Zorn’s Matrices and finite index subloops

Carmen Rosa Giraldo Vergara
Instituto de Matemática, Universidade Federal do Rio de Janeiro
CEP 21945-970, Rio de Janeiro, Brasil
E-mail: carmita@pg.im.ufrj.br

Fabio Enrique Brochero Martínez
Instituto de Matemática Pura e Aplicada
CEP 22460-320, Rio de Janeiro RJ, Brasil
E-mail: fbrocher@impa.br

Abstract

The Zorn’s Algebra \( \mathcal{Z}(R) \) has a multiplicative function called determinant with properties similar to the usual one. The set of elements in \( \mathcal{Z}(R) \) with determinant 1 is a Moufang loop that we will denote by \( \mathbb{I} \). In our main result we prove that if \( R \) is a Dedekind algebraic number domain that contains an infinite order unit, each finite index subloop \( \mathcal{L} \), such that \( \mathbb{I} \) has the weak Lagrange property relative to \( \mathcal{L} \), is congruence subloop. In addition, if \( R = \mathbb{Z} \), then we present normal subloops of finite index in \( \mathbb{I} \) that are not congruence subloops.

1 Introduction

Let \( R \) be a commutative ring with unit 1, \( I \) an ideal of \( R \) and \( SL(n, R) \) the \( n \times n \) special linear group over \( R \). The principal congruence group of level \( I \)

\footnote{2000 Mathematics Subject Classification: Primary 20N05, 20H05; Secondary 17D05. This research was supported by CNPq, Brasil.}
in $SL(n, R)$ is a set of matrices congruent to the identity modulo the ideal $I$. It said that $SL(n, R)$ satisfies the congruence subgroups property if every finite index subgroup contains a principal congruence group.

In the last decades the congruence groups achieved own relevance, different from the traditional application in the geometric field about the classification of elliptic curves over $\mathbb{C}$ and the study of modular forms. This relevance is due to the works of Mennicke, Serre, Lazard, Bass, Vaseršteı̇n, Newman and some others. Mennicke [5] proved that $SL(n, \mathbb{Z})$ with $n \geq 3$ satisfies the congruence subgroups property. In addition Bass, Milnor, Serre [4] proved that $SL(n, R)$ satisfies that property for $n \geq 3$ for an ample variety of rings (in particular for any ring of algebraic numbers). For $n = 2$, Wohlfahrt (See [7]) showed a criterion of determining when a finite index subgroup is a congruence group, and used this criterion to show that in $SL(2, \mathbb{Z})$ exists finite index subgroups that is not congruence subgroup. In general,

**Theorem 1.1 (Serre [8])** Let $R$ be an algebraic integer domain that contains an infinite order unit. Then $SL(2, R)$ satisfies the congruence subgroups property.

In that article, Serre also proved that if $R$ is an algebraic integer ring $\mathcal{O}_d$ of the field $\mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{N}^*$, then the group $SL(2, \mathcal{O}_d)$ does not have the congruence subgroups property.

In addition, Vaseršteı̇n showed a relationship between congruence subgroup and groups generated by elementary matrices when $R$ is a Dedekind algebraic domain that contains infinitely many units.

**Theorem 1.2 (Vaseršteı̇n [9])** Let $R$ be a Dedekind algebraic numbers domain that contains infinitely many units, $\mathfrak{q}$ an ideal of $R$ and $E(\mathfrak{q})$ the subgroup generated by the matrices \( \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \) with $a \in \mathfrak{q}$. Then the group $E(\mathfrak{q})$ has finite index in $SL(2, R)$, in particular $E(R) = SL(2, R)$.

On the other side, Zorn’s algebra $3(R)$ contains Moufang loops analogous to the groups $GL(2, R)$ and $SL(2, R)$. In fact, denote by $R^3$ the three
dimensional vector space over $R$. Zorn’s Algebra $\mathcal{Z}(R)$ over $R$ is the set of $2\times 2$ matrices

$$\begin{bmatrix} a & x \\ y & b \end{bmatrix} \quad a, b \in R \quad x, y \in R^3,$$

with the binary operations sum and product, where the sum is defined by the natural form, component to component, and the product is given by the rule

$$\begin{bmatrix} a_1 & x_1 \\ y_1 & b_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & x_2 \\ y_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + x_1\cdot y_2 & a_1x_2 + b_2x_1 - y_1\times y_2 \\ a_2y_1 + b_1y_2 + x_1\times x_2 & b_1b_2 + y_1\cdot x_2 \end{bmatrix}$$

where $\cdot$ and $\times$ denote the dot and cross vectorial product in $R^3$.

The determinant function $\det : \mathcal{Z}(R) \to R$ defined by $\det(A) = ab - x\cdot y$, where $A = \begin{bmatrix} a & x \\ y & b \end{bmatrix}$, is a multiplicative function. Thus, an element $A$ is invertible if and only if $\det(A) \in R^*$ and then $A^{-1} = \frac{1}{\det A} \begin{bmatrix} b & -x \\ -y & a \end{bmatrix}$.

Zorn’s Algebra is alternative, it follows that the invertible elements set is a Moufang Loop. This set is called a general linear loop and it is denoted by

$$\text{GLL}(2, R) = \{ A \in \mathcal{Z}(R) | \det(A) \in R^* \}.$$

Similarly, we define the special linear loop as follows

$$\Gamma = \text{SLL}(2, R) = \{ A \in \text{GLL}(2, R) | \det A = 1 \}.$$

We are going to developed for loops an analogue theory to the congruences groups theory, where $R$ is a Dedekind algebraic numbers domain. In particular, if $R$ contains an infinite order unit, we will prove an analogous Serre’s Theorem for these loop. In addition, if $R = \mathbb{Z}$, we find a family of finite index subloops that are not congruence loops.

2 Congruence subloop and finite index subloop

Let $q$ be an ideal of $R$. We define a principal congruence subloop of $\Gamma$ of level $q$ as a set of all matrices $A$ of $\Gamma$ such that

$$A \equiv I \pmod{q},$$

$$\text{GLL}(2, R) = \{ A \in \mathcal{Z}(R) | \det(A) \in R^* \}.$$
where the congruence is component by component. This loop is denoted by $\Gamma(q)$. In particular, $\Gamma(R) = \Gamma$. A subloop of $\Gamma$ is called a congruence subloop if it contains a principal congruence subloop $\Gamma(q)$ for some ideal $q$ of $R$.

In the follow, $R$ denote a Dedekind domain, and for each non zero ideal of $R$, $\Delta(q)$ denotes the smallest normal subloop of $\Gamma$ that contains every matrix of the form 
\[
\begin{bmatrix}
1 & x \\
0 & 1
\end{bmatrix}, \begin{bmatrix}
1 & 0 \\
y & 1
\end{bmatrix}
\]
where $x, y \in q^3$.

**Definition 2.1** Let $\mathcal{L}$ be a subloop of $\Gamma$, and suppose that the set 
\[S = \{q \subset R | \Delta(q) \subset \mathcal{L}\}\]
is not empty. Define the level of $\mathcal{L}$ as the maximal element of $S$.

**Lemma 2.1** Let $q$ be an non zero ideal of $R$ and $A \in \Gamma(q)$. If $A = \begin{bmatrix} v \\ 1 \\ u \end{bmatrix}$, then $A$ can be written as product of the matrices 
\[
\begin{bmatrix}
1 & \ae_j \\
0 & 1
\end{bmatrix}
\]
and 
\[
\begin{bmatrix}
1 & 0 \\
\ae_j & 1
\end{bmatrix}
\]
where $a \in q$, $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ and $e_3 = (0,0,1)$.

**Proof.** First, suppose $A$ has the form 
\[
\begin{bmatrix}
1 & (0,0,0) \\
(u_1, u_2, u_3) & 1
\end{bmatrix}
\]
then define
\[
B = \begin{bmatrix}
1 \\
(0, u_2, u_3)
\end{bmatrix}
\]
\[
\begin{bmatrix}
0 \\
1
\end{bmatrix}
\]
\[
\in \Gamma(q), \text{ thus}
\]
\[
A = B + \begin{bmatrix}
u e_1 \\
0
\end{bmatrix}
\]
\[
= B \left(I + B^{-1} \begin{bmatrix}
0 \\
u e_1
\end{bmatrix} \right)
\]
\[
= B \begin{bmatrix}
1 \\
(0, u_1, 0)
\end{bmatrix}
\begin{bmatrix}
0 \\
1
\end{bmatrix}
\begin{bmatrix}
0, u_1 u_3, -u_1 u_2 \\
1
\end{bmatrix}
\]
By the same procedure, we obtain that 
\[
B = \begin{bmatrix}
1 \\
u e_3
\end{bmatrix}
\begin{bmatrix}
1 \\
u e_3
\end{bmatrix}
\begin{bmatrix}
1 \\
u e_2
\end{bmatrix}
\]
and
\[
\begin{bmatrix}
1 & (0, u_1 u_3, -u_1 u_2) \\
0 & 1
\end{bmatrix}
= \begin{bmatrix}
1 & -u_1 u_2 e_3 \\
0 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 \\
u_1^2 u_2 u_3 e_1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & u_1 u_3 e_2 \\
0 & 1
\end{bmatrix}
\]

In the general case, if 
\[A = \begin{bmatrix}
1 & (v_1, v_2, v_3) \\
(u_1, u_2, u_3) & b
\end{bmatrix},\]
we have 
\[A = ((CA_3)A_2)A_1\]
where 
\[A_j = \begin{bmatrix}
1 & v_j e_j \\
0 & 1
\end{bmatrix}\]
and 
\[C = \begin{bmatrix}
1 & (u_1 + v_3 v_2, u_2 - v_3 v_1, u_3 + v_2 v_1) \\
0 & 1
\end{bmatrix}
\]
The result follows from the first case. ■

Let \(\Gamma_j(q)\) denote a subloop
\[\Gamma_j(q) := \left\{ \begin{bmatrix} a & b \\ c e_j & d \end{bmatrix} \in \Gamma \left| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv I \pmod{q} \right. \right\} \quad \text{and} \quad G\Gamma_j := G\Gamma_j(R).
\]

We are going to show that these three subloops generate the loop \(\Gamma(q)\), but before we need a result from commutative ring theory. Let \(R\) be a commutative ring with unit 1, and \(M\) be a \(R\)-module. \(R\) is called a local ring if there is an unique local maximal ideal, and when there are a finite number of maximal ideals, it is called semilocal. An element \(x \in M\) is called unimodular if there is a linear form \(L : M \to R\) such that \(L(x) = 1\).

**Lemma 2.2** Let \(x = (x_1, \ldots, x_m)\) be an unimodular element of \(R^m\). If \(R\) is a semilocal noetherian ring, then there are \(y_2, \ldots, y_m \in R\) such that
\[x_1 + y_2 x_2 + \cdots + y_m x_m
\]
is invertible in \(R\).

**Proof.** See [1] page 386. ■

**Theorem 2.1** Let \(R\) be a Dedekind domain. For every \(q\) non zero ideal of \(R\), \(\Gamma(q)\) is generated by \(\Gamma_1(q), \Gamma_2(q)\) and \(\Gamma_3(q)\).

**Proof.** Let \(\mathcal{L} = \langle \Gamma_1(q), \Gamma_2(q), \Gamma_3(q) \rangle\). It is clear that \(\mathcal{L} \subset \Gamma(q)\), thus, we only need to show \(\Gamma(q) \subset \mathcal{L}\). Let \(A \in \Gamma(q)\), i.e., \(A\) is a matrix of the
form \[ \begin{bmatrix} a \\ (v_1, v_2, v_3) \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \] with \( ab - (v_1u_1 + v_2u_2 + v_3u_3) = 1 \) and \( a \) and \( b \) congruent to 1 modulo \( q \), in particular, \( a \neq 0 \). If \( q = R \) and \( a = 0 \), since \( ab - (v_1u_1 + v_2u_2 + v_3u_3) = 1 \), there is \( j \) such that \( v_ju_j \neq 0 \). It follows that it is sufficient to prove

\[ T_jA = \begin{bmatrix} e_j \cdot u & be_j + e_j \times v \\ -ae_j + e_j \times v & -e_j \cdot v \end{bmatrix} \]

is in \( L \), and therefore we can suppose, in this case too, that \( a \neq 0 \).

Since \( R \) is Dedekind, \( \mathbb{R}_a \) is a semilocal ring and \((-v_1)u_1 + (-u_2)v_2 + (-u_3)v_3 \equiv 1 \pmod{a} \), thus \((u_1, v_2, v_3)\) is unimodular in \( \mathbb{R}_a^3 \). Therefore from the lemma 2.3, exist \( t \) and \( s \) such that \( u_1 + v_2t + v_3s = u_1' \) is invertible in \( \mathbb{R}_a \) and it follows that \( a \) and \( u_1' \) are relative primes. Define

\[ u_2' = -v_1t + u_2 \quad \text{and} \quad u_3' = -v_1s + u_3. \]

It is easy to prove that \( B = \begin{bmatrix} a \\ (v_1, v_2, v_3) \end{bmatrix} \begin{bmatrix} u_1' \\ u_2' \\ u_3' \end{bmatrix} \in \mathbb{I}(q) \) and

\[ A = B \begin{bmatrix} 1 \\ -(u_2'v_3 - u_3'u_2, u_3'u_1 - u_1'u_3, u_1'u_2 - u_2'u_1) \end{bmatrix} B(u_1 - u_1', u_2 - u_2', u_3 - u_3') \]

It follows from lemma 2.1 that we only need to prove that \( B \in \mathcal{L} \). Let \( q \) be an arbitrary element of \( q^* \). Since \((a, qu_1') = 1 \), there are \( x, y \) integer numbers such that \( ax + qu_1'y = 1 \). But \( a \equiv 1 \pmod{q} \), therefore \( x \equiv 1 \pmod{q} \) and

\[ \begin{bmatrix} a \\ (-qy, 0, 0) \end{bmatrix} \in \mathbb{I}(1)(q). \]

Thus

\[ \begin{bmatrix} a \\ (v_1, v_2, v_3) \end{bmatrix} \begin{bmatrix} u_1' \\ u_2' \\ u_3' \end{bmatrix} = \begin{bmatrix} (xu_1 + bqu_2, xu_2 - u_1'u_1, xu_3 + u_2'u_1) \\ (xv_1 + bqu_2, xv_2 - u_1'u_1, xv_3 + u_2'u_1) \end{bmatrix} \begin{bmatrix} a \\ (-qy, 0, 0) \end{bmatrix} \]

Finally, lemma 2.1 shows that \( B \in \mathcal{L} \).

**Corollary 2.1** Let \( R \) be a Dedekind algebraic domain that contains infinitely many units. Then \( \mathbb{I} \) is generated by the matrices \( \begin{bmatrix} 1 \\ 0 \end{bmatrix} \) and \( \begin{bmatrix} 1 \\ ae_j \end{bmatrix} \), where \( a \in R \) and \( j = 1, 2, 3 \).
Proof. It follows from Vaseršteǐn theorem. □

The following theorem is a generalization of Wohlfahrt’s criterion to $\Pi$. 

**Theorem 2.2** Let $q_1, q_2$ be ideals of the Dedekind domain $R$. Then $\Pi(q_1) \subseteq \Delta(q_1)\Pi(q_2)$.

**Proof.** This proof is similar to the proof of Wohlfahrt’s theorem made by Mason and Stothers (see [4]). Let $A = \begin{bmatrix} a & (v_1, v_2, v_3) \\ (u_1, u_2, u_3) & b \end{bmatrix}$ be an arbitrary element of $\Pi(q_1)$, we need to find $B \in \Delta(q_1)$ such that $A \equiv B \pmod{q_2}$, and therefore $A = B(B^{-1}A)$ where $B^{-1}A \in \Pi(q_2)$.

*Case 1:* If $a \equiv 1 \pmod{q_2}$, then it is sufficient to take $B = \begin{bmatrix} 1 & (v_1, v_2, v_3) \\ (u_1, u_2, u_3) & ab \end{bmatrix}$, because lemma 2.1 shows that $B \in \Delta(q_1)$. In addition,

$$B^{-1}A = \begin{bmatrix} a^2b - (u_1v_1 + u_2v_2 + u_3v_3) & (ab - b)(v_1, v_2, v_3) \\ (1 - a)(u_1, u_2, u_3) & b - (u_1v_1 + u_2v_2 + u_3v_3) \end{bmatrix}$$

Thus $A \in \Delta(q_1)\Pi(q_2)$.

*Case 2:* If $(a, q_2) = 1$, then the congruence $ax \equiv 1 \pmod{q_2}$ has solution. Let $a'$ be a solution, $c = gcd(v_1, v_2, v_3)$, $v'_j = \frac{v_j}{c}$ for $j = 1, 2, 3$ and $X = \begin{bmatrix} 1 & a'(1 - a - c)(v'_1, v'_2, v'_3) \\ (0, 0, 0) & 1 \end{bmatrix}$. Notice that $a'(1 - a - c)$ is in $q_1$ since $1 - a \in q_1$ and $c \in q_1$, thus $X \in \Delta(q_1)$. In addition,

$$AX \equiv \begin{bmatrix} a & (1 - a)(v'_1, v'_2, v'_3) \\ (u_1, u_2, u_3) & b + a'(1 - a - c)(\frac{ab - 1}{c}) \end{bmatrix} \pmod{q_2}.$$ 

Define $T_1 = \begin{bmatrix} 1 & (0, 0, 0) \\ (t_1, t_2, t_3) & 1 \end{bmatrix}$ where $v'_1t_1 + v'_2t_2 + v'_3t_3 = 1$. We have

$$T_1^{-1}(AX)T_1 \equiv \begin{bmatrix} 1 & * \\ * & * \end{bmatrix} \pmod{q_2}.$$ 

7
It follows from Case 1 that \( T_1^{-1}(AX)T_1 \equiv B \pmod{q_2} \) for some \( B \in \Delta(q_1) \), therefore \( A \equiv (T_1BT_1^{-1})X^{-1} \pmod{q_2} \), with \( (T_1BT_1^{-1})X^{-1} \in \Delta(q_1) \).

Case 3: In the general case, denoting \( d = (u_1v_1 + u_2v_2 + u_3v_3) \), we have \( ab - d = 1 \). Then \( (a, d) \) seen as an element of \( \left( \mathcal{R}_{q_2} \right)^2 \) is unimodular, and since \( \mathcal{R}_{q_2} \) is semilocal ring, from lemma 2.2, exists \( t \) such that \( a - td \) is invertible in \( \mathcal{R}_{q_2} \). Define \( T = \begin{bmatrix} 1 & (0, 0, 0) \\ -t(u_1, u_2, u_3) & 1 \end{bmatrix} \), then

\[
T^{-1}AT = \begin{bmatrix} a - td & (v_1, v_2, v_3) \\ -(at - 1 + bt + t^2d)(u_1, u_2, u_3) & b + td \end{bmatrix},
\]

where \( (a + td, q_2) = 1 \), and from Case 2, \( T^{-1}AT \equiv B \pmod{q_2} \) for some \( B \in \Delta(q_1) \). Therefore \( A \equiv TBT^{-1} \pmod{q_2} \), with \( TBT^{-1} \in \Delta(q_1) \).

**Corollary 2.2** Let \( L \) be a congruence subloop of \( \Gamma \) of level \( q \). Then \( L \supset \Gamma(q) \).

**Proof.** Since \( L \) is a congruence subloop, then there is an ideal \( q' \) such that \( \Gamma(q') \subset L \), furthermore \( \Delta(q) \subset L \), then \( \Gamma(q) \subset \Delta(q) \Gamma(q') \subset L \). ■

To show a generalization of Serre’s Theorem to \( \Gamma \), we need the following fact about Loop Theory

**Definition 2.2** Let \( L \) be a loop with the inverse property and \( H \) a subloop of \( L \). We said that \( L \) has the Lagrange property relative to \( H \), if \( L \) and \( H \) satisfy one of the following equivalent conditions (see [3] page 52)

1. \( Hx \cap Hy \neq \emptyset \), \( x, y \in L \) if and only if \( Hx = Hy \).
2. \( H(hx) = Hx \) for all \( x \in L \) and \( h \in H \)

We said that \( L \) has the weak Lagrange property relative to \( H \), if there exists \( F \), finite index subloop of \( H \), such that \( L \) has the Lagrange property relative to \( F \).
Observe that if $H$ is normal subloop of $L$, then $L$ has the Lagrange property relative to $H$, and there exist subloops, such that $\Gamma$ have not the Lagrange property relative to these subloops. For instance, $I_\Gamma(1) \subset \{ [0 (a,b,c) (0,d,e) c] \in I_\Gamma \}$ and $\Gamma(1) = [2,3,2] \notin \Gamma \Gamma(1) \{ 1 e_1 = (1) e_1 = 0 e_1 + e_2 - e_2 + e_3 0 \} = (0, -3, 4) 3 \notin \Gamma \Gamma(1) \{ 1 e_1 = (1) e_1 = 0 e_1 + e_2 - e_2 + e_3 0 \}$, thus $\Gamma$ has not the Lagrange property relative to $G_A(1)$. Similarly, $\Gamma$ has not the Lagrange property relative to $\Gamma(1) \Gamma(n)$, for all $n \geq 2$. In addition, when $L$ has the Lagrange property relative to $H$, there exists a subset $T$ of $\mathcal{H}$ called a transversal of $H$ such that $L = \bigcup_{x \in T} \mathcal{H}x$ with $\mathcal{H}x \cap \mathcal{H}y = \emptyset$ for $x, y \in T$.

**Lemma 2.3** Let $L$ be a loop with the inverse property and suppose that $\mathcal{H}$ is a finite index subloop of $L$ such that $L$ has the Lagrange property relative to $\mathcal{H}$. Let $F$ be a subloop of $L$. Then $\mathcal{H} \cap F$ is a finite index subloop of $F$ and $F$ has the Lagrange property relative to $\mathcal{H} \cap F$.

**Proof.** For all $a \in \mathcal{H} \cap F$ and $f \in F$, we have

$$(\mathcal{H} \cap F)(af) = \mathcal{H}(af) \cap F(af) = \mathcal{H}f \cap Ff = (H \cap F)f,$$

thus $F$ has the Lagrange property relative to $H \cap F$. Let $n = [L : H]$ and $T = \{ t_1, \ldots t_n \}$ a transversal of $\mathcal{H}$. We can suppose that $\mathcal{H}t_j \cap F \neq \emptyset$ if and only if $j \leq m$ for some $m \leq n$, thus $F = \bigcup_{j=1}^{m} \mathcal{H}t_j \cap F$. Let $s_j$ be an arbitrary element of $\mathcal{H}t_j \cap F$. We claim that $(\mathcal{H} \cap F)s_j = \mathcal{H}t_j \cap F$. In fact, since $s_j = ht_j$ for some $h \in \mathcal{H}$, then

$$(\mathcal{H} \cap F)s_j = \mathcal{H}(ht_j) \cap Fs_j = \mathcal{H}t_j \cap F, \text{ thus } [\mathcal{H} \cap F : F] = m. \quad \blacksquare$$

**Theorem 2.3** Let $R$ be a Dedekind algebraic integer domain, and suppose that $R$ contains an infinite order unit. If $L$ is a finite index subloop of $\Gamma$ and $\Gamma$ has the weak Lagrange property, then $L$ is a congruence subloop.
Proof. Let $\mathcal{F}$ be a finite index subloop of $\mathcal{H}$, such that $\Gamma$ has the Lagrange property relative to $\mathcal{F}$. From lemma 2.3 follows

$$[\Gamma_{(j)} : \Gamma_{(j)} \cap \mathcal{F}] \leq [\Gamma : \mathcal{F}] \leq [\Gamma : \mathcal{L}][\mathcal{L} : \mathcal{F}] < \infty.$$ 

Then from Serre’s Theorem follows that there are ideals $q_j$ for $j = 1, 2, 3$, such that $\Gamma_{(j)}(q_j) \subset \mathcal{F} \cap \Gamma_{(j)} \subset \mathcal{L}$. Define $q = q_1 \cap q_2 \cap q_3$, then $\Gamma_{(j)}(q) \subset \mathcal{L}$ for $j = 1, 2, 3$, and from theorem 2.1 follows that $I_{\Gamma}(q) \subset \mathcal{F} \subset \mathcal{L}$. ■

Proposition 2.1 Let $R$ be a Dedekind algebraic integer domain with an infinite order unit and $q$ an ideal of $R$. Then $\Delta(q) = \Gamma(q)$.

Proof. From Varserštai theorem $\Delta(q) \cap \Gamma_{(j)}$ is a finite index subgroup of $\Gamma_{(j)}$, then from Serre’s Theorem there are $q_j$ ideals such that $\Gamma_{(j)}(q_j) \subset \Delta(q) \cap \Gamma_{(j)} \subset \Delta(q)$. Thus, from theorem 2.1 follows that $I_{\Gamma}(q') \subset \Delta(q)$ where $q' = q_1 \cap q_2 \cap q_3$. Finally, from corollary 2.2 follows that $\Delta(q) = I_{\Gamma}(q)$. ■

3 The Loop $SLL(2, \mathbb{Z})$

In this section, $\Gamma$ denotes the loop $SLL(2, \mathbb{Z})$. For each $n \geq 1$ $\Gamma(n)$ is a principal congruence subloop of level $n$ and $\Gamma'(n)$ is a subloop of $\Gamma(n)$ generated by the associators and commutators, i.e., the smallest loop that contains any element of the form

$$[A, B] = ABA^{-1}B^{-1} \quad \text{and} \quad [A, B, C] = ((AB)C)(A(BC))^{-1},$$

with $A, B$ and $C \in \Gamma(n)$. For $j = 1, 2, 3$, we denote

$$T_j = \begin{bmatrix} 0 & e_j \\ -e_j & 0 \end{bmatrix} \quad S_j = \begin{bmatrix} 1 & e_j \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad U_j = \begin{bmatrix} 0 & e_j \\ -e_j & 1 \end{bmatrix}$$

Observe that $\Gamma_{(j)} \cong SL(2, \mathbb{Z})$ for each $j = 1, 2, 3$. Specially, $\Gamma_{(j)}$ is generated by two of the following matrices $T_j$, $S_j$ and $U_j$ (See [1] pag 139).

Proposition 3.1 $\Gamma$ has minimal set of generators $\{S_1, S_2, U_3\}$. In general, for every positive integer $n$, $\Gamma(n)$ is finitely generated.
Proof. Since $T_1$, $T_2$, $S_3$ and $T_3$ can be written as a product of $S_1$, $S_2$ and $U_3$ (see [14] pag 190) and $\Gamma$ is dissociative, it follows that this is a minimal set of generator. For every $n > 1$, each $\Gamma(j)(n)$ are finitely generated free groups. The proposition follows as a trivial consequences of theorem 2.1. ■

Remark 3.1 From proof of theorem 2.1, we can observe that $\Gamma(n)$ can be generated by the generators of $\Gamma(1)(n)$ and the matrices $\begin{bmatrix} 1 & ne_j \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ ne_j & 1 \end{bmatrix}$ for $j = 2, 3$. Thus $\Gamma(n) = \Gamma(1)(n)\Delta(n)$.

Proposition 3.2 Let $p$ be a prime number and $k \in \mathbb{N}$. Then $\Gamma(p^k)$ is a normal subloop of $\Gamma$ and it has index $p^{7k}(1 - \frac{1}{p^4})$.

Proof. Consider a loop homomorphism from $\Gamma$ onto $SLL(2, \mathbb{Z}_{p^k})$

$$\Theta : \Gamma \longrightarrow SLL(2, \mathbb{Z}_{p^k})$$

$$A \longrightarrow A \pmod{p^k}$$

It is easy to prove that $\ker(\Theta) = \Gamma(p^k)$. Then

$$[\Gamma : \Gamma(p^k)] = \text{cardinality of } SLL(2, \mathbb{Z}_{p^k}).$$

Now to obtain the cardinality of $SLL(2, \mathbb{Z}_{p^k})$, let us take an arbitrary element $A = \begin{pmatrix} a \\ (v_1, v_2, v_3) \\ b \end{pmatrix}$, such that

$$\det A = ab - v_1u_1 - v_2u_2 - v_3u_3 \equiv 1 \pmod{p^k}.$$ 

Observe that $(a, v_1, v_2, v_3)$ can assume any value different from $p(n_1, n_2, n_3, n_4)$, i.e. this vector can assume $p^{4k} - p^{4(k-1)}$ different values. Fixing this vector, we know that there is a coordinate non-divisible by $p$. Without loss of generality, suppose that $a$ is not divisible by $p$ (In the case $a$ is divisible by $p$ there is some $v_j$ that is not divisible by $p$ and the argument follows similarly). Then, when we fix the values $u_1, u_2, u_3$ the congruence

$$ab \equiv 1 + v_1u_1 + v_2u_2 + v_3u_3 \pmod{p^k}$$

has an unique solution $b$ modulo $p^k$, i.e., $u_1, u_2$ and $u_3$ determine exactly one value of $b$ modulo $p^k$ and thus $(b, u_1, u_2, u_3)$ can assume $p^{3k}$ values. ■
Theorem 3.1 \( \Gamma(n) \) is a normal subloop of \( \Gamma \) with index \( n^7 \prod_{p \mid n} \left( 1 - \frac{1}{p^4} \right) \).

Proof. Suppose \( n = p_1^{k_1} \cdots p_l^{k_l} \). Consider the surjective loops homomorphism

\[
\Theta : \Gamma \longrightarrow \prod_{j=1}^{l} \text{SLL}(2, \mathbb{Z}_{p_j^{k_j}})
\]

\[
A \longmapsto \prod_{j=1}^{l} A \pmod{p_j^{k_j}}
\]

It is easy to prove that \( \ker(\Theta) = \Gamma(n) \) and then \( \Gamma(n) \) is a normal subloop of \( \Gamma \), in addition

\[
[\Gamma : \Gamma(n)] = \text{number of elements of } \prod_{j=1}^{l} \text{SLL}(2, \mathbb{Z}_{p_j^{k_j}}).
\]

Then the theorem follows from the proposition before. □

Lemma 3.1 Let \( \mathcal{L} \) be a normal subloop \( \Gamma \), \( m \) and \( n \) positive integers such that \( \Delta(n) \subset \mathcal{L} \) and \( \Delta(m) \subset \mathcal{L} \). If \( d = (n, m) \), then \( \Delta(d) \subset \mathcal{L} \).

Proof. Since \( d = tn + sm \) where \( t, s \in \mathbb{Z} \), then lemma follows from

\[
\begin{bmatrix}
1 & dx \\
0 & 1
\end{bmatrix}
= \begin{bmatrix}
1 & nx \\
0 & 1
\end{bmatrix}^t \begin{bmatrix}
1 & mx \\
0 & 1
\end{bmatrix}^s \quad \text{and} \quad
\begin{bmatrix}
1 & 0 \\
dx & 1
\end{bmatrix}
= \begin{bmatrix}
1 & 0 \\
mx & 1
\end{bmatrix}^t
\]

for every \( x \in \mathbb{Z}^3 \). □

It is known that \( \Gamma'(n) \) is a normal subloop of \( \Gamma(n) \) (ver \{3\} pág. 56). Let \( G(n) \) denote the group \( \frac{\Gamma(n)}{\Gamma'(n)} \). From proposition 3.1 follows that \( \Gamma(n) \) is finitely generated, and thus \( G(n) \) is a finite generated abelian group.

Lemma 3.2 For \( n > 5 \), \( G(n) \) is infinite.
Proof. For each $A \in \Pi(n)$, from observation 3.1 we know that $A = BC$ where $B \in \Pi(1)(n)$ and $C \in \Delta(n)$. Let $\Theta : \Pi(n) \to \frac{\Pi(1)(n)}{\Delta(1)(n)}$ defined by the rule $\Theta(A) = B\Delta(1)(n)$. To show that $\Theta$ is well defined, suppose that $A = B_1C_1 = B_2C_2$ where $B_1, B_2 \in \Pi(1)(n)$ and $C_1, C_2 \in \Delta(n)$. Since $\Delta(n)$ is normal,

$$B_1\Delta(n) = (B_1C_1)\Delta(n) = (B_2C_2)\Delta(n) = B_2\Delta(n),$$

thus $B_1^{-1}B_2 \in \Delta(n) \cap \Pi(1)(n) = \Delta(1)(n)$ and $\Theta$ is a loop homomorphism with kernel $\Delta(n)$. It follows that

$$\frac{\Pi(n)}{\Delta(n)} \simeq \frac{\Pi(1)(n)}{\Delta(1)(n)}.$$

Now, from the second and third homomorphism theorems for loops, we have

$$\frac{\Pi(n)}{\Delta(n)} \simeq \frac{\Pi(n)}{\Delta(n) \cap \Pi(1)(n)} \simeq \frac{\Pi(n)}{\Pi'(n)\Delta(n)} \simeq \frac{\Pi(n)}{\Pi'(n)\Delta(n)}.$$

Let $C(n)$ denote the group $\frac{\Pi(1)(n)}{\Delta(1)(n)}$. In [1] it proved that profinite cohomology group

$$H^1(\lim_\leftarrow C(n), \mathbb{Q}/\mathbb{Z}) = \text{Hom}(\frac{C(n)}{C(n)'}, \mathbb{Q}/\mathbb{Z}) = 0$$

and

$$H^1(\lim_\leftarrow C(n), \mathbb{Q}/\mathbb{Z}) = \text{Hom}(\frac{C(n)}{C(n)'}, \mathbb{Z})$$

is infinity, thus $\frac{C(n)}{C(n)'}$ is a abelian torsion-free group for all $n \geq 1$. Since $C(n)$ is an infinite group for $n > 5$ (see [1] pag 145), it follows that $[C(n) : (C(n))']$ is infinite for $n > 5$ and

$$|\mathbb{G}(n)| = [\Pi(n) : \Pi'(n)] \geq [\Pi(n) : \Pi'(n)\Delta(n)] = [C(n) : (C(n))'] = \infty.$$  

Denote $\mathbb{G}_s(n)$ the subgroup of $\mathbb{G}(n)$ generated by the s-th powers, i.e. $\mathbb{G}_s(n) = \langle A^s | A \in \mathbb{G}(n) \rangle$, then $\mathbb{G}(n)/\mathbb{G}_s(n)$ is finite, in fact, $[\mathbb{G}(n) : \mathbb{G}_s(n)] \leq s^k$ where $k$ is the number of generators of $\mathbb{G}(n)$. Observe that the homomorphisms

$$\Pi(n) \xrightarrow{\pi} \mathbb{G}(n) \xrightarrow{\psi} \frac{\mathbb{G}(n)}{\mathbb{G}_s(n)}$$
are well defined and surjective. Denote $\Gamma(n, s) = \ker(\psi \circ \pi) = \pi^{-1}(G_s(n))$. It is easy to see that $\Gamma(n, s)$ is generated by the commutators, associators and the set $\{A^s | A \in \Gamma(n)\}$.

**Theorem 3.2** Let $n > 5$ and $s$ be an odd integer such that $(n, s) = 1$. Then $\Gamma(n, s)$ is a finite index subloop of $\Gamma$ that is not a congruence subloop.

**Proof.** Since $\left[\Gamma : \Gamma(n, s)\right] = \left[\Gamma : \Gamma(n)\right]\left[\Gamma(n) : \Gamma(n, s)\right]$, from theorem 3.1, the definition of $\Gamma(n, s)$ and the homomorphisms theorem we have

$$\left[\Gamma : \Gamma(n)\right] = n^7 \prod_{p|n} \left(1 - \frac{1}{p^t}\right) \quad \text{and} \quad \left[\Gamma(n) : \Gamma(n, s)\right] = [G(n) : G_s(n)]$$

thus $[\Gamma : \Gamma(n, s)]$ is finite. In addition, since $G(n)$ is a finite generated abelian group and for $n > 5$ is infinite, it follows that $G(n)$ has a factor isomorphic to $\mathbb{Z}$, and thus

$$\left[\Gamma(n) : \Gamma(n, s)\right] = [G(n) : G_s(n)] \geq s > 1,$$

in particular $\Gamma(n, s) \subsetneq \Gamma(n)$. Now, suppose $\Gamma(n, s)$ is a congruence subloop, since $A_{jn}^2, B_{jn}^2 \in \Gamma'(n)$ for every $j = 1, 2, 3$, then

$$\Delta(2n^2) \subset \Gamma'(n) \subset \Gamma(n, s).$$

In the same way, from the definition of $\Gamma(n, s)$, we have that $A^s \in \Gamma(n, s)$ for every $A \in \Gamma(n)$, in particular $\begin{bmatrix} 1 & nx \\ 0 & 1 \end{bmatrix}^s, \begin{bmatrix} 1 & 0 \\ nx & 1 \end{bmatrix}^s \in \Gamma(n, s)$ for every $x \in \mathbb{Z}^3$. Then $\Delta(ns) \subset \Gamma(n, s)$. Now, $(ns, 2n^2) = n$, then from lemma 3.1, we have $\Delta(n) \subset \Gamma(n, s)$ and, finally from corollary 2.2, it follows that

$$\Gamma(n) \subset \Gamma(n, s) \subsetneq \Gamma(n),$$

but this is impossible. ■

If $s > 120$ is even, the theorem above is also true. In fact, since $(ns, 2n^2) = 2n$, from lemma 3.1 we have $\Delta(2n) \subset \Gamma(n, s)$, it follows that $\Gamma(2n) \subset \Gamma(n, s)$ and

$$s \leq \left[\Gamma(n) : \Gamma(n, s)\right] \leq [\Gamma(n) : \Gamma(2n)] = 120,$$

but this is a contradiction, since $s > 120$. 

14
Acknowledgement

The authors are grateful to Guilherme Leal for suggesting the problem and helpful conversations.

References

[1] H. Bass, M. Lazard and J. P. Serre, Sous-groupes d’indice fini dans $SL(n,\mathbb{Z})$, *Bull. Amer. Math. Soc.* 70 (1964), 385-392.

[2] H. Bass, J. Milnor and J. P. Serre, Solution of the congruence group problem for $SL_n$ ($n \geq 3$) and $Sp_{2n}$ ($n \geq 2$), *Publ. Math. I.H.E.S.* 33 (1967), 59-137.

[3] E. G. Goodaire, E. Jesper and C. P. Miles, “Alternative loop Rings”, North-Holland Math. Studies, Vol 184, Elsevier, Amsterdam, 1996.

[4] A. W. Mason and W. W. Stothers, On subgroups of $GL(n, A)$ which are Generated by Commutators, *Inventiones Math.* 23 (1974), 327-346.

[5] J. L. Mennicke, Finite factor groups of the unimodular group, *Ann. of Math.* 81 (1965), 31-37.

[6] M. Newman, “Integral Matrices”, Academic Press, New York, 1972.

[7] I. Reiner, Normal Subgroups of the unimodular group, *Illinois J. Math.* 2 (1958), 142-144.

[8] J. P. Serre, Le problème des groupes de congruence pour $SL_2$, *Ann of Math.* 92 (1970), 489-527.

[9] L. N. Varščtein, On the group $SL_2$ over Dedekind Rings of arithmetic type, *Math USSR Sbornik* 18 (1972), 321-332.

[10] P. Vojtěchovský, Generators of Nonassociative simple Moufang loops over finite prime Fields, *Journal of Algebra* 241 (2001), 181-192, doi:10.1006/jabr.2001.8776

[11] Zhevlakov, Slin’ko, Shestakov and Shirshov. “Rings that are nearly associative”. Academic Press, New York, 1982.