre un groupe A et le SC_2 apparenté (Proposition 8.1).

L'examen des groupes A illustre ce qu'on peut attendre d'une entreprise visant à décrire les sous-groupes normaux de $SL_2(\mathfrak{o})$ en l'absence de la Propriété T .

2. Définitions et notation. Pour deux groupes H et G , $H \leq G$ signifiera que H est un sous-groupe de G ; de même pour $H < G$, sauf qu'ici l'inclusion est

stricte. On emploie la notation usuelle \triangleleft pour désigner un sous-groupe normal.

Sauf à la dernière section où nous serons explicites, \mathfrak{o} sera toujours un anneau local d'idéal maximal \mathfrak{p} , dont le corps résiduel $\mathfrak{o}/\mathfrak{p}$ est de caractéristique 2 (i.e. $2 \in \mathfrak{p}$) et possède plus de 2 éléments (donc au moins 4). On écrit $N_{\mathfrak{p}}$ pour la cardinalité de $\mathfrak{o}/\mathfrak{p}$.

Lorsque \mathfrak{o} est principal, nous dénotons le générateur de \mathfrak{p} par π , de sorte que tout idéal propre est de la forme $\mathfrak{p}^n = \pi^n \mathfrak{o}$ (à moins que $\bigcap_{i=1}^{\infty} \mathfrak{p}^i \neq 0$, mais notre discussion ne portera que sur les idéaux \mathfrak{p}^n et les éléments $\pi^n \alpha$).

L'ensemble $u = \mathfrak{o} \setminus \mathfrak{p}$ est le groupe des inversibles de \mathfrak{o} . On pose

$$u^2 = \{x^2 \mid x \in u\}, \quad 1 + \mathfrak{p}^r = \{1 + \pi^r \alpha \mid \alpha \in \mathfrak{o}\},$$

$$u^2 + \mathfrak{a} = \{x^2 + \zeta \mid x \in u \text{ et } \zeta \in \mathfrak{a}\} \text{ où } \mathfrak{a} \text{ est un idéal de } \mathfrak{o}.$$

Afin d'éviter l'écriture de certaines matrices, posons par définition,

$$\sigma = \begin{pmatrix} a & c \\ d & b \end{pmatrix}, \quad E_{12}(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \quad E_{21}(\lambda) = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix},$$

$$\text{Diag}(\alpha, \beta) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

Les matrices $E_{12}(\lambda)$ et $E_{21}(\lambda)$ sont des transvections (élémentaires).

On définit l'ordre $o(\sigma)$ de σ comme l'idéal de \mathfrak{o} engendré par les éléments $a-b, c$ et d . Pour un groupe $G \leq SL_2(\mathfrak{o})$, on définit l'ordre $o(G)$ de G comme l'idéal engendré par les idéaux $o(\sigma), \forall \sigma \in G$.

On définit $SC_2(\mathfrak{a})$, le groupe de congruences spécial mod \mathfrak{a} par: $\sigma \in SC_2(\mathfrak{a}) \Leftrightarrow \sigma \equiv \text{identité mod } \mathfrak{a}$ et $\det \sigma = 1$, où le signe \equiv traduit que l'on lit les éléments de σ modulo l'idéal $\mathfrak{a} \subseteq \mathfrak{o}$.

Soit $\omega \in \mathfrak{p}$; appelons $A(\omega)$ le sous-groupes normal de $SL_2(\mathfrak{o})$ engendré par $E_{12}(\omega)$. On voit aisément que $E_{12}(\omega), A(\omega)$ et $SC_2(\omega\mathfrak{o})$ ont même ordre $\omega\mathfrak{o}$.

En général, $A(\omega) \neq SC_2(\omega\mathfrak{o})$, c'est-à-dire, $A(\omega) < SC_2(\omega\mathfrak{o})$, alors que le sous-groupe normal de $GL_2(\mathfrak{o})$ engendré par $E_{12}(\omega)$ est $SC_2(\omega\mathfrak{o})$; cf. [2], p. 118 et p. 123.

Si $A(\omega) = SC_2(\omega\mathfrak{o})$ pour tout $\omega \in \mathfrak{p}$, on dit que \mathfrak{o} possède la *Propriété T* (cette notation faisant allusion aux transvections).

3. Lemmes de base. Cette section énumère les faits d'usage courant, certains d'entre eux étant identifiés comme lemmes.

Si—représente les homomorphismes

$$\text{—} : \mathfrak{o} \rightarrow \mathfrak{o}/\mathfrak{b} \text{ et } \text{—} : SL_2(\mathfrak{o}) \rightarrow SL_2(\mathfrak{o}/\mathfrak{b}),$$

il est aisé de vérifier que $A(\bar{\omega}) = \overline{A(\omega)}$.

Si $G \triangleleft SL_2(\mathfrak{o})$ avec $o(G) = \omega\mathfrak{o}$, alors nous savons ([2], p. 109) que G contient

$$\sigma = \begin{pmatrix} a & c \\ d & b \end{pmatrix} \text{ et } \sigma_1 = \begin{pmatrix} a_1 & c_1 \\ d_1 & b_1 \end{pmatrix} \text{ avec } d\mathfrak{o} = \omega\mathfrak{o} = c_1\mathfrak{o},$$

et sans perte de généralité, nous pouvons supposer que $G \leq SC_2(\omega v)$, c'est-à-dire que l'étude de $G \cap SC_2(\omega v)$ suffit.

Si $G \triangleleft SL_2(v)$ et si $\alpha \in u$, alors $E_{12}(\lambda) \in G \Leftrightarrow E_{12}(\lambda \alpha^2) \in G$. Il suffit de conjuguer $E_{12}(\lambda)$ par $\text{Diag}(\alpha, \alpha^{-1})$.

FORMULE 3.1. Soit σ avec $c, d \in p$ et $\det \sigma = 1$ et soit

$$\Xi = \begin{pmatrix} \alpha & \mu \\ 0 & \beta \end{pmatrix}$$

où $\beta = 1 - b^{-1}d \in u$, $\alpha = \beta^{-1}$, $\mu = 1 + \alpha$. Alors $\Xi \in SL_2(v)$, $\alpha = 1 + \varepsilon d$ où $\varepsilon \in u$, $\mu = 2 + \varepsilon d$ et $\Xi \sigma \Xi^{-1} \sigma^{-1} a$

$$\begin{cases} \text{élément (1, 2)} = ac(\alpha^2 - 1) - \alpha \mu a(a - b) - \mu d(\beta c + \mu a), \\ \text{élément (2, 1)} = 0 \end{cases}$$

LEMME 3.2. $A(\omega) \geq SC_2(2\omega v)$.

Démonstration. Si $\gamma \in u$ avec $\gamma \not\equiv 1 \pmod p$, on arrive à $E_{12}(2\gamma\omega) \in A(\omega)$ en considérant le produit $E_{12}(\omega\gamma^2)E_{12}(-\omega(\gamma - 1)^2)$. Si $\gamma \equiv 1 \pmod p$, on choisit $\delta \in u$ avec $\delta \not\equiv 1 \pmod p$ et on arrive à $E_{12}(2\gamma\omega) \in A(\omega)$ en considérant $E_{12}(2(\gamma - \delta)\omega)E_{12}(2\delta\omega)$. Enfin, pour $\zeta \in p$, on trouve $E_{12}(2\zeta\omega) \in A(\omega)$ avec $E_{12}(2(-1 + \zeta)\omega)E_{12}(2\omega)$. Q.E.D.

LEMME 3.3. Soit $\sigma = \begin{pmatrix} a & X \\ 0 & b \end{pmatrix} \in G \triangleleft SL_2(v)$. Alors

- (i) $E_{12}(Xa) \in G$ et $E_{12}(Xb) \in G$,
- (ii) $E_{12}((a - b)\alpha) \in G$ pour tout $\alpha \in v$, i.e. $G \geq SC_2((a - b)v)$.

Démonstration. Ici $b = a^{-1}$. (i) Soit $\gamma \in u$ avec $\gamma \not\equiv 1 \pmod p$; alors

$$\text{Diag}(\gamma, \gamma^{-1})\sigma \text{Diag}(\gamma^{-1}, \gamma)\sigma^{-1} = E_{12}(X(\gamma^2 - 1)a) \in G;$$

comme $G \geq A(X(\gamma^2 - 1)a) \geq SC_2(2Xv)$, alors G contient

$$E_{12}(Xa(\gamma^2 - 1))E_{12}(2X(\gamma + 1)a) = E_{12}(Xa(\gamma + 1)^2),$$

d'où $E_{12}(Xa) \in G$.

- (ii) Pour tout $\alpha \in v$, $E_{12}(-b\alpha)\sigma E_{12}(b\alpha)\sigma^{-1} = E_{12}((a - b)\alpha) \in G$. Q.E.D.

LEMME 3.4. $A(\omega) \geq SC_2(\omega^2 v)$.

Démonstration. (i) Conjuguant $E_{12}(\omega)$ avec $\text{Diag}(1 + \omega, (1 + \omega)^{-1})$, nous obtenons $E_{12}(\omega(1 + \omega^2))E_{12}(2\omega^2) \in A(\omega)$, d'où $E_{12}(\omega(1 + \omega^2)) \in A(\omega)$. Donc $E_{12}(-\omega(1 + \omega^2)^{-1}) \in A(\omega)$ et le produit

$$E_{12}(-\omega(1 + \omega^2)^{-1})E_{21}(\omega)E_{12}(\omega)E_{21}(-\omega)$$

montre, grâce aux lemmes précédents, que $A(\omega) \geq SC_2(\omega^4 v)$.

(ii) $A(\omega)$ contient

$$\psi = E_{21}(\omega)(E_{21}(1)E_{12}(\omega)E_{21}(-1))E_{12}(-\omega).$$

Appelons τ le résultat de la conjugaison de ψ avec $\text{Diag}(x^{-1}, x)$ où $x \in u$ vérifie $x \not\equiv 1 \pmod{p}$. Soit γ l'élément $(1, 1)$ de $\sigma = E_{12}(1)\tau E_{12}(-1)\tau^{-1}$. Comme $A(\omega) \geq SC_2(\omega^4 v)$, alors $E_{21}(-\omega^4 x^4 \gamma^{-1})\sigma \in A(\omega)$. Donc

$$E_{12}(2\omega\gamma)E_{12}(\omega^2(x^2 - 1)\gamma)E_{12}(-\omega^3 x^2 \gamma) \in A(\omega).$$

Comme $E_{12}(\omega(1 + \omega^2)) \in A(\omega)$, alors $E_{12}(\omega^3 x^2) \in A(\omega)$, d'où l'on vérifie que $E_{12}(-\omega^3 x^2 \gamma) \in A(\omega)$ et ensuite que $E_{12}(\omega^2(x^2 - 1))$, $E_{12}(\omega^2(x + 1)^2)$ et enfin $E_{12}(\omega^2)$ appartiennent à $A(\omega)$. Avec $E_{12}(\omega^2)$ et $E_{12}(\omega^3)$, on arrive à $\phi = E_{21}(\omega^2(1 - \omega)^{-1}) \in A(\omega)$. Alors $\phi\psi \in A(\omega)$, et nous avons la conclusion grâce aux lemmes 3.3 (ii) et 3.2. Q.E.D.

LEMME 3.5. $A(\omega) \geq SC_2(\omega^2 v + 2\omega v)$.

Démonstration. Le résultat découle des lemmes 3.2 et 3.4. Q.E.D.

4. Equivalence de la propriété T et de la classification des sous-groupes normaux de SL_2 .

On pose $\mathfrak{Z}(\omega) = \{x \mid x\omega \in \omega^2 v + 2\omega v\}$,

ce qui est un idéal de v . Le lemme suivant sera utilisé à la section 8.

LEMME 4.1. Si $\bar{\cdot}$ représente les homomorphismes

$$\bar{\cdot} : v \rightarrow v/\mathfrak{Z}(\omega) \quad \text{et} \quad \bar{\cdot} : u \rightarrow u/(1 + \mathfrak{Z}(\omega)).$$

alors $u/u^2 + \mathfrak{Z}(\omega) \cong u/u^2(1 + \mathfrak{Z}(\omega)) \cong \bar{u}/\bar{u}^2$.

Le prochain résultat montre que $\mathfrak{Z}(\omega)$ caractérise les transvections élémentaires de $A(\omega)$.

PROPOSITION 4.2. Soit $\gamma \in v$. Alors

$$E_{12}(\omega\gamma) \in A(\omega) \Leftrightarrow \gamma \equiv \text{un carré mod } \mathfrak{Z}(\omega).$$

Démonstration. (i) Soit $\gamma = x^2 + z$ avec $x \in v$ et $z \in \mathfrak{Z}(\omega)$. Si $x \in u$, $E_{12}(\omega x^2) \in A(\omega)$. Si $x \in p$, alors $A(\omega)$ contient aussi $E_{12}(\omega x^2) = E_{12}(-2\omega x)E_{12}(-\omega)\text{Diag}(1 + x, (1 + x)^{-1})E_{12}(\omega)\text{Diag}((1 + x)^{-1}, 1 + x)$. D'où $A(\omega)$ contient $E_{12}(\omega\gamma) = E_{12}(\omega x^2)E_{12}(z\omega)$.

(ii) Soit $\gamma \not\equiv$ un carré mod $\mathfrak{Z}(\omega)$. Soit $\bar{v} = v/\omega^2 v + 2\omega v$. Nous avons $\mathfrak{Z}(\bar{\omega}) = \bar{\mathfrak{Z}}(\omega)$ et la démonstration se fait maintenant de façon semblable à celle de la proposition 2.2.1 de N. H. J. Lacroix [2], à l'exception qu'ici $\bar{2}\bar{\omega} = \bar{0}$. Q.E.D.

THEOREME 4.3. La Propriété T peut être définie en termes du comportement des seuls éléments de l'anneau v , c'est-à-dire:

$$v \text{ a la Propriété T} \Leftrightarrow \gamma \equiv \text{un carré mod } \mathfrak{Z}(\omega), \quad \forall \gamma \in v, \quad \forall \omega \in p.$$

Démonstration. Le résultat découle des définitions de la Propriété T et de $SC_2(\omega\mathfrak{o})$, de la Proposition 4.2 et du fait que $SC_2(\omega\mathfrak{o})$ est engendré par les transvections élémentaires d'ordre $\subseteq \omega\mathfrak{o}$ (cf. [2], p. 112). Q.E.D.

THEOREME 4.4. *Lorsque $2 \in \mathfrak{p}$ et $\mathfrak{o}/\mathfrak{p}$ a plus de 2 éléments, les sous-groupes normaux de $SL_2(\mathfrak{o})$ obéissent à la classification de Klingenberg si et seulement si l'anneau \mathfrak{o} a la Propriété T .*

Démonstration. Explicitement, il faut démontrer l'équivalence entre les énoncés (i) et (ii) suivants:

(i) étant donné un sous-groupe $G \leq SL_2(\mathfrak{o})$ avec $\mathfrak{o}(G) = \mathfrak{a} \subseteq \mathfrak{p}$, alors $G \triangleleft SL_2(\mathfrak{o}) \Leftrightarrow G \cong SC_2(\mathfrak{a})$;

(ii) \mathfrak{o} a la Propriété T .

L'implication (ii) \Rightarrow (i) fut démontrée en [2] (cf. p. 124 et pp. 114–115). L'implication (i) \Rightarrow (ii) est immédiate car (i) dit en particulier que $A(\omega) = SC_2(\omega\mathfrak{o})$. Q.E.D.

Bien sûr, ce théorème 4.4 aurait pu être reconnu et énoncé en [2], mais il acquiert ici une plus grande portée, conférée par l'équivalence exprimée au Théorème 4.3.

REMARQUE 4.5. Les résultats ci-dessus permettent de faire deux observations d'un certain intérêt.

Supposons que \mathfrak{o} est principal avec $\mathfrak{o}/\mathfrak{p}$ parfait et $2\mathfrak{o} = \mathfrak{p}$. Alors $A(\pi^n \alpha) = SC_2(\mathfrak{p}^n)$ pour tout $\alpha \in \mathfrak{u}$ et tout entier $n \geq 1$, ceci résultant du fait que $\mathfrak{Z}(\pi^n \alpha) = \mathfrak{p}$ et que pour tout $\gamma \in \mathfrak{o}$, $\gamma \equiv$ un carré mod \mathfrak{p} . Ainsi \mathfrak{o} a la Propriété T et l'on a la classification de Klingenberg (en supposant qu'on n'a pas $\bigcap_{i=1}^{\infty} \mathfrak{p}^i \neq 0$; autrement l'on aurait des idéaux pour lesquels on ne saurait tirer de conclusions).

Par contre, si \mathfrak{o} est l'anneau des entiers d'un corps local dyadique avec (\mathfrak{o} principal, $\mathfrak{o}/\mathfrak{p}$ parfait et) $2\mathfrak{o} \subset \mathfrak{p}$, alors $A(\pi^n \alpha) < SC_2(\mathfrak{p}^n)$ pour tout $\alpha \in \mathfrak{u}$ et tout entier $n > 1$, ceci résultant du fait que le défaut quadratique de $1 + \pi$ est \mathfrak{p} (cf. p. 162 de [3]). Ainsi cet \mathfrak{o} n'a pas la Propriété T et l'on n'a pas la classification de Klingenberg.

5. Non-existence d'une classification basée sur les transvections. Nous nous consacrons désormais à l'étude des sous-groupes (normaux) de $SL_2(\mathfrak{o})$ en l'absence de la Propriété T .

Certains groupes peuvent ne contenir que très peu de transvections, par exemple des groupes distincts $A(\omega)$, $A(\omega\gamma)$, $A(\omega\delta)$, ... (voir Propositions 4.2 et 6.1 et Théorème 4.3).

Au moyen d'un théorème (5.1) et de la fausseté de sa réciproque (Exemple 5.2), la présente section montre qu'il n'existe pas de classification des sous-groupes normaux de $SL_2(\mathfrak{o})$ basée sur les transvections. Pour cela, il suffit que le théorème et l'exemple portent sur un groupe G dont l'ordre est principal: $\mathfrak{o}(G) = \mathfrak{a} = \omega\mathfrak{o} \subseteq \mathfrak{p}$.

THEOREME 5.1. Soit $G \langle SL_2(\mathfrak{o})$ avec $\mathfrak{o}(G) = \omega\mathfrak{o} \subseteq \mathfrak{p}$. Alors il existe un inversible α tel que $G \geq A(\omega\alpha)$.

Démonstration. (i) Montrons d'abord que si $\omega^m = 0$ pour un entier $m \geq 1$, il existe $\alpha \in \mathfrak{u}$ tel que $G \geq A(\omega\alpha)$. Procédons par induction sur m , le cas $m = 1$ étant trivial. Lorsque $m = 2$, il s'agit de prendre un élément $\sigma \in G$ avec $d\mathfrak{o} = \omega\mathfrak{o}$, de considérer $E_{12}(1)\sigma E_{12}(-1)\sigma^{-1}$ et d'utiliser le Lemme 3.3. Lorsque $m \geq 3$, nous quotientons (opération \dashv) \mathfrak{o} par $\omega^{m-1}\mathfrak{o}$ de sorte que G contient une image inverse σ de $E_{12}(\bar{\omega}\bar{\alpha})$, où $\bar{\alpha} \in \bar{\mathfrak{u}}$. Il s'agit ensuite de considérer l'élément $E_{21}(c^{m-2})\sigma E_{21}(-c^{m-2})\sigma^{-1}$ pour conclure que $G \geq SC_2(2\omega^{m-1}\mathfrak{o})$, et l'élément $E_{12}(1)\sigma E_{12}(-1)\sigma^{-1}$ pour conclure que $E_{12}(-da) \in G$. D'où $E_{21}(-da^{-1})\sigma \in G$, de sorte que $E_{12}(ca) \in G$.

(ii) Montrons maintenant par induction que si $2^m\omega = 0$ pour un entier $m \geq 1$, alors il existe $\alpha \in \mathfrak{u}$ tel que $G \geq A(\omega\alpha)$. Soit $m = 1$. Nous déduisons de la partie (i) qu'il existe $\beta \in \mathfrak{u}$ tel que G contient

$$\sigma = \begin{pmatrix} 1+x & c \\ \omega\beta+z & 1+y \end{pmatrix} = \begin{pmatrix} 1+x & c \\ d & 1+y \end{pmatrix} \text{ avec } x, y, z, c \in \omega^4\mathfrak{o} \text{ et } d\mathfrak{o} = \omega\mathfrak{o}.$$

Utilisant la Formule 3.1, nous obtenons la matrice $\Xi\sigma\Xi^{-1}\sigma^{-1}$ dont l'élément (1, 2) engendre $\omega^3\mathfrak{o}$. Appliquant les lemmes 3.3 et 3.4, nous déduisons qu'il existe $\delta \in \mathfrak{u}$ tel que $G \geq A(\omega^3\delta) \geq SC_2(\omega^6\mathfrak{o})$. Encore d'après la partie (i), nous savons qu'il existe $\beta \in \mathfrak{u}$ tel que G contient

$$\phi = \begin{pmatrix} 1+x & \omega\beta+z \\ w & 1+y \end{pmatrix} = \begin{pmatrix} a & c \\ w & b \end{pmatrix} \text{ avec } x, y, z, w \in \omega^6\mathfrak{o} \text{ et } c\mathfrak{o} = \omega\mathfrak{o}.$$

Soit $\tau = E_{21}(-(1+x)^{-1}w) \in SC_2(\omega^6\mathfrak{o})$. Alors $\tau\phi \in G$ implique que $E_{12}(ca) \in G$, i.e. $G \geq A(\omega\alpha)$ pur un $\alpha \in \mathfrak{u}$.

Pour $m \geq 2$, il s'agit de quotienter (opération \dashv) \mathfrak{o} par $2^{m-1}\omega\mathfrak{o}$, d'utiliser le fait que G contient une image inverse σ de $E_{12}(\bar{\omega}\bar{\alpha})$ avec $\bar{\alpha} \in \bar{\mathfrak{u}}$, de considérer $E_{12}(1)\sigma E_{12}(-1)\sigma^{-1}$ et de constater que $E_{12}(-da) \in G$, pour conclure que $E_{21}(-da^{-1})\sigma \in G$ et obtenir le résultat.

(iii) Sans perte de généralité, supposons $2^4\omega\mathfrak{o} \neq 0$ et quotientons \mathfrak{o} par $2^4\omega\mathfrak{o}$ (opération \dashv). Nous concluons de la partie (ii) qu'il existe un inversible $\bar{\alpha} \in \bar{\mathfrak{u}}$ tel que $\bar{G} \geq A(\bar{\omega}\bar{\alpha}) \geq SC_2(\bar{2}\bar{\omega}\bar{\mathfrak{o}})$. Alors G contient une image inverse σ de $E_{21}(\bar{2}\bar{\omega})$ et la formule 3.1 nous donne la matrice $\Xi\sigma\Xi^{-1}\sigma^{-1}$ dont l'élément (1, 2) engendre $2^3\omega\mathfrak{o}$. Il existe donc $\beta \in \mathfrak{u}$ tel que $G \geq A(2^3\omega\beta) \geq SC_2(2^4\omega\mathfrak{o})$. Comme G contient une image inverse de $E_{12}(\bar{\omega}\bar{\alpha})$ de la forme

$$\phi = \begin{pmatrix} 1+x & \omega\alpha+z \\ w & 1+y \end{pmatrix} = \begin{pmatrix} a & c \\ w & b \end{pmatrix} \text{ avec } x, y, z, w \in 2^4\omega\mathfrak{o} \text{ et } c\mathfrak{o} = \omega\mathfrak{o},$$

alors G contient $\tau\phi$ où τ est choisi comme à la partie (ii). D'où la conclusion. Q.E.D.

Ce théorème n'a pas de réciproque comme en témoigne l'exemple suivant.

EXEMPLE 5.2. Choisissons $A(\omega)$ tel que $A(\omega) < SC_2(\omega\mathfrak{o})$. Soit $x \in \mathfrak{u}$ tel que $x \neq 1 \pmod{\mathfrak{p}}$; il existe $\beta \in \mathfrak{u}$ tel que $\phi = E_{12}(\omega\beta(x^2 + 1)^{-1}) \notin A(\omega)$ et $E_{12}(\omega\beta) \notin A(\omega)$. Supposons que $2\omega\mathfrak{o} = 0$. Alors ϕ est d'ordre 2 et $G = A(\omega) \cup \phi A(\omega)$ est un sous-groupe de $SL_2(\mathfrak{o})$ d'ordre $\omega\mathfrak{o}$ contenant $A(\omega)$. Cependant, si $\rho = \text{Diag}(x, x^{-1}) \in SL_2(\mathfrak{o})$, alors $\rho\phi\rho^{-1}\phi^{-1} = E_{12}(\omega\beta) \notin A(\omega)$, de sorte que $\rho\phi\rho^{-1} \notin G$, i.e. $G \not\triangleleft SL_2(\mathfrak{o})$. Si $2\omega\mathfrak{o} \neq 0$, il s'agit de considérer le groupe G engendré par $\{\phi\} \cup A(\omega)$ et de conclure pour $\bar{\mathfrak{o}} = \mathfrak{o}/2\omega\mathfrak{o}$ que $\bar{G} \triangleleft SL_2(\bar{\mathfrak{o}}) = \overline{SL_2(\mathfrak{o})}$, i.e. $G \triangleleft SL_2(\mathfrak{o})$.

6. Nombre de groupes $A(\omega)$ distincts. On peut déduire facilement du Théorème 4.3 qu'il y a un groupe $A(\omega\alpha)$ par classe d'inversibles mod $u^2 + \mathfrak{J}(\omega)$. On énonce donc explicitement:

PROPOSITION 6.1. *Le nombre de sous-groupes normaux $A(\omega\alpha)$ différents, quand α varie dans \mathfrak{u} , est*

$$l = (\mathfrak{u} : \mathfrak{u}^2 + \mathfrak{J}(\omega)),$$

ce qui peut être infini.

Au besoin, on pourra écrire $l = (\bar{\mathfrak{u}} : \bar{\mathfrak{u}}^2)$ en invoquant le Lemme 4.1.

Couplé aux conclusions de la section précédente, ce résultat-ci mesure en un certain sens combien l'on est loin d'une classification basée sur les transvections.

7. Sur le groupe quotient $SC_2(\omega\mathfrak{o})/A(\omega)$. L'expression particulière que l'on obtient ici pour $SC_2(\omega\mathfrak{o})/A(\omega)$ sera surtout utilisée plus loin lorsque nous considérerons \mathfrak{o} principal, mais elle peut avoir un intérêt en soi si l'on fait le lien avec la dernière remarque ci-dessus.

Nous introduisons maintenant deux groupes S_ω et A_ω , la notation même reflétant le fait que l'on est dans une situation où $\omega^2\mathfrak{o} + 2\omega\mathfrak{o} = 0$. Soit donc dans une telle situation

$$S_\omega = \left\{ \begin{pmatrix} 1 + \omega\beta & \omega\gamma \\ \omega\delta & 1 + \omega\beta \end{pmatrix} \mid \beta, \gamma, \delta \in \mathfrak{o} \right\} \text{ et}$$

$$A_\omega = \left\{ \begin{pmatrix} 1 + \omega\beta & \omega\gamma^2 \\ \omega\delta^2 & 1 + \omega\beta \end{pmatrix} \mid b, \gamma, \delta \in \mathfrak{o} \right\}.$$

On vérifie facilement que $S_\omega = SC_2(\omega\mathfrak{o})$. On a aussi $A_\omega = A(\omega)$; en effet, $A(\omega) \subseteq A_\omega$, étant donné qu'un élément typique de $A(\omega)$ est de la forme

$$\sigma = \prod_{i=1}^r \rho_i E_{12}(\pm\omega)\rho_i^{-1} \text{ avec } \rho_i = \begin{pmatrix} a_i & c_i \\ d_i & b_i \end{pmatrix} \in SL_2(\mathfrak{o}),$$

i.e. est de la forme

$$\sigma = \begin{pmatrix} 1 + \omega(a_1d_1 + a_2d_2 + \dots + a_r d_r) & \omega(a_1 + a_2 + \dots + a_r)^2 \\ \omega(d_1 + d_2 + \dots + d_r)^2 & 1 + \omega(a_1d_1 + a_2d_2 + \dots + a_r d_r) \end{pmatrix};$$

comme un élément typique de A_ω s'écrit sous la forme

$$E_{21}(\omega\delta^2)\text{Diag}(1 + \omega\beta, 1 + \omega\beta)E_{12}(\omega\gamma^2),$$

et comme $\text{Diag}(1 + \omega\beta, 1 + \omega\beta) = E_{21}(\omega\beta^2)E_{21}(\beta)E_{12}(\omega)E_{21}(-\beta)E_{12}(\omega) \in A(\omega)$, alors $A_\omega \subseteq A(\omega)$. Remarquons que tout élément de A_ω est d'ordre 2.

PROPOSITION 7.1. Si—représente les homomorphismes

$$—: \mathfrak{o} \rightarrow \mathfrak{o}/\omega^2\mathfrak{o} + 2\omega\mathfrak{o} \quad \text{et} \quad —: SL_2(\mathfrak{o}) \rightarrow SL_2(\bar{\mathfrak{o}}),$$

alors $SC_2(\omega\mathfrak{o})/A(\omega) \cong S_{\bar{\omega}}/A_{\bar{\omega}}$.

Démonstration. C'est une conséquence du fait que le noyau de l'homomorphisme—restreint à $A(\omega)$ est égal à $SC_2(\omega^2\mathfrak{o} + 2\omega\mathfrak{o})$. Q.E.D.

8. Résultats particuliers avec un anneau principal. Supposons maintenant que \mathfrak{o} est principal et la cardinalité $N\mathfrak{p}$ de $\mathfrak{o}/\mathfrak{p}$ est finie, donc égale à 2^h . Alors $\mathfrak{o}/\mathfrak{p}$ est parfait.

Si $\mathfrak{p}^n \neq 0$ et $\mathfrak{p}^{n+1} = 0$, alors $SC_2(\mathfrak{p}^n)$ est isomorphe à une somme directe de $3h$ copies de \mathbb{Z}_2 , de sorte que si $\mathfrak{p}^{n+1} \neq 0$,

$$(SC_2(\mathfrak{p}^n) : SC_2(\mathfrak{p}^{n+1})) = (N\mathfrak{p})^3 = (2^h)^3.$$

Soit $\mathfrak{p}^{2n} + 2\mathfrak{p}^n = 0$ et soit $\alpha \in \mathfrak{u}$. Alors il existe un entier $s, 1 \leq s \leq n$, tel que $\mathfrak{p}^{n+s} = 0$ et $\mathfrak{p}^{n+s-1} \neq 0$. Grâce à la section 7, il est facile de vérifier que pour $\alpha \in \mathfrak{u}$,

$$A(\pi^n\alpha) \cong \text{somme directe de } \begin{cases} 2sh \text{ copies de } \mathbb{Z}_2 & \text{si } s \text{ est pair,} \\ (2s+1)h \text{ copies de } \mathbb{Z}_2 & \text{si } s \text{ est impair,} \end{cases}$$

$$(SC_2(\mathfrak{p}^n) : A(\pi^n\alpha)) = \begin{cases} (N\mathfrak{p})^s & \text{si } s \text{ est pair,} \\ (N\mathfrak{p})^{s-1} & \text{si } s \text{ est impair.} \end{cases}$$

PROPOSITION 8.1. Soit \mathfrak{o} principal avec $N\mathfrak{p}$ fini (≥ 4) et $2\mathfrak{o} = \mathfrak{p}^k$ où $k \geq 1$ et soit $\alpha \in \mathfrak{u}$. Soit $\mathfrak{p}^n \neq 0$. Alors

$$(SC_2(\mathfrak{p}^n) : A(\pi^n\alpha)) = \begin{cases} (N\mathfrak{p})^n & \text{si } n < k \text{ est pair,} \\ (N\mathfrak{p})^{n-1} & \text{si } n < k \text{ est impair,} \\ (N\mathfrak{p})^k & \text{si } n \geq k \text{ et si } k \text{ est pair,} \\ (N\mathfrak{p})^{k-1} & \text{si } n \geq k \text{ et si } k \text{ est impair,} \end{cases}$$

lorsque $\mathfrak{p}^{2n} + 2\mathfrak{p}^n \neq 0$. Dans le cas contraire, les deux exposants sont s et $s - 1$, où s est l'entier tel que $\mathfrak{p}^{n+s} = 0, \mathfrak{p}^{n+s-1} \neq 0$.

Démonstration. Dans le cas où $\mathfrak{p}^{2n} + 2\mathfrak{p}^n = 0$, on invoque ce qui précède l'énoncé de la proposition. Autrement, on quotiente \mathfrak{o} par $\mathfrak{p}^{2n} + 2\mathfrak{p}^n$. Q.E.D.

PROPOSITION 8.2. Soit \mathfrak{o} principal avec $N\mathfrak{p}$ fini (≥ 4) et $2\mathfrak{o} = \mathfrak{p}^k$ avec $k \geq 1$. Soit $\mathfrak{p}^n \neq 0$. Alors le nombre de sous-groupes normaux $A(\pi^n\alpha)$ différents quand α

varie dans u est

$$l = \begin{cases} (Np)^{n/2} & \text{si } n < k \text{ est pair,} \\ (Np)^{(n-1)/2} & \text{si } n < k \text{ est impair,} \\ (Np)^{k/2} & \text{si } n \geq k \text{ et si } k \text{ est pair,} \\ (Np)^{(k-1)/2} & \text{si } n \geq k \text{ et si } k \text{ est impair,} \end{cases}$$

lorsque $p^{2n} + 2p^n \neq 0$. Dans le cas contraire, les deux exposants sont $s/2$ et $(s - 1)/2$, où s est l'entier tel que $p^{n+s} = 0$, $p^{n+s-1} \neq 0$.

Démonstration. Il est facile de voir que $\mathfrak{Z}(\pi^n) = p^n + 2v$. Posons $\mathfrak{Z}(\pi^n) = p^s$ et $\bar{v} = v/p^s$; notons que $2\bar{v} = \bar{0}$ et que $N\bar{p} = Np$. La cardinalité de \bar{u}^2 est

$$|\bar{u}^2| = \begin{cases} (Np - 1)(Np)^{(s-2)/2} = |\bar{u}|/(Np)^{s/2} & \text{si } s \text{ est pair,} \\ (Np - 1)(Np)^{(s-1)/2} = |\bar{u}|/(Np)^{(s-1)/2} & \text{si } s \text{ est impair.} \end{cases}$$

Donc (rappelant le lemme 4.1), nous obtenons

$$(u : u^2 + \mathfrak{Z}(\pi^n)) = (\bar{u} : \bar{u}^2) = \begin{cases} (Np)^{s/2} & \text{si } s \text{ est pair,} \\ (Np)^{(s-1)/2} & \text{si } s \text{ est impair.} \end{cases}$$

D'où la conclusion, à cause de la proposition 6.1. Q.E.D.

Les deux propositions permettent de constater que l'écart entre $SC_2(p^n)$ et $A(\pi^n\alpha)$ se mesure par l^2 . Cette "coïncidence" s'explique par le fait que parler de l et l^2 équivaut à parler de $s/2$ (ou $(s - 1)/2$) et de s (ou $s - 1$) respectivement, où s quantifie l'écart entre p^n et $0 = p^{n+s}$, où $p^{n+s-1} \neq 0$; les calculs en détail font voir que le tout est basé sur les congruences auxquelles on doit avoir recours.

9. Calcul d'indices. Cette dernière section sert de complément d'information pour son intérêt en soi et en vue d'un usage possible par quiconque poursuivrait l'étude de questions en suspens. En effet, le rôle joué au cours de la preuve de la Proposition 8.2 par l'indice $(u : u^2(1 + \mathfrak{Z}(\pi^n)))$ nous suggère d'évaluer de façon générale l'indice $(u : u^2(1 + p^s))$, où $s \in \mathbb{N}$. Nous voulons donc grouper ensemble quelques résultats sur certains groupes d'unités où par souci de généralité, nous permettons le cas $Np = 2$.

On écrit $\text{ord } \alpha$ pour l'entier r tel que $\alpha v = \pi^r v = p^r$.

PROPOSITION 9.1. *Supposons que v est l'anneau des entiers d'un corps local dyadique avec $2 \in p$, $p = \pi v$ et $Np \geq 2$. Alors*

- (i) $(1 + p^s : 1 + p^{s+1}) = Np$,
- (ii) $(u : 1 + p^s) = (Np - 1)(Np)^{s-1}$,
- (iii) $(u : u^2) = 2(Np)^{\text{ord}2}$,

$$(iv) \quad u^2 \cap (1 + p^s) = \begin{cases} (1 + p^{s/2})^2 & \text{si } p^s \geq 4v \text{ et si } s \text{ est pair,} \\ (1 + p^{(s+1)/2})^2 & \text{si } p^s \geq 4v \text{ et si } s \text{ est impair,} \\ 1 + p^s = (1 + p^{s-\text{ord}2})^2 & \text{si } p^s \leq 4p, \end{cases}$$

$$(v) \quad ((1+p^s):(1+p^s)^2) = \begin{cases} 2(Np)^{ord2} & \text{si } p^s \geq 2v, \\ (Np)^{ord2} & \text{si } p^s \leq 2p, \end{cases}$$

$$(vi) \quad (u:u^2(1+p^s)) = \begin{cases} (Np)^{s/2} & \text{si } p^s \geq 4v \text{ et si } s \text{ est pair,} \\ (Np)^{(s-1)/2} & \text{si } p^s \geq 4v \text{ et si } s \text{ est impair,} \\ 2(Np)^{ord2} & \text{si } p^s \leq 4p. \end{cases}$$

Démonstration. Les parties (i), (ii) et (iii) proviennent de la page 163 de [3].

(iv) Si $p^s \leq 4p$, le résultat découle du théorème du carré local ([3], p. 159). Le cas où $p^s \geq 4v$ est laissé au lecteur.

(v) Il s'agit d'appliquer le lemme 63.7 de [3] et de poser $G = 1 + p^s$, $H = 1 + 2p^s$ et $\theta(\alpha) = \alpha^2$ pour tout $\alpha \in G$.

(vi) Nous pouvons noter que $u^2(1+p^s) = u^2(1+p^{s+1})$ si $p^s \geq 4v$ avec s pair. Etant donné que $(u:u^2) = (u:u^2(1+p^s))(u^2(1+p^s):u^2)$ et que $(u^2(1+p^s):u^2) = (1+p^s:u^2 \cap (1+p^s))$, nous pouvons tirer la conclusion appropriée. Q.E.D.

BIBLIOGRAPHIE

1. W. Klingenberg, *Lineare Gruppen über lokalen Ringen*, Amer. J. Math. **83** (1961), 137–153.
2. N. H. J. Lacroix, *Two-dimensional Linear Groups Over Local Rings*, Can. J. Math. **21** (1969), 106–135.
3. O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, Berlin, 1963.

UNIVERSITÉ LAVAL,
QUÉBEC, CANADA