ε-representations of groups and Ulam stability

Christoph Gamm

October 18, 2011

Contents

I

Introduction

The notion of ε-representations or rather of ε-homomorphisms first appeared in a book by Ulam [**Ula60**]. Therein the author asks the following, very general question: "*When is it true that the solution of an equation differing slightly from a given one, must of necessity be close to the solution of the given equation?*"([**Ula60**], p. 63).

ε-representations arise when considering this question for the functional equation $\pi(gh) = \pi(g)\pi(h)$, which is satisfied by a representation $\pi : G \to \mathrm{U}(\mathcal{H})$ of a group G. The meaning of the "*equation differing slightly from a given one*" is in this case interpreted as follows: The group $\mathrm{U}(\mathcal{H})$ is equipped with a metric induced by the operator norm on $\mathrm{B}(\mathcal{H})$. Instead of requiring the two elements $\pi(gh)$ and $\pi(g)\pi(h)$ to be equal, their difference should be uniformly small in the operator norm. Put differently, the original equation $\mathrm{d}(\mu(gh), \mu(g)\mu(h)) = 0$ is perturbed to become the inequality $\mathrm{d}(\mu(gh), \mu(g)\mu(h)) \leq \varepsilon$. The objects μ satisfying this new inequality will be called ε-representations. In the spirit of Ulam's question, it will be studied under which assumptions a ε-representation is close to an actual representation. A group for which this property holds, will be called strongly Ulam stable. As before, the notion of two maps being close is defined by using the operator norm on $\mathrm{B}(\mathcal{H})$.

The first result in this direction was given by Kazhdan [**Kaz82**]. He proved that amenable groups are strongly Ulam stable by showing that any ε-representation of an amenable group is 2ε-close to an actual representation. He also gave a first example of a group that is not Ulam stable. Recently Burger, Ozawa and Thom proved that any group containing the free group with two generators is not Ulam stable [**BOT10**]. This leads to the question whether a non-amenable group is necessarily not Ulam stable.

Furthermore, it was proved that there are groups containing the free group, for which every finite dimensional ε-representation is close to a representation [**BOT10**]. These groups are of the form $G = \mathrm{SL}_n(\mathcal{O}_S)$ for $n \geq 3$, where $\mathcal{O}_S$ is the localization of the ring of integers of a number field $\mathcal{O}$ at a multiplicative subset S. A consequence of this theorem is that infinite dimensional ε-representations will have to be considered to prove the existence of non-trivial ε-representations for non-amenable groups. Additionally, a new notion of Ulam stability can be introduced, stating that all finite-dimensional ε-representation are trivial. This leads to the question of which classes of groups satisfy this property.

The purpose of the thesis in hand is to prove Ulam stability for groups of the form $\mathrm{SL}_2(A)$, for certain rings A. More explicitly, this work will focus on the following theorem:

Theorem I.1. *Let A be the localization of the ring of integers of a number field at a multiplicative subset. Assume the ring A has infinitely many units. Then* $\mathrm{SL}_2(A)$ *is Ulam stable.*

The basic idea for the proof of this theorem is taken from [**BOT10**]. Note that the groups $\mathrm{SL}_2(A)$ are are not strongly Ulam stable, as they contain a free group with two generators.

Overall, the following chapters are structured as follows.

(1) The first chapter presents a general introduction into the theory of ε-representations and Ulam stability. After the basic definitions, some known examples will be presented alongside counterexamples of Ulam stable groups. In addition, the proof of some lemmas for the behavior of Ulam stability under group operations will be recapitulated.

(2) The second and longest part of the thesis is based on the article 'Bounded generation of SL(n, A) ' by Dave Witte Morris [**Mor07**]. The objective will be to reprove Theorem 5.26 of the article. The importance of this theorem lies in its application in the proof of the main theorem of this work.

(3) The last chapter will focus on the proof of the main Theorem I.1 and conclude the thesis with a discussion of the result.

II

ε-Representations and Ulam stability

This chapter serves as a general introduction into the theory of ε-representations and Ulam stability. Along with the definitions we will present known examples and counterexamples for Ulam stability and reprove some lemmas that appeared in [**BOT10**].

1. Basic definitions

The most fundamental definition is the definition of a ε-representation.

Definition II.1. Let $\mathcal{H}$ be a Hilbert space and $\varepsilon > 0$ a real number. A *ε-representation* of a group G is a map $\mu : G \to \mathrm{U}(\mathcal{H})$ with $\mu(e) = \mathbb{1}$, which is almost multiplicative in the sense

$$\mathrm{def}(\mu) := \sup_{g,h \in G} \|\mu(gh) - \mu(g)\mu(h)\| \leq \varepsilon,$$

where $\|\cdot\|$ denotes the operator norm on $\mathrm{U}(\mathcal{H})$. The dimension of $\mathcal{H}$ will be called the dimension of the ε-representation. Denote by $\mathrm{Rep}_\varepsilon(\mathcal{H})$ the set of all ε-representations for a fixed Hilbert space $\mathcal{H}$. In the case $\varepsilon = 0$, we recover the set of all representations on $\mathcal{H}$, for which the subscript ε will be suppressed.

Remark II.2. The condition $\mu(e) = \mathbb{1}$ is not a strong restriction. If a map μ is almost multiplicative, then

$$\|\mathbb{1} - \mu(e)\| = \|\mu(e) - \mu(e)\mu(e)\| \leq \varepsilon.$$

Therefore, if we define a map $\tilde{\mu}$ as

$$\tilde{\mu}(g) := \begin{cases} \mathbb{1} & \text{if } g = e \\ \mu(g) & \text{otherwise} \end{cases}$$

then $\tilde{\mu}$ is a 2ε-representation that has distance ε to μ and satisfies all the conditions of definition II.1.

Very simple examples of ε-representations are actual representations or perturbations of representations. μ is called a δ-perturbation of a representation π if the distance between μ and π in the operator norm is small:

$$\mathrm{d}(\mu, \pi) := \sup_{g \in G} \|\mu(g) - \pi(g)\| \leq \delta$$

It is clear that a δ-perturbation μ of π is a ε-representation if $\delta \leq \frac{\varepsilon}{3}$.

ε-representations that are perturbations of actual representations are not particularly interesting and we would like to call such ε- representations *trivial*. This evokes the following question:

Question 1. *For which groups do non-trivial ε-representations exist?*

However there are some problems with the definition of ε-representations. First, the definition of a trivial ε-representation is not precise enough. Without specification of how the distance of the ε-representation to the nearest representation depends on ε, any ε-representation is trivial, as the distance of any map into the group $\mathrm{U}(\mathcal{H})$ to the trivial homomorphism is less or equal to 2.
Additionally, as we want to analyse the behavior in the limit where ε tends to zero, the set of ε-representations for a fixed ε is of limited interest.

These issues are solved by introducing the definition of Ulam stability, beginning with the following definition.

Definition II.3. Let G be a group and $\mathcal{F}$ a family of Hilbert spaces. Define $\delta_G^{\mathcal{F}} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ to be the following function:

$$\delta_G^{\mathcal{F}}(\varepsilon) := \sup_{\mathcal{H}\in\mathcal{F}} \sup_{\mu\in\mathrm{Rep}_\varepsilon(\mathcal{H})} \inf_{\pi\in\mathrm{Rep}(\mathcal{H})} \{\mathrm{d}(\mu,\pi)\}$$

Note that the value of the function $\delta_G^{\mathcal{F}}$ at 0 is always 0, because a 0-representation is an ordinary representation and the term $\mathrm{d}(\mu,\pi)$ can be minimized by taking $\pi = \mu$.

It is now possible to define Ulam stability by using the function $\delta_G^{\mathcal{F}}$.

Definition II.4 ([**BOT10**, Def. 2.1])**.** A group G is called *strongly Ulam stable* if the function $\delta_G^{\mathcal{F}}$ is continuous at 0 for any choice of $\mathcal{F}$.

If $\delta_G^{\mathcal{F}}$ is continuous for any family $\mathcal{F}$ of finite dimensional Hilbert spaces, we call the group G *Ulam stable*.

In the following paragraphs, the index $\mathcal{F}$ will be suppressed, as only the cases of $\mathcal{F}$ being either the family of all Hilbert spaces or the family of all finite dimensional Hilbert spaces will be treated. It will be assumed that any ε-representation is $\delta_G(\varepsilon)$-close to some representation and the context will show whether only finite dimensional representations are considered.

The definition of Ulam stability can be rephrased as follows: A group G being Ulam stable means that for any $\delta > 0$ there is a $\varepsilon > 0$, such that any ε-representation of G has distance at most δ to some representation.

The definition also clearly shows that strong Ulam stability implies Ulam stability, implying that Ulam stability is the weaker notion.

This allows to refine the Question 1 and to formulate the question that forms the main interest of this thesis.

Question 2. *Which groups are (strongly) Ulam stable?*

Some answers to this question will be given in the next section.

2. Examples of Ulam stable groups

In this section we present two examples of groups that are Ulam stable, resp. strongly Ulam stable.

2.1. Amenable groups. The first and so far only known example of strongly Ulam stable groups are amenable groups. The following theorem was proved by Kazhdan:

Theorem II.5 (Kazhdan;[**Kaz82**])**.** *Amenable groups are strongly Ulam stable. More precisely, if $\varepsilon \leq \frac{1}{100}$, then for any ε-representation μ of an amenable group G there is a representation π, such that:*

$$\sup_{g \in G} \|\mu(g) - \pi(g)\| \leq 2\varepsilon$$

Interestingly, the obtained representation π, close to the ε-representation μ, is unique up to conjugation (for ε sufficiently small). This can be easily deduced from a theorem by Johnson, which will be proved in the sequel (see Theorem IV.5).

2.2. $\mathrm{SL}_n(R)$ **for** $n \geq 3$**.** In contrast to amenable groups the groups presented next are only Ulam stable.

First of all, consider a ring R of the following type: Let K be an algebraic number field of finite degree k over $\mathbb{Q}$. Take an order B in K a multiplicative subset $S \subset K$ (see definition III.30). Define R to be $R = BS^{-1}$. The groups of interest are of the form $G = \mathrm{SL}_n(R)$ for $n \geq 3$. Note that these groups are neither amenable nor strongly Ulam stable because they contain the free group with two generators $\mathbb{F}_2$ as a subgroup (see lemma II.17). The following theorem was proved in [**BOT10**].

Theorem II.6 (Burger, Ozawa, Thom;[**BOT10**])**.** *If $n \geq 3$, then the group $\mathrm{SL}_3(R)$ is Ulam stable, but it is not strongly Ulam stable.*

This theorem will be refined in section IV for the case of $n = 2$, with an additional condition on the ring R.

3. Examples of non- Ulam stable groups

We will now present two classes of groups that are not Ulam stable. The first class consists of groups that have non-trivial quasimorphisms and the second is the class of groups that are free products. Note that later class is already contained in the first one, as free products exhibit quasimorphisms (this can be deduced for example from a result by Fujiwara [**Fuj00**]). This means that the two examples are not independent. In the second case we rather obtain an alternative proof for some special case than a new result.

3.1. Quasimorphisms. Quasimorphisms can be regarded as a commutative analog to ε-representation. A general discussion and examples of quasimorphisms can be found in section 2.2 of [**Cal09**]. The reason we will look at quasimorphisms here is given in Lemma II.11, which states that if a group has non-trivial quasimorphisms then it will also have non-trivial ε-representations. In the following paragraph, the definition of quasimorphisms will be given, followed by the proof of a few well known lemmas that will simplify computations later on.

Definition II.7. Let G be a group. A quasimorphism is a map $\varphi : G \to \mathbb{R}$ with bounded defect:

$$\operatorname{def}(\varphi) := \sup_{g,h\in G} |\varphi(gh) - \varphi(g) - \varphi(h)| < \infty$$

A quasimorphism φ is homogeneous, if $\varphi(g^n) = n\varphi(g)$ for all $n \in \mathbb{N}$ and $g \in G$.

Remark II.8. Note that the definition of a quasimorphism is similar to the definition of a ε-representation. In place of almost multiplicative maps into the group of unitaries, we now consider almost additive maps into the abelian group $\mathbb{R}$. As a common generalisation, the target group could be replaced by an arbitrary metric group $(\mathcal{G}, d)$ and the defect of a map $f : G \to \mathcal{G}$ could be defined as $\operatorname{def}(f) = \sup_{g,h\in G} \mathrm{d}(f(gh), f(g)f(h))$. Therefore, there is no need to introduce an extra notation for the defect of a quasimorphism and we stick to the one form def.

As for ε-representations, our main interest lies in quasimorphisms that are not perturbations of homomorphisms. It is said that a quasimorphism φ is a perturbation of a homomorphism π, if the distance between φ and π is finite, i.e. $\sup_{g\in G} |\mu(g) - \pi(g)| < \infty$. As the set of quasimorphisms is a vector space, finding quasimorphisms that are not homomorphisms comes down to the study of the quotient $\mathrm{QM}(G)/(\mathrm{Hom}(G;\mathbb{R}) \oplus \mathrm{C}^1_b(G;\mathbb{R}))$. Here $\mathrm{QM}(G)$ is the set of all quasimorphisms, $\mathrm{Hom}(G;\mathbb{R})$ denotes the set of all homomorphisms from G to $\mathbb{R}$, and $\mathrm{C}^1_b(G;\mathbb{R})$ is the space of all bounded maps from G to $\mathbb{R}$. Interestingly, this quotient can be described in terms of bounded cohomology as the kernel of the comparison map $\mathrm{H}^2_b(G;\mathbb{R}) \to \mathrm{H}^2(G;\mathbb{R})$.

The next objective is to show the identity of the quotient from above and the quotient $\mathrm{QM}_h(G)/\mathrm{Hom}(G;\mathbb{R})$. In this case, the space $\mathrm{QM}_h(G)$ is the space of homogeneous quasimorphisms. The following lemmas will prove this statement.

Lemma II.9. *Any quasimorphism is in bounded distance to a homogeneous quasimorphism.*

Proof. If φ is a quasimorphism, then we would like to define a homogeneous quasimorphism, called the homogenization of φ, by

$$\overline{\varphi}(g) := \lim_{i\to\infty} \frac{\varphi(g^{2^i})}{2^i}.$$

We need to show the existence of this limit and that the map defined in this way has bounded distance to φ. The first observation is that, by the definition of the defect, we have

$$|\varphi(g^{2^i}) - 2\varphi(g^{2^{i-1}})| \leq \mathrm{def}(\varphi).$$

Using the triangle inequality this gives for any $j < i$

$$|\varphi(g^{2^i}) - 2^{i-j}\varphi(g^{2^j})| \leq \sum_{k=1}^{i-j} 2^{k-1}\mathrm{def}(\varphi) = (2^{i-j}-1)\mathrm{def}(\varphi).$$

Dividing this equation by 2^i shows that $\frac{\varphi(g^{2^n})}{2^n}$ is a Cauchy sequence, hence it is convergent and $\overline{\varphi}$ is well defined. If $j = 0$ is inserted in the inequality above, obtain $|\frac{\varphi(g^{2^n})}{2^n} - \varphi(g)| \leq \mathrm{def}(\varphi)$ for any $n \in \mathbb{N}$ and therefore $|\overline{\varphi} - \varphi| \leq \mathrm{def}(\varphi)$. This means that $\overline{\varphi}$ is in bounded distance to φ, which in addition implies that $\overline{\varphi}$ is a quasimorphism.

The homogeneity of $\overline{\varphi}$ is proved by the following simple calculation:

$$|\overline{\varphi}(g^n) - n\overline{\varphi}(g)| = \lim_{i\to\infty}\left|\frac{1}{2^i}\left(\varphi(g^{n2^i} - n\varphi(g^{2^i}))\right)\right| = \lim_{i\to\infty}\frac{n-1}{2^i}\mathrm{def}(\varphi) = 0$$

□

A useful feature of homogeneous quasimorphisms is stated in the next lemma.

Lemma II.10. *A homogeneous quasimorphism is in bounded distance to a homomorphism if and only if it is already a homomorphism.*

Proof. Assume the existence of a homogeneous quasimorphism φ, that is not a homomorphism. We need to show that its distance to any homomorphism is unbounded. So let π be a homomorphism. Since $\varphi \neq \pi$, there is an element $g \in G$ such that $|\pi(g) - \varphi(g)| = c > 0$. For $n \in \mathbb{N}$ it follows

$$|\pi(g^n) - \varphi(g^n)| = n|\pi(g) - \varphi(g)| = nc.$$

It follows that the distance between π and φ is arbitrarily large. □

We conclude that a group has non-trivial quasimorphisms, i.e.

$$\mathrm{QM}(G)/(\mathrm{Hom}(G;\mathbb{R}) \oplus \mathrm{C}_b^1(G;\mathbb{R})) \neq \{1\},$$

if and only if there is a homogeneous quasimorphisms that is not a homomorphism.

Now we can establish the connection between quasimorphisms and Ulam stability.

Lemma II.11 ([**BOT10**, Cor. 3.5])**.** *If a group G has a non-trivial quasimorphism, then G is not Ulam stable.*

Proof. Denote by φ a homogeneous quasimorphism of G that is not a homomorphism. We want to exponentiate φ to obtain one-dimensional ε-representations. For $t > 0$ define the maps $\mu_t : G \to \mathrm{U}_1(\mathbb{C})$ by

$$\mu_t := e^{2\pi i t\varphi}.$$

In order to show that this defines ε-representations, the computation of the defect is necessary. Under the assumption that t is sufficiently small, it results:

$$\mathrm{def}(\mu_t) = \sup_{g,h\in G} |e^{2\pi i t\varphi(gh)} - e^{2\pi i t(\varphi(g)+\varphi(h))}| \overset{\text{if } t\approx 0}{\leq} |1 - e^{2\pi i t\cdot \mathrm{def}(\varphi)}|$$

In the limit of $t \to 0$, thus $\mathrm{def}(\mu_t) \to 0$. This proves that for any $\varepsilon > 0$ there is a t_ε, such that μ_t is a ε-representation for all $t \leq t_\varepsilon$.

The next step is the estimation of the distance between μ_t and an arbitrary homomorphism. For some $\delta > 0$ fix $t \in \mathbb{R}$, such that $\mathrm{def}(t\varphi) = t\mathrm{def}(\varphi) \leq \delta$ and let $\nu : G \to \mathrm{U}_1(\mathbb{C})$ be a homomorphism. Assume that δ is sufficiently small, e.g. $\delta \leq \frac{1}{10}$. Now choose a map $\psi : G \to \mathbb{R}$, that satisfies $\nu = e^{2\pi i\psi}$. Furthermore ensure

$$\sup_{g\in G} |\psi(g) - t\varphi(g)| \leq \tfrac{1}{2}. \tag{3.1}$$

This is no restriction because the integer part of ψ can be chosen arbitrarily. From the facts that $t\varphi$ is a homogeneous quasimorphism that is not a homomorphism and that the distance between $t\varphi$ and ψ is bounded, we deduce by Lemma II.10 that the defect of ψ is greater than zero. In addition, as ν is a homomorphism, the defect of ψ has to be an integer. The combination of the two results yields: $\mathrm{def}(\psi) \geq 1$.

Therefore the following estimation can be computed using the triangle inequality in the second step:

$$\begin{aligned} 1 - \delta &\leq \mathrm{def}(\psi) - \mathrm{def}(t\varphi) \\ &\leq \sup_{g,h\in G} |\underbrace{(\psi - t\varphi)(gh)}_{a_{gh}} - \underbrace{(\psi - t\varphi)(g)}_{a_g} - \underbrace{(\psi - t\varphi)(h)}_{a_h}| \end{aligned}$$

It follows that there have to be $g, h \in G$, such that the value of $|a_{gh} - a_g - a_h|$ is greater than $1 - 2\delta$. This implies that a least for one of the numbers the absolute value is greater or equal to $(1-2\delta)/3$. Therefore:

$$\sup_{g\in G} |\psi(g) - t\varphi(g)| \geq \tfrac{1-2\delta}{3} \tag{3.2}$$

In combination with the condition of equation (3.1), this shows that there is a $g \in G$ such that:

$$|\nu(g) - \mu_t(g)| = |e^{2\pi i(\psi(g)-t\varphi(g))} - 1| \geq c(\delta) > 0$$

$c(\delta)$ denotes some constant that only depends on δ. If the parameter t is restricted to an interval $[0, s]$ for some s small enough, $c = 1$ can be chosen as a constant, which then is independent of the parameter t. It can be shown that $c(\delta) \longrightarrow \sqrt{3}$ as $\delta \to 0$.

Hence for any ε there is $t \in [0, s]$, such that μ_t is a ε-representation and the distance to an arbitrary homomorphism is at least 1. This proves that G is not Ulam stable. □

As free groups have non-trivial quasimorphisms we obtain the following corollary.

Corollary II.12. *Free groups $\mathcal{F}_n$ are not (strongly) Ulam stable for $n \geq 2$.*

Of course there are many more examples of groups that have non-trivial quasimorphisms (see e.g. [**Cal09**]). However we are not going to present any of these example here, as the case of free groups is already the most interesting for us.

3.2. Free Products. Corollary II.12 points out that free groups are not Ulam stable. An alternative proof of this fact is given by a construction by Rolli [**Rol09**] that shows that free groups, or, more generally, free products of groups, have ε-representations in any dimension. This construction will be presented in this section.

At first fix some $n \in N$ and let $\{G_i | i \in I\}$ be a family of non-trivial groups. Denote by $B_\delta(\mathbb{1})$ the ball of radius δ around the neutral element in $\mathrm{U}(n)$:

$$B_\delta(\mathbb{1}) = \{u \in \mathrm{U}(n) | \|\mathbb{1} - u\| \leq \delta\}$$

For any group G_i of the family choose a map $\mu_i : G_i \to B_\delta(\mathbb{1}) \subset \mathrm{U}(n)$ with $\mu_i(g_i^{-1}) = \mu_i(g_i)^{-1}$ for all $g_i \in G_i$. Note that there is at least one map with this property that is not the trivial map $\mathbb{1} : g \mapsto \mathbb{1}$, as soon as the cardinality of G_i is greater than 2. From now on it will be assumed that there is at least one group in the family $\{G_i\}$ with more than 2 elements and that the family consists of at least two groups. Denote by $G = *_{i \in I} G_i$ the free product of the groups G_i.

Free products of groups are particularly interesting in that every element of a free product has a unique factorization. So if $g \in G$ is an element of the free product, g can be written in a unique way as

$$g = g_1 g_2 \ldots g_n,$$

where there are indices $i(g_j) \in I$ for $j \leq n$, such that $g_j \in G_{i(g_j)}$ and $i(g_j) \neq i(g_{j\pm1})$. This allows to extend the maps μ_i to a ε-representation $\mu : G \to \mathrm{U}(n)$ of the free product $G = *_{i \in I} G_i$. The value of μ at an element $g = g_1 \ldots g_n$ is defined as

$$\mu(g) := \mu_{i(g_1)}(g_1) \mu_{i(g_2)}(g_2) \ldots \mu_{i(g_n)}(g_n)$$

By using the construction of the map μ, it can be shown that the group G is not Ulam stable. More precisely the following lemma holds for μ.

Lemma II.13 ([**Rol09**, Prop. 5.2])**.** *The map $\mu : *_{i\in I} G_i \to \mathrm{U}(n)$ is a 3δ-representation and is bounded away from any homomorphism by $\sqrt{3} - \delta$.*

The proof makes use of the well known fact that $\mathrm{U}(n)$ does not have small subgroups. This statement will be proved first.

Lemma II.14. *The only subgroup H of $\mathrm{U}(n)$ that has distance less than $\sqrt{3}$ to the identity is the trivial subgroup, i.e.:*

$$\sup_{h\in H} \|h - \mathbb{1}\| < \sqrt{3} \implies H = \{e\}$$

Proof. First of all note that it is sufficient to consider cyclic subgroups. Furthermore, the statement clearly holds for $n = 1$.

Now let $H = \{a^k | k \in \mathbb{N}\}$ be a cyclic subgroup of $\mathrm{U}(n)$ for arbitrary $n \in \mathbb{N}$. We can diagonalize a by conjugation with some unitary element, i.e. there is a unitary element $u \in \mathrm{U}(n)$ and a diagonal matrix $d \in \mathrm{U}(n)$, such that $d = uau^*$. As the norm is invariant under conjugation by unitary elements, $H' = \{d^k | k \in \mathbb{N}\}$ has the same distance from the identity as H. But as d is diagonal, it is possible to apply the case of $n = 1$ to the entries of the diagonal to find that either all of those entries are 1, or the group has distance greater than $\sqrt{3}$ from the identity. □

We continue by proving Lemma II.13.

Proof of Lemma II.13: Let $g = g_1 \dots g_n$ and $h = h_1 \dots h_m$ be two elements of G with their factorization. In order to estimate the distance between $\mu(gh)$ and $\mu(g)\mu(h)$, we will consider two cases:

(1) g_n and h_1 are not in the same group, so the factorization of gh equals $g_1 \dots g_n h_1 \dots h_m$. It follows $\mu(gh) = \mu(g)\mu(h)$.

(2) There is some cancellation in the product, i.e. the factorization of gh is $gh = g_1 \dots g_{n-k} z h_{k+1} \dots h_m$, where z is an element of a G_{i_z} for some $i_z \in I$. Using the bi-invariance of the norm, we can compute in this case:

$$\begin{aligned} \|\mu(gh) - \mu(g)\mu(h)\| &= \|\mu(z) - \mu(g_{n-k+1})\mu(h_k)\| \\ &= \|\mu_{i_z}(z) - \mu_{i_{g_{n-k+1}}}(g_{n-k+1})\mu_{i_{h_k}}(h_k)\| \\ &\le 3\delta \end{aligned}$$

This shows that μ is a 3δ-representation.

The next task is to compute the distance of μ to an arbitrary homomorphism. We will do this by using Lemma II.14. Assume ν is a homomorphism with $\|\nu - \mu\| < \sqrt{3} - \delta$. We compute, using the condition $\mu(g_i) \in B_\delta(\mathbb{1})$:

$$\sup_{g_i \in G_i} \|\nu(g_i) - \mathbb{1}\| \leq \sup_{g_i \in G_i} (\|\nu(g_i) - \mu(g_i)\| + \|\mu(g_i) - \mathbb{1}\|) \leq \sqrt{3} \quad \forall i \in I$$

This means that the subgroup $\nu(G_i)$ is $\sqrt{3}$-close to the identity, hence it is trivial by Lemma II.14. Therefore ν is trivial on the generating set $\bigcup_{i \in I} G_i$ of G, implying that it is the trivial homomorphism:

$$\nu(g) = \mathbb{1} \quad \forall g \in G$$

The condition $\|\nu - \mu\| < \sqrt{3} - \delta$ now states that $\mu(G)$ has distance $\sqrt{3} - \delta$ from $\mathbb{1}$:

$$\sup_{g \in G} \|g - \mathbb{1}\| \leq \sqrt{3} - \delta$$

Let $g_1 \in G_{i_1}$ and $g_2 \in G_{i_2}$ be two arbitrary non-trivial elements of different groups ($i_1 \neq i_2$). From the definition of μ it follows for every $k \in \mathbb{Z}$:

$$\mu((g_1 g_2)^k) = (\mu(g_1)\mu(g_2))^k$$
$$\mu((g_2^{-1} g_1^{-1})^k) = (\mu(g_2)^{-1}\mu(g_1)^{-1})^k$$

The subgroup generated by the element $\mu(g_1)\mu(g_2)$ thus lies in the image of μ. It follows again by Lemma II.14 that this subgroup is trivial. As the elements g_1 and g_2 were chosen arbitrarily, we conclude that μ is the trivial map. This contradicts the assumptions and the proof is completed. □

So far, only a fixed map μ was considered. Yet, if the same construction is done for different values of δ, the Ulam stability of the group G is obtained by considering the limit of $\delta \to 0$. This leads to the following corollary, which is the final result of this section.

Corollary II.15. *Let $G = *_{i \in I} G_i$ be a free product that is not the group $D_\infty = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. Then G is not Ulam stable.*

Note that the case where all factor groups are of order two does not follow directly from the construction above. Instead we have to rewrite the product as a free product of one factor D_∞ and the rest of the $\mathbb{Z}/2\mathbb{Z}$ factors first.

Of course the case $G = \mathbb{F}_2$ is included in this corollary as $\mathbb{F}_2 = \mathbb{Z} * \mathbb{Z}$. This is useful do deduce non- strong Ulam stability for a much larger class of groups by applying a lemma that will be proved in the next section.

4. Transfer properties of Ulam stability

This section comprises the proof of some results for the behavior of Ulam stability under group operations.

The first observation is that Ulam stability is preserved under taking quotients.

Lemma II.16 ([**BOT10**, Lem. 2.2])**.** *Let $\pi : G \to H$ be a surjective homomorphism. Then (strong) Ulam stability of G implies (strong) Ulam stability of H. In other words, quotients of (strongly) Ulam stable groups are (strongly) Ulam stable.*

Proof. Take a ε-representation $\mu : H \to \mathrm{U}(\mathcal{H})$. The map $\mu \circ \pi$ will thus be a ε-representation for G, given that $\operatorname{def}(\mu \circ \pi) = \operatorname{def}(\mu)$. Let ν be a representation of G such that

$$\sup_{g \in G} \|\mu \circ \pi(g) - \nu(g)\| \leq \delta(\varepsilon) < \sqrt{3}.$$

Note that by Ulam stability of G, $\delta(\varepsilon)$ tends to zero if $\varepsilon \to 0$, and the condition $\delta < \sqrt{3}$ can be satisfied by choosing ε small enough. For $g \in \operatorname{Ker}(\pi)$ this formula reads:

$$\|\nu(g)^n - \mathbb{1}\| < \sqrt{3} \quad \forall n \in \mathbb{Z}$$

Because Lemma II.14 also holds for $\mathrm{U}(\mathcal{H})$, $\nu(g) = \mathbb{1}$ for all $g \in \operatorname{Ker}(\pi)$. So ν factors through H, i.e. there is a representation $\nu_0 : H \to \mathrm{U}(\mathcal{H})$, such that $\nu = \nu_0 \circ \pi$. ν_0 satisfies $\sup_{h \in H} \|\nu_0(h) - \mu\| \leq \delta(\varepsilon)$, which proves that H is Ulam stable. □

(Strong) Ulam stability thus behaves very nicely under taking quotients. However, the case of subgroups has to be handled more carefully. For example, it is not in general true that Ulam stability of a group implies Ulam stability of its subgroups (counterexamples are the groups $\mathrm{SL}_2(A)$, see Chapter IV). An interesting result is the following.

Lemma II.17 ([**BOT10**, Cor. 2.7])**.** *Let $H \subset G$ be a subgroup of the group G. If G is strongly Ulam stable, then H is Ulam stable.*

The proof makes use of the possibility to induce ε-representations for a group from ε-representations of a subgroup. Therefore, the definition of induced ε-representations is given beforehand.

Definition II.18 ([**BOT10**])**.** Let H be a subgroup of the group G. For each left coset Hg of H choose a representative r_{Hg} and let $\mathcal{R} = \{r_{Hg} | Hg \in H\backslash G\}$ be the set of all those representatives. Note that $r_{Hr_{Hg}h} = r_{Hgh}$.

Now let $\mu : H \to \mathrm{U}(\mathcal{H})$ be a ε-representation. We define the induced ε-representation to be:

$$\begin{aligned} \overline{\mu} &: G \to \mathrm{U}(\ell^2(\mathcal{R}, \mathcal{H})) \\ \overline{\mu}(g) &:= \big(f \mapsto \big(x \mapsto \mu(xg \cdot r_{Hxg}^{-1}) f(r_{Hxg})\big)\big) \end{aligned}$$

Remark II.19. The induced map $\overline{\mu}$ is indeed a ε-representation as the following computation shows:

$$\begin{aligned}(\overline{\mu}(g)\overline{\mu}(h)f)(x) &= \mu(xg \cdot r_{Hxg}^{-1})((\overline{\mu}(h)f)(r_{Hxg})) \\ &= \mu(xg \cdot r_{Hxg}^{-1})\mu(r_{Hxg}h \cdot r_{Hxgh}^{-1})f(r_{Hxgh}) \\ &\approx_\varepsilon \mu(xgh \cdot r_{Hxgh}^{-1})f(r_{Hxgh}) = (\overline{\mu}(gh)f)(x)\end{aligned}$$

Here the notation $\approx_\varepsilon$ means that the left- and the right-hand side have distance less or equal to ε.

The next lemma will be required in the proof of Lemma II.17.

Lemma II.20 ([**BOT10**, Lem. (2.6)])**.** *Let $\pi : G \to \mathrm{U}(\mathcal{H})$ be a representation and $p \in \mathrm{B}(\mathcal{H})$ an orthogonal projection onto a finite dimensional subspace such that*

$$\sup_{g\in G} \|p\pi(g) - \pi(g)p\| < \delta.$$

Then there is an orthogonal projection $q \in \mathrm{B}(\mathcal{H})$ that commutes with $\pi(g)$ for all $g \in G$ and satisfies

$$\|p - q\| \leq 2\delta$$

Proof. p is a finite rank operator and thus a Hilbert-Schmidt operator. Now let G act on the space of Hilbert-Schmidt operators by conjugation and let C be the convex hull of the orbit of p under this action:

$$C = \mathrm{Conv}(\{\pi(g)^* p\pi(g) | g \in G\})$$

Furthermore let $\overline{C}$ be the closure of C in the Hilbert-Schmidt norm. Note that the assumption $\sup_{g\in G} \|p - \pi(g)^* p\pi(g)\| < \delta$ implies that the set $\overline{C}$ is contained in the δ-ball $B_\delta(p)$ around p. In addition we have $\overline{C} \subset \{A \in \mathrm{B}(\mathcal{H}) | 0 \leq A \leq \mathbb{1}\}$, as C is clearly contained in this set. Thus

$$\overline{C} \subset \{A \in \mathrm{B}(\mathcal{H}) | \|A - p\| \leq \delta, 0 \leq A \leq \mathbb{1}\}$$

Now let $q_0 \in \overline{C}$ be the circumcenter of $\overline{C}$ and q the projection onto the support of q_0. Because the circumcenter is unique and C is invariant under the conjugation-action of H, q_0 is a fixed point of the action. This means that q_0 commutes with G and the same holds for q.

Now we need to estimate the distance between q and p. However, as the spectrum of the projection p only contains 0 and 1, we can conclude from the condition $\|q_0 - p\| \leq \delta$ that the spectrum of q_0 is a subset of the union of $[0, \delta]$ and $[1 - \delta, 1]$. So we get

$$\|q - q_0\| \leq \delta,$$

from which it follows that

$$\|p - q\| \leq 2\delta.$$

This proves that q has all the required properties. □

We can now proceed by proving Lemma II.17.

Proof of Lemma II.17: Let $\mu : H \to \mathrm{U}(\mathcal{H})$ be a ε-representation for a finite dimensional Hilbert space $\mathcal{H}$ and let $\overline{\mu}$ be the induced map. By strong Ulam stability of G there is a representation $\overline{\nu}$ that is $\delta(\varepsilon)$ close to $\overline{\mu}$:

$$\sup_{g\in G} \|\overline{\nu}(g) - \overline{\mu}(g)\| \leq \delta(\varepsilon)$$

It would be preferable to restrict $\overline{\nu}$ to the subspace $\mathcal{H} = \ell^2(\{r_{He}\}, \mathcal{H})$ in order to get a representation of the subgroup H. However, this is not always possible because $\mathcal{H}$ is not always an invariant subspace. In other words, the projection $p_{\mathcal{H}}$ does not necessarily commute with $\overline{\nu}(H)$. At least it follows from the definition of the induced ε-representation that $\overline{\mu}(H)$ commutes with $\mathcal{H}$ and we get

$$\begin{aligned}\|p_{\mathcal{H}}\overline{\nu}(h) - \overline{\nu}(h)p_{\mathcal{H}}\| &\leq \|p_{\mathcal{H}}\overline{\nu}(h) - p_{\mathcal{H}}\overline{\mu}(h)\| + \|\overline{\mu}(h)p_{\mathcal{H}} - \overline{\nu}(h)p_{\mathcal{H}}\| \\ &\leq 2\delta(\varepsilon).\end{aligned}$$

Therefore, it is possible to apply Lemma II.20 and obtain a projection q that commutes with $\overline{\nu}(H)$ and is close to $p_{\mathcal{H}}$:

$$\|p_{\mathcal{H}} - q\| \leq 4\delta \tag{4.1}$$

Now let u be the partial isometry of the polar decomposition $p_{\mathcal{H}}q = u|p_{\mathcal{H}}q|$. Note that the range projection uu^* and the support projection u^*u coincide with the projections $p_{\mathcal{H}}$ and q:

$$p_{\mathcal{H}} = uu^*, \qquad q = u^*u$$

This follows from the conditions $\mathrm{Ker}(p_{\mathcal{H}}q) = \mathrm{Ker}(q)$ and $\mathrm{Ker}(qp_{\mathcal{H}}) = \mathrm{Ker}(p_{\mathcal{H}})$, which are implied by (4.1). To see this, assume there was an element $x \in \mathrm{Ker}(p_{\mathcal{H}}q)$, that is not in $\mathrm{Ker}(q)$. We can assume that x is of norm one and lies in the subspace onto which q projects, hence $q(x) = x$. But then $\|p_{\mathcal{H}}q(x) - q(x)\| = 1 > 4\delta$, which is a contradiction.

We have $\mathbb{1} \geq p_{\mathcal{H}}$, which, together with (4.1), implies $q \geq qp_{\mathcal{H}}q \geq (1-4\delta)q$. The same equation holds for the root $\sqrt{qp_{\mathcal{H}}q} = |p_{\mathcal{H}}q|$ and hence we get $\||p_{\mathcal{H}}q| - q\| \leq 4\delta$. Now compute:

$$\begin{aligned}\|p_{\mathcal{H}} - u\| &\leq \|p_{\mathcal{H}} - p_{\mathcal{H}}q\| + \|p_{\mathcal{H}}q - u\| = \|p_{\mathcal{H}}p_{\mathcal{H}} - p_{\mathcal{H}}q\| + \|u|p_{\mathcal{H}}q| - uq\| \\ &\leq \|p_{\mathcal{H}} - q\| \cdot \|p_{\mathcal{H}}\| + \||p_{\mathcal{H}}q| - q\| \cdot \|u\| \leq 4\delta + 4\delta \\ &= 8\delta\end{aligned}$$

To finish the proof, define $\nu : H \to \mathrm{U}(\mathcal{H})$ as $\nu = u\overline{\nu}u^*$. By the previous work ν is indeed a representation on $\mathcal{H}$ and it satisfies:

$$\begin{aligned}\|\nu(h) - \mu(h)\| &= \|u\overline{\nu}(h)u^* - p_{\mathcal{H}}\overline{\mu}(h)p_{\mathcal{H}}\| \\ &\leq \|p_{\mathcal{H}}\overline{\nu}(h)p_{\mathcal{H}} - p_{\mathcal{H}}\overline{\mu}(h)p_{\mathcal{H}}\| + 16\delta \leq 17\delta\end{aligned}$$

□

Lemma II.17 allows to enlarge the class of groups that are known to be not strongly Ulam stable. Remember that by Corollary II.12 free groups have one-dimensional ε-representations. We obtain:

Corollary II.21. *Let G be a group, that contains a free group $\mathbb{F}_n$ $n \geq 2$ as a subgroup. Then G is not strongly Ulam stable.*

Corollary II.21 is the most important result of this section. It will be applied to deduce that the groups $\mathrm{SL}_2(A)$ studied in the last chapter are not strongly Ulam stable. It is possible to get a slightly stronger result than Lemma II.17 for subgroups of finite index: The proof of Lemma II.17 implicates that the induced ε-representation of a finite dimensional ε-representation for a finite index subgroup is again finite dimensional, so we have:

Lemma II.22. *Let H be a finite-index subgroup of G. If G is Ulam stable then so is H.*

As an immediate consequence we obtain:

Corollary II.23. *If G is a group that contains a free group $\mathbb{F}_n$ for $n \geq 2$ as a finite index subgroup, then G is not Ulam stable.*

We conclude this chapter with a result that will be used later when proving that $\mathrm{SL}_2(R)$ is Ulam stable.

Lemma II.24. *Let H be a normal subgroup of G, whose quotient $Q = G/H$ is (strongly) Ulam stable. If $\kappa, \varepsilon > 0$ are small enough and $\mu : G \to \mathrm{U}(\mathcal{H})$ is a ε-representation with the property*

$$\|\mu(h) - \mathbb{1}\| \leq \kappa \qquad \forall h \in H,$$

then there is a representation π of G with $\|\mu - \pi\| \leq \kappa + \varepsilon + \delta(\kappa + 2\varepsilon)$. Here $\delta(\varepsilon)$ is the maximal distance of a ε-representation of Q to a representation.

Proof. Denote by $p : G \to Q$ the quotient map and let $s : Q \to G$ be a section. The composition of μ with s is a $(\kappa + 2\varepsilon)$-representation of Q:

$$\begin{aligned}\|\mu(s(qp)) - &\mu(s(q))\mu(s(p))\| \\ &\leq \|\mu(s(qp)s(p)^{-1}s(q)^{-1}s(q)s(p)) - \mu(s(q)s(p))\| + \varepsilon \\ &\leq \|\mu(\underbrace{s(qp)s(p)^{-1}s(q)^{-1}}_{\in H})\mu(s(q)s(p)) - \mu(s(q)s(p))\| + 2\varepsilon \\ &\leq \kappa + 2\varepsilon\end{aligned}$$

As Q is strongly Ulam stable, there is a representation π of Q with $\|\mu \circ s - \pi\| \leq \delta(\kappa + 2\varepsilon)$. The composition of π with the quotient map p results in a representation of G that is $(\varepsilon + \kappa + \delta(\kappa + 2\varepsilon))$-close to the original ε-representation μ:

$$\begin{aligned}\|\mu(g)-\pi(p(g))\| \leq & \|\mu(g)-\mu(s(p(g)))\|+\delta(\kappa+2\varepsilon)\\ \leq & \|\mu(g)-\mu(g)\mu(g^{-1}s(p(g)))\|+\varepsilon+\delta(\kappa+2\varepsilon)\\ \leq & \varepsilon+\kappa+\delta(\kappa+2\varepsilon)\end{aligned}$$

This proves the desired statement. □

III

Bounded Generation of $\mathrm{SL}_2(R)$

First, we would like to fix the some notations for this chapter.

Definition III.1. Let R be a commutative ring and I an ideal in R.

(1) $\mathrm{SL}_2(R;I)$ is the subset of $\mathrm{SL}_2(R)$ consisting of the matrices, that are congruent to $\mathbb{1} \bmod I$.

(2) $\mathrm{e}_2(X) = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ a' & 1 \end{smallmatrix}\right) | a, a' \in X\}$ is the set of elementary matrices whose off-diagonal entries are elements of $X \subset R$.

(3) $\mathrm{e}_2^{\triangleleft}(X)$ is the set of $\mathrm{e}_2(R)$-conjugates of $\mathrm{e}_2(X)$.

(4) $\mathrm{E}_2(X)$ (resp. $\mathrm{E}_2^{\triangleleft}(X)$) will denote the subgroup generated by the set $\mathrm{e}_2(X)$ (resp. $\mathrm{e}_2^{\triangleleft}(X)$). This means $\mathrm{E}_2^{\triangleleft}(X)$ is the smallest normal subgroup of $\mathrm{E}_2(R)$ that contains $\mathrm{e}_2^{\triangleleft}(X)$.

Furthermore we introduce the following definition.

Definition III.2. Denote by W_I the following subset of R^2:

$$W_I = \{(a,b) \,|\, (a,b) \equiv (1,0) \mod I; aR + bR = R\}$$

Remark III.3. A pair $(a,b) \in R^2$ is in W_I if and only if there are $c, d \in R$, such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R;I)$. Indeed, since $aR + bR = R$, $x, y \in R$ can be chosen with $ax + by = 1$. Now define $c = -by^2$ and $d = x + bxy$. Then $d \equiv 1 \bmod I$ and $ad - bc = 1$, as desired.

1. Statement of the theorem and an outline of the proof

The objective of this chapter is to prove a theorem that can be found in an article by Dave Witte Morris [**Mor07**], which itself is based on unpublished work by Carter, Keller, and Paige [**CKP92**].

At the beginning of this chapter, the statement of the theorem will be presented together with a brief sketch of the proof. The theorem is concerned with a property called bounded generation, which is defined as follows: Consider a group G and a symmetric subset $X = X^{-1}$. Denote by $\langle X \rangle_r$ the set of elements of G that are a product of at most r elements of X.

Definition III.4. The group is said to be boundedly generated by a symmetric subset K, if there is $r \in \mathbb{N}$, such that $\langle K \rangle_r = G$, i.e. every element of G can be written as a word in K of word length less or equal to r.

A basic example of bounded generation is given by the special linear group $\mathrm{SL}_n(F)$ for a field F, as it can easily be shown that these groups are boundedly generated by the elementary matrices. Nevertheless, if the field F is replaced by some arbitrary commutative ring R this is in general no longer true. A counterexample is provided by the group $\mathrm{SL}_2(\mathbb{Z})$ following from the fact that $\mathrm{SL}_2(\mathbb{Z})$ contains a free group as a subgroup of finite index. However, $\mathrm{SL}_n(\mathbb{Z})$ is boundedly generated by the elementary matrices, if $n \geq 3$ (see e.g. [**BHV08**], where bounded generation is treated in the context of Kazhdan's property T). This leads naturally to the following question:

Question 3. *For which rings R and $n \in \mathbb{N}$ do the elementary matrices boundedly generate some subgroup of $\mathrm{SL}_n(R)$?*

An answer to this question is given in [**CKP92**] and [**Mor07**]. The authors prove that the elementary matrices $\mathrm{e}_2(R)$ boundedly generate a subgroup of $\mathrm{SL}_n(R)$, provided that the ring R satisfies some ring theoretic properties. This proof will be repeated here for the case $n = 2$, as this is the situation that will occur in the proof of the main theorem in chapter IV. Note however that the case $n \geq 3$ is in some respects included in this proof. The most difficult part of the proof (which is showing the existence of a Mennicke symbol with some nice properties) is much simpler under the condition $n \geq 3$.

The theorem we are interested in is the following:

Theorem ([**Mor07**, Thm. 5.26]; [**CKP92**])**.** *Let $A = BS^{-1}$ be the localization of an order in an algebraic number field. If A has infinitely many units, then for any ideal I in A the elementary matrices $\mathrm{e}_2^{\triangleleft}(I)$ boundedly generate a subgroup in $\mathrm{SL}_2(R)$.*

Two main components are necessary for the proof. The first is the compactness theorem of first order logic (see III.37), the second is the theory of Mennicke symbols which will be presented in the next section.

The proof can be summarized as follows: The compactness theorem allows to prove bounded generation in a much more general context (see Thm. III.39). The essential condition in the statement of this general theorem is that the subgroup that is supposed to be boundedly generated is of finite index in the ambient group. It follows that, to prove bounded generation by elementary matrices, it is only needed to bound the size of the quotient $\mathrm{SL}_2(R; I)/\mathrm{E}_2^{\triangleleft}(I)$. This can be done in two steps by using the theory of Mennicke symbols. The first step is to show that under certain conditions for the ring R any Mennicke symbol has finite range, which is done in section 4. The second step then is to find a Mennicke symbol whose range is exactly the quotient $\mathrm{SL}_2(R; I)/\mathrm{E}_2^{\triangleleft}(I)$. This is the hardest part of the proof and will be done in section 5.

2. Mennicke Symbols

Mennicke symbols were originally defined by Mennicke [**Men65**] and used by Bass, Milnor, and Serre in [**BMS67**] to find a solution to the congruence subgroup problem. In the context of bounded generation Mennicke symbols make their appearance in Theorem III.23, which states that the quotient $\mathrm{SL}_2(R;I)/\mathrm{E}_2^{\triangleleft}(I)$ is the range of a certain Mennicke symbol. This section contains the definition of as well as some lemmas for Mennicke symbols.

Definition III.5 ([**Mor07**, Def. 2.16 and Lem. 2.19])**.** Let R be a commutative ring and I be an ideal in R. A Mennicke symbol is a function $[\,] : W_I \to A; (a,b) \mapsto \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$, where A is an abelian group, that satisfies the following conditions:

$$\begin{bmatrix} b+ta \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}, \text{if } (a,b) \in W_I, t \in I; \tag{M1}$$

$$\begin{bmatrix} b \\ a+sb \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}, \text{if } (a,b) \in W_I, s \in R; \tag{M2}$$

$$\begin{bmatrix} b_1 \\ a \end{bmatrix}\begin{bmatrix} b_2 \\ a \end{bmatrix} = \begin{bmatrix} b_1 b_2 \\ a \end{bmatrix}, \text{if } (a,b_1), (a,b_2) \in W_I. \tag{M3}$$

If the ideal I is principal, add a fourth condition:

$$\begin{bmatrix} b \\ a_1 \end{bmatrix}\begin{bmatrix} b \\ a_2 \end{bmatrix} = \begin{bmatrix} b \\ a_1 a_2 \end{bmatrix}, \text{if } (a_1,b), (a_2,b) \in W_I \tag{M4}$$

Remark III.6. The last condition (M4) can be deduced from the other properties, given the ideal is principal. It is added to the definition here to simplify the proofs later on. Conversely, it can be proved that (M4) always implies (M3). Furthermore, if (M4) holds whenever $\left[\begin{smallmatrix} b \\ a_2 \end{smallmatrix}\right] = 1$ then (M3) holds as well (see Corollary 2.24 in [**Mor07**]).

Likewise, the condition of the group A being abelian is superfluous as the image of a Mennicke symbol is automatically abelian.

As mentioned before, an important fact about Mennicke symbols is that there is a universal Mennicke symbol.

Lemma III.7. *There is a universal Mennicke symbol, i.e. an abelian group A_I, called the universal Mennicke group, and a Mennicke symbol $[\,]_I : W_I \to A_I$, such that for any Mennicke symbol $[\,] : W_I \to A$ there exists a unique homomorphism $\varphi : A_I \to A$, that makes the following diagram commutative:*

$$\begin{tikzcd}
W_I \arrow[r, "{[\,]_I}"] \arrow[rd, "{[\,]}"'] & A_I \arrow[d, "\varphi"] \\
 & A
\end{tikzcd}$$

The universal Mennicke symbol and the universal Mennicke group are unique up to isomorphism.

Proof. Define A_I to be the abelian group with generators W_I and relations given by the conditions of definition III.5. Let $[\,]_I : W_I \to A_I$

be the map that assigns an element to the generator it represents. This defines a universal Mennicke symbol. The uniqueness up to isomorphism follows easily from the uniqueness of the map φ. □

For every ideal I in R there is a universal Mennicke symbol. Universal Mennicke symbols of two different ideals can be put in relation with each other, if one of the ideals is contained in the other. The condition $I' \subset I$ implies $W_{I'} \subset W_I$ and the restriction of a Mennicke symbol $[\,] : W_I \to A$ of the ideal I induces a Mennicke symbol $[\,] : W_{I'} \to A$ of the ideal I'. If the universal Mennicke symbol $[\,]_I : W_I \to A_I$ is restricted to $W_{I'}$, we therefore get a canonical homomorphism $A_{I'} \to A_I$ by using the universal property of $[\,]_I$. Importantly, this homomorphism is surjective, as proved in the following lemma.

Lemma III.8 ([**Bas68**, VI. Prop. 1.4])**.** *The canonical homomorphism $A_{I'} \to A_I$ is surjective.*

Proof. For the proof of this statement, it is necessary to show that for any $(a, b) \in W_I$ there is some $(a', b') \in W_{I'}$, such that

$$\begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b' \\ a' \end{bmatrix}.$$

For this, consider the ring $\tilde{R} = R/I'$ with the ideal I/I' and denote by $\hat{a}, \hat{b} \in \tilde{R}$ the elements that are represented by $a, b \in R$. Then $\tilde{R}$ is a semi-local ring, in which an element $t \in \tilde{R}$ can be found, such that $u = \hat{a} + t\hat{b}$ is a unit (see [**Bas68**, III. Prop. 2.8]). Now compute:

$$\begin{aligned} \begin{bmatrix} \hat{b} \\ \hat{a} \end{bmatrix} &= \begin{bmatrix} \hat{b} \\ \hat{a} + t\hat{b} \end{bmatrix} = \begin{bmatrix} \hat{b} + u(u^{-1}(1-u-\hat{b})) \\ u \end{bmatrix} \\ &= \begin{bmatrix} 1-u \\ u \end{bmatrix} = \begin{bmatrix} 1-u \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{aligned} \tag{2.1}$$

Observe that the second equation requires $(1-u-\hat{b}) \in I/I'$. This is true under condition $(\hat{a}, \hat{b}) \in W_{I/I'}$, which implies $(\hat{a}, \hat{b}) \equiv (1, 0) \mod I/I'$ and therefore

$$\hat{b} \in I/I' \text{ and } (1-u) = (1-\hat{a}) + t\hat{b} \in I/I'.$$

Equation (2.1) proves the desired statement. □

The canonical homomorphism allows the deduction of properties of a Mennicke symbol by analyzing smaller ideals, which may be easier to handle.

Two additional properties of Mennicke symbols will be required for the computations. They are proved in the following lemma.

Lemma III.9 ([**Mor07**, Lem. 2.25])**.** *Let $[\;] : W_I \to A$ be a Mennicke symbol.*

(1) If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(R;I)$, *then*

$$\begin{bmatrix} c \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}^{-1}. \tag{2.2}$$

(2) Assume that the ideal I *is principal and*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(R;I) \text{ and } f\mathbb{1} + g\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(R;I),$$

then

$$\begin{bmatrix} bg \\ f+bg \end{bmatrix}^2 = \begin{bmatrix} b \\ f+bg \end{bmatrix}^2. \tag{2.3}$$

Proof. (1) Since $b, c \in I$ and $a \equiv 1 \bmod I$, $(bc + d(1-a)) \in I$ and

$$\begin{aligned} \begin{bmatrix} b \\ a \end{bmatrix}\begin{bmatrix} c \\ a \end{bmatrix} &= \begin{bmatrix} bc \\ a \end{bmatrix} = \begin{bmatrix} bc - a(bc + d(1-a)) \\ a \end{bmatrix} \\ &= \begin{bmatrix} (bc-ad)(1-a) \\ a \end{bmatrix} = \begin{bmatrix} a-1 \\ a \end{bmatrix} = 1. \end{aligned}$$

(2) $a \equiv d \equiv f + ga \equiv 1 \bmod I$, therefore

$$1 = (f+ga)^2 \bmod qR \text{ and} \tag{2.4}$$

$$\begin{aligned} 1 &= \det\left(f\mathbb{1} + g\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \\ &= f^2 + fg(a+d) + g^2(ad-cb) = f^2 + fg(a+d) + g^2 \\ &\equiv f^2 + fg(1+1) + g^2 \equiv (f+ga)^2 \bmod gqR. \end{aligned} \tag{2.5}$$

The following computation proves the desired statement:

$$\begin{aligned} \begin{bmatrix} bg \\ f+ga \end{bmatrix}^2 &= \begin{bmatrix} bg \\ (f+ga)^2 \end{bmatrix}\begin{bmatrix} q \\ 1 \end{bmatrix} \overset{(2.4)}{=} \begin{bmatrix} b \\ (f+ga)^2 \end{bmatrix}\begin{bmatrix} g \\ (f+ga)^2 \end{bmatrix}\begin{bmatrix} q \\ (f+ga)^2 \end{bmatrix} \\ &= \begin{bmatrix} b \\ f+ga \end{bmatrix}^2 \begin{bmatrix} gq \\ (f+ga)^2 \end{bmatrix} \overset{(2.5)}{=} \begin{bmatrix} b \\ f+ga \end{bmatrix}^2 \begin{bmatrix} gq \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} b \\ f+ga \end{bmatrix}^2 \end{aligned}$$

□

3. Properties of number rings

In this section we will define some ring theoretic properties that are required in the proofs in the later sections. Some of these properties may on first sight seem a bit arbitrary and in fact we do not give a better motivation for them other than that they are exactly what is required to make the proofs possible.

As we eventually want to apply the compactness theorem of first order logic it is important that all these properties can be expressed as a collection of first order formulas. This is however not very hard to verify and we will omit explicit proofs here.

3.1. Stable Range Condition. The first property to be defined is the stable range condition.

Definition III.10 ([Mor07, Def. 2.9])**.** A commutative ring R satisfies the stable range condition SR_m for some $0 < m \in \mathbb{N}$, if the following holds: For any elements $a_i \in R$, $0 \leq i \leq r$, such that $r \geq m$ and $\sum_{i=0}^{r} a_i R = R$, there are $a_i' \in R$, such that:

(1) $a_i' \equiv a_i \mathrm{mod}\, a_0 R$, for $1 \leq i \leq r$,
(2) $\sum_{i=1}^{r} a_i' R = R$

If R/I satisfies SR_1 for every non-zero ideal $I \subset R$, the ring R is said to satisfy $\mathrm{SR}_{1\frac{1}{2}}$.

The following lemma describes rings that satisfy the stable range condition $\mathrm{SR}_{1\frac{1}{2}}$.

Lemma III.11. *If R has the stable range condition $\mathrm{SR}_{1\frac{1}{2}}$, and $a, b, c \in R, a \neq 0$ satisfy $aR + bR + cR = R$, then there exists $b' \equiv b \bmod cR$, such that $aR + b'R = R$.*

Proof. The proof is a simple application of SR_1 for the quotient $R' = R/aR$. By assumption $bR' + cR' = R'$, so by $\mathrm{SR}_{1\frac{1}{2}}$ there is a $\tilde{b} \equiv c \bmod cR'$, such that $\tilde{b}R' = R'$. This implies $aR + b'R = R$ for some element $b' \in R$ in the coset represented by $\tilde{b}$. □

3.2. Few Generator Property. The few generator property is used to limit the number of generators of the universal Mennicke group.

Let $R^\times$ be the group of units (with multiplication as group operation) of the ring R.

Definition III.12 ([Mor07, Def. 3.2])**.** A commutative ring R has the few generator property $\mathrm{Gen}(t, r)$ for some $t, r \in \mathbb{N}$, if the following holds: For any $a, b \in R$ that satisfy $aR + bR = R$, there is a principal ideal $I = hR$ for $h \in a + bR$, such that the quotient $(R/I)^\times/((R/I)^\times)^t$ has r generators.

3.3. Exponent Property. The exponent property will be required to bound the order of the elements of the universal Mennicke group. Together with the few generator property this will bound to number of elements in the universal Mennicke group.

Definition III.13 ([Mor07, Def. 3.6])**.** A commutative ring R has the exponent property $\mathrm{Exp}(t, l)$ for some $t, l \in \mathbb{N}, l > 0$, if the following holds: For any principal ideal $I = qR, 0 \neq q$ and $(a, b) \in W_I$, there are

$a', c, d \in R$ and $f_i, g_i, b'_i, d'_i \in R$ and units $u_i \in R$, where $1 \leq i \leq l$, such that:

$$a' \equiv a \mod bR; \tag{E1}$$

$$f_i + g_i a' \equiv u_i \mod b'_i R \text{ for } 1 \leq i \leq l; \tag{E2}$$

$$\begin{pmatrix} a' & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(R; I), \tag{E3}$$

$$\begin{pmatrix} a' & b'_i \\ c & d'_i \end{pmatrix}, f_i \mathbb{1} + g_i \begin{pmatrix} a' & b'_i \\ c & d'_i \end{pmatrix} \in \mathrm{SL}_2(R; I) \text{ for } 1 \leq i \leq l; \tag{E4}$$

$$\prod_{i=1}^{l} (f_i + g_i a')^2 \equiv (a')^t \mod cR. \tag{E5}$$

Remark III.14. Note that the fourth property (E4) meets what is required to apply the property of Mennicke symbols proved in Lemma III.9.

3.4. Unit Property. The next two properties are necessary to prove the existence of a Mennicke symbol with $\mathrm{SL}_2(R; I)/\mathrm{E}_2^{\triangleleft}(I)$ as target group.

The unit property allows to transform the conjugation by certain matrices into multiplication with elementary matrices.

Definition III.15 ([**Mor07**, Def. 4.3])**.** A commutative ring R has the unit property $\mathrm{Unit}(r, x)$ for some integers $r, x \geq 1$, if:

(1) For any principal ideal $I = qR$, there exists a unit $u \in R$, such that

$$u \equiv 1 \bmod I \quad \text{ and } u^4 \neq 1$$

(2) There is a unit $u_0 \in R$, such that $u_0^2 \neq 1$ and for any ideal I with r generators and any $A \in \mathrm{SL}_2(R; I)$, there are $e_1, e_2, \ldots, e_x \in \mathrm{e}_2(I)$ with:

$$\begin{pmatrix} u_0 & 0 \\ 0 & u_0^{-1} \end{pmatrix} A \begin{pmatrix} u_0^{-1} & 0 \\ 0 & u_0 \end{pmatrix} = e_1 A e_2 \ldots e_x$$

Remark III.16. Clearly, it holds

$$\begin{pmatrix} u_0 - 1 & 0 \\ 0 & u_0 \end{pmatrix} A \begin{pmatrix} u_0 & 0 \\ 0 & u_0^{-1} \end{pmatrix} = e'_1 A e'_2 \ldots e'_x,$$

for any $A \in \mathrm{SL}_2(R; I)$ and some $e'_i \in \mathrm{e}_2(I)$. To prove this, simply apply the statement above to the matrix $\tilde{A} = \left(\begin{smallmatrix} u_0 - 1 & 0 \\ 0 & u_0 \end{smallmatrix}\right) A \left(\begin{smallmatrix} u_0 & 0 \\ 0 & u_0^{-1} \end{smallmatrix}\right)$.

It is also interesting to note, that the first condition is stronger than what is needed in the proofs later on. The condition $u^4 \neq 1$ could be replaced be $u^2 \neq 1$. However, we want to keep the definition of [**Mor07**], where the stronger statement is required in a proof of a different theorem.

3.5. Conjugation Property. The last property is the conjugation property. As the name suggest, it allows to control the behavior of elementary matrices under conjugation by the elementary matrix $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$.

For an ideal I in a ring R let $\mathcal{M}_I$ be the following set:

$$\mathcal{M}_I := \left\{ y \in I \middle| 1 + yz = u^2, \quad \begin{array}{c}\text{for some } z \equiv \pm 1 \bmod I \\ \text{and a unit } u \in R\end{array} \right\}$$

Definition III.17 ([**Mor07**, Def. 4.5])**.** A commutative ring R has the conjugation property $\mathrm{Conj}(z)$ for some $z \in \mathbb{N}$, if for all nonzero $q \in R$ there is a $q' \in R$, such that any $x \in q'R$ can be written as a sum

$$x = \sum_{i=1}^{k} y_i s_i^{-2}, \tag{3.1}$$

where $k \leq z$, $y_i \in M_{qR}$ and s_i are units, such that $s_i^{-2} \equiv 1 \bmod qR$.

Remark III.18. The definition of the conjugation property introduced here differs slightly from the one in [**Mor07**], where

(1) $y \in \mathcal{M}_I$ satisfies the condition $1 + zyu_1^2 = u^2$ for z and u as before and an additional unit u_1 and

(2) the units s_i are removed in the equation (3.1).

These changes were introduced to make the proof of Lemma III.26 easier. Note however, that the proof of Theorem 4.6 in [**Mor07**] can be altered to show that rings A of the form $A = BS^{-1}$ still satisfy this new conjugation property.

4. Finiteness of the Universal Mennicke group

It is now possible to start with the first crucial proof of this chapter. In this section it will be shown that the universal Mennicke group is finite if a ring satisfies the ring theoretic properties defined before for a suitable choice of the parameters.

The universal Mennicke group is abelian and it therefore is sufficient to bound its number of generators and the order of its elements. First, a bound for the latter will be established. Note that the additional requirement of the ideal being principal will be dropped later on.

Lemma III.19 ([**Mor07**])**.** *Let R be an integral domain, that satisfies the property* $\mathrm{Exp}(t, l)$*, and let $I \subset R$ be a principal ideal.*

Then every element of the universal Mennicke group A_I has order t.

Proof. Let $\left[\begin{smallmatrix}b\\a\end{smallmatrix}\right]_I$ for $(a, b) \in W_I$ be an arbitrary element of the universal Mennicke group A_I. The aim is to compute the t-fold power of $\left[\begin{smallmatrix}b\\a\end{smallmatrix}\right]_I$. For the following computation choose elements

$$a', c, d, u_i, f_i, g_i, b_i', d_i' \in R$$

as in definition III.13, which is possible since R has the exponent property $\mathrm{Exp}(t,l)$.

$$\begin{aligned}
\begin{bmatrix} b \\ a \end{bmatrix}_I^t &\overset{(E1);(M2)}{=} \begin{bmatrix} b \\ a' \end{bmatrix}_I^t \overset{(E3);(2.2)}{=} \begin{bmatrix} c \\ a' \end{bmatrix}_I^{-t} \overset{(M4)}{=} \begin{bmatrix} c \\ a'^{-t} \end{bmatrix}_I \\
&\overset{(E5);(M4)}{=} \prod_{i=1}^{l} \begin{bmatrix} c \\ f_i + g_i a' \end{bmatrix}_I^{-2} \overset{(2.3)}{=} \prod_{i=1}^{l} \begin{bmatrix} c g_i \\ f_i + g_i a' \end{bmatrix}_I^{-2} \\
&\overset{(E4);(2.2)}{=} \prod_{i=1}^{l} \begin{bmatrix} b'_i g_i \\ f_i + g_i a' \end{bmatrix}_I^{2} \overset{(2.3)}{=} \prod_{i=1}^{l} \begin{bmatrix} b'_i \\ f_i + g_i a' \end{bmatrix}_I^{2} \\
&\overset{(E2);(M2)}{=} \prod_{i=1}^{l} \begin{bmatrix} b'_i \\ u_i \end{bmatrix}_I^{2} \overset{(M1)}{=} \prod_{i=1}^{l} \begin{bmatrix} b'_i + u_i(u_i^{-1}(1 - u_i - b) \\ u_i \end{bmatrix}^{2} \\
&\overset{(M2)}{=} \prod_{i=1}^{l} \begin{bmatrix} 1 - u_i \\ 1 \end{bmatrix}^{2} \overset{(M1)}{=} \prod_{i=1}^{l} \begin{bmatrix} 0 \\ 1 \end{bmatrix}^{2} \overset{(M3)}{=} 1
\end{aligned}$$

□

The next lemma establishes a bound to the number of generators of the universal Mennicke group.

Lemma III.20 ([**Mor07**])**.** *Let R be an integral domain that satisfies the properties $\mathrm{SR}_{1\frac{1}{2}}$, $\mathrm{Exp}(t,l)$ and $\mathrm{Gen}(t,r)$. Let $I = qR \subset R$ be a principal ideal.*
Then the universal Mennicke group A_I is generated by r elements.

Proof. Take arbitrary elements $\left[\begin{smallmatrix} b_i \\ a_i \end{smallmatrix}\right]_I \in A_I$ for $1 \le i \le r+1$. The aim is to prove that these elements satisfy some nontrivial relation. The first step is to show that the elements a_i can be replaced by coprime elements a'_i, i.e. we want to find elements a'_i such that

$$\begin{aligned}
&a'_i = a_i \bmod b_i R, &(4.1)\\
&a'_i R + a'_j R = R \text{ for any } 1 \le i < j \le r+1.
\end{aligned}$$

This can be done by inductively applying the stable range condition $\mathrm{SR}_{1\frac{1}{2}}$ and Lemma III.11. By definition of W_I it follows $b_i R + a_i R = R$, hence with $c_i = a_1 a_2 \ldots \widehat{a_i} \ldots a_{r+1}$ we get:

$$b_i R + a_i R + c_i R = R \overset{\mathrm{SR}_{1\frac{1}{2}}}{\Longrightarrow} \exists a'_i = a_i \bmod b_i : a'_i R + c_i R = R$$

Applying this for every $i \le r+1$ where $a_j, j < i$ is replaced by a'_j in the product c_i, proves the existence of elements a'_i that satisfy the desired property. Furthermore, by the condition $a'_i = 1 \bmod I$, which holds as $(a'_i, b_i) \in W_I$, the element q is coprime to a'_i. This is true for every i.

Consider now the following set of equations:

$$\begin{aligned}
&x \equiv 1 \bmod I (= qR),\\
&x \equiv b_i \bmod a'_i R \quad \text{ for } 1 \le i \le r+1. &(4.2)
\end{aligned}$$

Given that all the elements q and a'_i are coprime we, the Chinese remainder theorem can be applied to find a solution $y \in R$ for these equations. The conditions $a'_iR + b_iR = R$ imply that y is coprime to a_i for every i. As the first equation above says that y is coprime to q as well, it follows:

$$yR + a'_1a'_2 \dots a'_{r+1}qR = R.$$

Now apply the few generator property $\mathrm{Gen}(t, r)$ to find an ideal $H = hR \subset R$, such that

$$\begin{aligned} h \equiv y \bmod a'_1a'_2 \dots a'_{r+1}qR \quad \text{and} \\ (R/H)^\times/((R/H)^\times)^t \text{ has } r \text{ generators.} \end{aligned} \tag{4.3}$$

Note that the elements a'_i are units in R/H, which is revealed by combining the conditions $yR + a'_iR = R$ and $h \equiv y \bmod a'_iR$. The $r + 1$ elements a'_i therefore must satisfy some nontrivial relation in $(R/H)^\times/((R/H)^\times)^t$, i.e. there are $e_i \in \mathbb{N}$ for $1 \leq i \leq r+1$ and $\alpha \in R$, with:

$$\prod_{i=1}^{r+1} (a'_i)^{e_i} \equiv \alpha^t \bmod hR$$

Furthermore, it can be assumed that

$$\alpha \equiv 1 \bmod qR, \tag{4.4}$$

because of $h \equiv y \equiv 1 \bmod qR$, meaning that h and q are coprime and α could be replaced by a solution to the following equations using the Chinese remainder theorem.

$$\begin{aligned} x &\equiv \alpha \bmod hR \quad \text{and} \\ x &\equiv 1 \bmod qR. \end{aligned}$$

Now both α^t and $\prod_{i=1}^{r+1} a'_i$ are solutions to the equations

$$x \equiv \prod_{i=1}^{r+1} a'_i \bmod hR \quad \text{and} x \equiv 1 \bmod qR. \tag{4.5}$$

According to the Chinese remainder theorem, they differ by an element of the ideal hqR:

$$\prod_{i=1}^{r+1} (a'_i)^{e_i} \equiv \alpha^t \bmod hqR \tag{4.6}$$

The following two statements will be necessary for the later calculation.

$$\begin{bmatrix} q \\ a'_i \end{bmatrix}_I = 1 \tag{4.7}$$

$$h \equiv y \equiv b_i \bmod a'_iR \tag{4.8}$$

The first clearly follows from the condition $a_i' \equiv 1 \bmod qR$ and the properties of Mennicke symbols. The second statement is simply the combination of (4.2) and (4.3).

A first computation gives:

$$\begin{bmatrix} b_i \\ a_i \end{bmatrix}_I \overset{(4.1)}{=} \begin{bmatrix} b_i \\ a_i' \end{bmatrix}_I \overset{(4.7)}{=} \begin{bmatrix} b_i \\ a_i' \end{bmatrix}_I \begin{bmatrix} q \\ a_i' \end{bmatrix}_I = \begin{bmatrix} b_i q \\ a_i' \end{bmatrix}_I \overset{(4.8)}{=} \begin{bmatrix} hq \\ a_i' \end{bmatrix}_I \tag{4.9}$$

It is now possible to compute:

$$\prod_{i=1}^{r+1} \begin{bmatrix} b_i \\ a_i \end{bmatrix}_I^{e_i} \overset{(4.9)}{=} \prod_{i=1}^{r+1} \begin{bmatrix} hq \\ a_i' \end{bmatrix}_I^{e_i} = \begin{bmatrix} hq \\ \prod_{i=1}^{r+1} (a_i')^{e_i} \end{bmatrix}_I$$
$$\overset{(4.6)}{=} \begin{bmatrix} hq \\ \alpha^t \end{bmatrix}_I = \begin{bmatrix} hq \\ \alpha \end{bmatrix}_I^t = 1$$

The last equation follows from Lemma III.19. The computation shows that the elements satisfy some non-trivial relation. Therefore, the rank of the universal Mennicke group is less or equal to r. □

Combining the last two lemma we finally get:

Theorem III.21 ([**Mor07**, Thm. 3.11]; [**CKP92**]). *Let R be an integral domain that satisfies the properties $\mathrm{SR}_{1\frac{1}{2}}$, $\mathrm{Gen}(t,r)$ and $\mathrm{Exp}(t,l)$ for some natural numbers t, r, l and let $I \subset R$ be an ideal.*
The universal Mennicke group A_I is finite. More precisely:

$$|A_I| \leq t^r$$

Proof. First assume that the ideal is a principal ideal. Then the universal Mennicke group is by III.20 a finitely generated abelian group. This means it is a direct product $A_I = \bigoplus C_i$ of cyclic groups C_i. Lemma III.19 implies that each of these cyclic groups is finite, thus A_I is finite.

If I is not principal, the conclusion follows from Lemma III.8. With some non-trivial element $q \in I$, the natural homomorphism $A_{qR} \to A_I$ will be surjective. This means that A_I is a quotient of a finite group, hence it is finite itself. □

5. A Mennicke symbol for $\mathrm{SL}_2(R)$

At the very beginning of this section we will introduce some additional notation. Define:

$$e_u := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, e_l := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and}$$
$$\mathrm{P} := \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

For elements a, b denote by $\mathrm{D}(a,b)$ the matrix:

$$\mathrm{D}(a,b) := \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

If v is a unit this will be abbreviated to $\mathrm{D}(v) := \mathrm{D}(v, v^{-1})$. Furthermore, we will use the common notation $a^b := b^{-1}ab$ for conjugated elements.

In addition, the following definitions are required for the next sections.

Definition III.22. Throughout this section

(1) R will denote an integral domain that satisfies $\mathrm{SR}_{1\frac{1}{2}}$, $\mathrm{Gen}(2,1)$, $\mathrm{Unit}(1,x)$ and $\mathrm{Conj}(z)$ for positive integers x and z,
(2) I will be an ideal of R, and
(3) K is the localization of R at R (see III.31), i.e. K is a field that contains R as a subring.

Next, a connection between Mennicke symbols and bounded generation will be established by proving the following theorem:

Theorem III.23 ([**Mor07**])**.** *Let $\mathcal{N}$ be a normal subgroup of $\mathrm{SL}_2(R;I)$ that satisfies*

$$\mathrm{E}_2^{\triangleleft}(I) \subset \mathcal{N} \text{ and} \tag{5.1}$$

$$\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mathcal{N} \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \mathcal{N}. \tag{5.2}$$

The map $[\,] : W_I \to \mathrm{SL}_2(R;I)/\mathcal{N}$, defined by

$$\begin{bmatrix} b \\ a \end{bmatrix} := \begin{pmatrix} a & b \\ * & * \end{pmatrix} \mathcal{N}$$

is a well-defined Mennicke symbol.

Remark III.24. Note that the condition of (5.2) is not a strong restriction on $\mathcal{N}$. It can be forced by replacing the subgroup $\mathcal{N}$ by $N \cap \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) N \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Because conjugation by the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ fixes $\mathrm{SL}_2(R;I)$ and $\mathrm{E}_2^{\triangleleft}(I)$, the replacement group now satisfies the condition (5.2).

The following section treats the proof of Theorem III.23. The most difficult part of the proof is to show that the map $[\,]$ defined above satisfies the property (M4). The proof will be divided into two parts, first treating the other properties that are easier to verify.

Proof of Theorem III.23, Part 1. First we are going to prove that the map is well defined and satisfies the properties (M1) and (M2). If $(a,b) \in W_I$, then by remark III.3 there are $c, d \in R$, such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R;I)$. Assume there is a second pair $c', d' \in R$ with $\left(\begin{smallmatrix} a & b \\ c' & d' \end{smallmatrix}\right) \in$

$\mathrm{SL}_2(R;I)$. Thus

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c' & d' \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \text{ for some } x \in I \tag{5.3}$$

By the condition $\mathrm{E}_2^{\lhd}(I) \subset N$, the two possible images of $(a,b) \in W_I$ represent the same element in A and the map $[\,]$ is well-defined.

The properties (M1) and (M2) follow from simple computations:

(1) M1 : For $t \in I$ take the matrix $e_u(t) = \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{E}_2(I)$ and compute:

$$\begin{pmatrix} a & b \\ * & * \end{pmatrix} e_u(t) = \begin{pmatrix} a & b+ta \\ * & * \end{pmatrix}$$

This implies $\left[\begin{smallmatrix} b+ta \\ a \end{smallmatrix}\right] = \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$, as $\mathrm{E}_2^{\lhd}(I) \subset N$.

(2) M2: Take the matrix $e_l(s) = \left(\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix}\right)$ for $s \in R$. Thus:

$$\begin{pmatrix} a & b \\ * & * \end{pmatrix} [\left(\begin{smallmatrix} a & b \\ * & * \end{smallmatrix}\right), e_l(s)] = \begin{pmatrix} a & b \\ * & * \end{pmatrix}^{e_l(s)} = \begin{pmatrix} a+sb & b \\ * & * \end{pmatrix}$$

Hence we have $\left[\begin{smallmatrix} b \\ a+sb \end{smallmatrix}\right] = \left[\begin{smallmatrix} b \\ a \end{smallmatrix}\right]$, as $[\mathrm{E}_2(R), \mathrm{SL}_2(R;I)] \subset N$ by lemma III.27 (which will be proved later on).

□

Below the proofs of a variety of lemmas that will be important later on, especially lemma III.27 and III.29. These will be applied in the second part of the proof of Theorem III.23.

The following lemma will be cited without a proof. A proof for the first fact can be found in [**Bas64**, Thm. 4.2], the second one is proved in the article by Witte Morris [**Mor07**].

Lemma III.25 ([**Mor07**, Cor. 2.15], [**Mor07**, Lem. 5.6])**.** *Let S be a commutative ring and $J' \subset J$ ideals in S. If S/J' satisfies* SR_1*, then*

$$\mathrm{SL}_2(S;J) = \mathrm{SL}_2(S;J')\,\mathrm{E}_2^{\lhd}(J) \tag{5.4}$$

If instead J and J' are ideals such that $J' \subset J^2$ then

$$\mathrm{SL}_2(S;J^2) \subset \mathrm{SL}_2(S;J')\,\mathrm{E}_2(J) \tag{5.5}$$

The next lemma, using the conjugation property, will allow the specify of the subgroup in which the commutator $[\mathrm{e}_2(R), \mathrm{SL}_2(R;I)]$ is contained.

Lemma III.26. *For any $A \in \mathrm{GL}_2(K)$ and any ideal $J \subset R$ there is a nonzero ideal $J' \subset J$, such that*

$$A^{-1}\mathrm{E}_2(J')A \subset \mathrm{E}_2(J)$$

Proof. It is well-established that any matrix in $\mathrm{SL}_2(K)$ can be written as a product of $e_u = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathrm{P} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and matrices of the form

$\mathrm{D}(a,b) = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ for $a, b \in K$. More explicitly if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ then a possible decomposition is given by:

$$A = \mathrm{P}\mathrm{D}(a^{-1}c, 1)e_u\mathrm{D}(ac^{-1}d - b, a)\mathrm{P}\mathrm{D}(a^{-1}b, 1)e_u\mathrm{D}(ab^{-1}, 1)$$

In order to prove the lemma it suffices to find ideals J_p, J_{e_u} and $J_{\mathrm{D}(a,b)}$, such that the elementary matrices with entries in one of those ideals are mapped into $\mathrm{E}_2(J)$ by the conjugation action of the corresponding matrix. Because the ideal J was arbitrary, the statement of the lemma then follows by recursively applying the statements for the specific elements. The proofs for the different elements will be carried out elements separately:

(1) P: The conjugation by p maps the elementary matrices $e_l(a)$ to $e_u(a)$. This implies that $\mathrm{e}_2(J)$ is invariant under the conjugation by p for any ideal J.

(2) $\mathrm{D}(a,b)$: For an arbitrary ideal J define the ideal

$$J_{\mathrm{D}(a,b)} = a^{-1}bJ \cap b^{-1}aJ \cap R.$$

This ideal satisfies $\mathrm{D}(a,b)^{-1}\mathrm{E}_2(J_{\mathrm{D}(a,b)})\mathrm{D}(a,b) \subset \mathrm{E}_2(J)$.

(3) e_u: We will prove the following statement: There is an ideal $J_{e_u} \subset J$, such that

$$e_u^{-1}\mathrm{e}_2(J_{e_u})e_u \subset \langle \mathrm{e}_2(J)\rangle_{33z},$$

i.e. the e_u-conjugates of any elementary matrix in $\mathrm{e}_2(J_{e_u})$ is a product of finitely many elementary matrices in $\mathrm{e}_2(J)$. Because the group $e_u(*) = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) | a \in R\}$ is commutative, we only need to carry out the proof for e_u-conjugates of elementary matrices of the form $e_l(a) = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$.

First of all, observe the following: For any unit $v \in R$ there is

$$\begin{aligned} e_l(a)^{\mathrm{D}(v)} &= e_l(v^2a) \text{ and} \\ e_u(a)^{\mathrm{D}(v)} &= e_u(av^{-2}). \end{aligned}$$

This leads to:

$$((e_l(a)^{e_u^{-1}})^{\mathrm{D}(v)})^{e_u} = e_l(v^2a)^{e_u(1-v^{-2})}.$$

If now v is a unit with $v^2 - 1 \in qR$ obtain:

$$A^{e_u} \in \mathrm{e}_2(qR) \implies (A^{\mathrm{D}(v)})^{e_u} \in \langle \mathrm{e}_2(qR)\rangle_3 \tag{5.6}$$

Now fix some $q \in J$ and a unit $u \in R$ with $u^2 \neq 1$ and $u \equiv 1 \bmod qR$ (which exists by the unit property). By the conjugation property, there is a q', such that any element of the ideal $q'R$ is a sum of z or less elements of the form ys^{-2}, with $y \in \mathcal{M}_qR$ and $s \equiv 1 \bmod qR$. If we define $J_{e_u} := (1 - u^2)q'R$, the only thing left to show is that for $y \in \mathcal{M}_{qR}$ and $s \equiv 1 \bmod qR$ it follows:

$$e_l((1-u^2)ys^{-2})^{e_u} \in \langle \mathrm{e}_2(J)\rangle_{33}$$

So let y be in $\mathcal{M}_{qR}$, i.e. there are $z, u_1 \in R$ with:

$$\begin{aligned} z &\equiv 1 \bmod qR \\ u_1^2 &= 1 + zy \end{aligned}$$

The first condition can be established by changing y to $-y$, if necessary. Now define

$$\begin{aligned} w &:= (u^2-1)u_1^{-2}, \\ M &:= \begin{pmatrix} 1 & z-1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \in \langle \mathrm{e}_2(qR)\rangle_2 \\ e_u(c) &:= e_u(w(1-z+yz)) \in \mathrm{e}_2(qR) \end{aligned}$$

With these definitions it is an elementary computation to show that

$$e_l(-wy) = M^{e_u^{-1}} \mathrm{D}(u)^{-1} (e_u(c)M^{-1})^{e_u^{-1}} \mathrm{D}(u)$$

Note that $(((e_u(c)M^{-1})^{e_u^{-1}})^{\mathrm{D}(u)})^{e_u} \in \langle \mathrm{e}_2(qR)\rangle_9$ by (5.6) and therefore $e_l(-wy)^{e_u} \in \langle \mathrm{e}_2(qR)\rangle_{11}$. The last step of the proof is now to observe, that $u_1^2 = 1 + zy \equiv 1 \bmod qR$. This implies $(su_1^{-1})^2 \equiv 1 \bmod qR$. Thus

$$e_l((1-u^2)ys^{-2}) = e_l(-wy\tfrac{s^2}{u_1^2}) = e_l(-wy)^{\mathrm{D}(s/u_1)}$$

and by (5.6) deduce

$$e_l((1-u^2)ys^{-2}) \in \langle \mathrm{e}_2(qR)\rangle_{33}.$$

.

This completes the proof. □

The following lemma is central.

Lemma III.27. $[\mathrm{E}_2(R), \mathrm{SL}_2(R;I)] \subset \mathrm{E}_2^{\triangleleft}(I)$

Proof. Let u be a unit satisfying the properties of definition III.15 (2). Take $T \in \mathrm{SL}_2(R;I)$ and $A = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{E}_2(R)$ and define $k = 2(u^2-1) \in R$ and $U = \left(\begin{smallmatrix} u & 0 \\ 0 & u^{-1} \end{smallmatrix}\right)$. With $e = \left(\begin{smallmatrix} 1 & ak^{-1} \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ follows:

$$A = e^{-1}Ue^2U^{-1}e^{-1}$$

Regard T and A as elements of $\mathrm{SL}_2(K)$ and apply Lemma III.26 multiple times to find ideals $J_4 \subset J_3 \subset J_2 \subset J_1 \subset I$, such that

$$\begin{aligned}
&T^{-1}\mathrm{E}_2(J_1)T \subset \mathrm{E}_2(I),\\
&A^{-1}\mathrm{E}_2(J_2)A \subset \mathrm{E}_2(J_1),\\
&e^{-1}\mathrm{E}_2(J_3)e \subset \mathrm{E}_2(J_2) \quad \text{and}\\
&e^{2}\mathrm{E}_2(J_4)e^{-2} \subset \mathrm{E}_2(J_3).
\end{aligned}$$

By restriction to a smaller ideal, we can assume that each of the ideals J_i is principal. This will be necessary for the application of the unit property $\mathrm{Unit}(1,x)$. Now Lemma III.25 allows to decompose T as

$$T = XE \quad \text{ with } X \in \mathrm{SL}_2(R; k^2 J_4) \text{ and } E \in \mathrm{E}_2^{\triangleleft}(I).$$

The following facts will be used:

$$\begin{aligned}
U\mathrm{E}_2(\tilde{I})U^{-1} &\subset \mathrm{E}_2(\tilde{I}) \qquad \text{for any ideal } \tilde{I},\\
X_1 &:= eXe^{-1} \in \mathrm{SL}_2(R; J_4) \quad \text{and}\\
X_2 &:= e^{-1}Xe \in \mathrm{SL}_2(R; J_4).
\end{aligned}$$

The unit property allows to substitute some elements $e_i, e'_I \in \mathrm{e}_2(J_4)$:

$$\begin{aligned}
&U^{-1}X_1U = e_1X_1e_2\dots e_x \quad \text{and}\\
&UX_2U^{-1} = e'_1\dots e'_x
\end{aligned}$$

Now compute the commutator of A and T:

$$\begin{aligned}
[T;A] &= T^{-1}A^{-1}TA = T^{-1}A^{-1}XA(A^{-1}EA) \in T^{-1}A^{-1}\underbrace{X}_{=e^{-1}UU^{-1}X_1UU^{-1}e}A\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&= T^{-1}A^{-1}e^{-1}UU^{-1}\underbrace{X_1}_{\in \mathrm{SL}_2(J_4)}UU^{-1}eA\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&= T^{-1}A^{-1}e^{-1}U\underbrace{e_1}_{\in \mathrm{E}_2(J_4)}X_1\underbrace{e_2\dots e_x}_{\in \mathrm{E}_2(J_4)}U^{-1}eA\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&\subset \mathrm{E}_2(I)\cdot T^{-1}A^{-1}e^{-1}U\underbrace{X_1}_{=e^2U^{-1}UX_2U^{-1}Ue-2}U^{-1}eA\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&= \mathrm{E}_2(I)\cdot T^{-1}A^{-1}e^{-1}Ue^2U^{-1}U\underbrace{X_2}_{\in \mathrm{SL}_2(R;J_4)}U^{-1}Ue^{-2}U^{-1}eA\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&= \mathrm{E}_2(I)\cdot T^{-1}A^{-1}e^{-1}Ue^2U^{-1}\underbrace{e'_1}_{\in \mathrm{E}_2(J_4)}X_2\underbrace{e'_2\dots e'_x}_{\in \mathrm{E}_2(J_4)}Ue^{-2}U^{-1}eA\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&\subset \mathrm{E}_2(I)\cdot T^{-1}A^{-1}e^{-1}Ue^2U^{-1}X_2Ue^{-2}U^{-1}eA\cdot \mathrm{E}_2^{\triangleleft}(I)\\
&\subset \mathrm{E}_2^{\triangleleft}(I)
\end{aligned}$$

A similar proof also gives us this statement for a matrix $A' = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$. The case of arbitrary element of $\mathrm{E}_2(R)$ now easily follows, as any element of $\mathrm{E}_2(R)$ is a finite product of elementary matrices. □

It is possible to modify the proof of Lemma III.27 to obtain a very similar result, stated in the corollary below. For an elementary matrix the proof is similar to the one stated above, except that the ideal I is replaced by an ideal I' that satisfies $I' \subset I^2$ and $A\mathrm{E}_2(I')A^{-1} \subset \mathrm{E}_2(I)$. This is possible according to Lemma III.26. Note that the second part of Lemma III.25 needs to be applied instead of the first one. For general matrices in $\mathrm{SL}_2(K)$, the claim follows from the fact that they can be written as a finite product of elementary matrices (because K is a field).

Corollary III.28. *For any $A \in \mathrm{SL}_2(K)$, there is an ideal J', such that $[A, \mathrm{SL}_2(R; J')] \subset \mathrm{E}_2^{\lhd}(I)$.*

The second important lemma now is a simple conclusion.

Lemma III.29. *For every $y \in R$ there is an ideal $I' \subset I$ such that*

$$\begin{bmatrix} by^2 \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} \qquad \forall (a, b) \in W_{I'}$$

Proof. According to Corollary III.28 there is an ideal I' satisfying $\left[\left(\begin{smallmatrix} y & 0 \\ 0 & y^{-1} \end{smallmatrix}\right), \mathrm{SL}_2(R; I')\right] \subset \mathrm{E}_2^{\lhd}(I)$. A simple computation yields:

$$\begin{aligned} \begin{bmatrix} by^2 \\ a \end{bmatrix} &= \begin{pmatrix} a & by^2 \\ * & * \end{pmatrix} \mathcal{N} = \begin{pmatrix} y & 0 \\ 0 & y^-1 \end{pmatrix} \begin{pmatrix} a & b \\ * & * \end{pmatrix} \begin{pmatrix} y^{-1} & 0 \\ 0 & y \end{pmatrix} \mathcal{N} \\ &= \begin{pmatrix} a & b \\ * & * \end{pmatrix} \left[\left(\begin{smallmatrix} a & b \\ * & * \end{smallmatrix}\right), \left(\begin{smallmatrix} y^{-1} & 0 \\ 0 & y \end{smallmatrix}\right)\right] N = \begin{bmatrix} b \\ a \end{bmatrix} \end{aligned}$$

using that $\mathrm{E}_2^{\lhd}(I') \subset \mathcal{N}$. This proves the desired statement. □

Now the proof of this section's main theorem can be completed.

Proof ofTheorem III.23, Part 2. First assume that the ideal I is principal: $I = qR$, for some $q \in R$. Furthermore, by the remark III.6 it is sufficient to prove

$$\begin{bmatrix} bq \\ a_1 \end{bmatrix} \begin{bmatrix} bq \\ a_2 \end{bmatrix} = \begin{bmatrix} bq \\ a_1 a_2 \end{bmatrix},$$

whenever $\left[\begin{smallmatrix} bq \\ a_1 \end{smallmatrix}\right] = \mathbb{1}$ or $\left[\begin{smallmatrix} bq \\ a_2 \end{smallmatrix}\right] = \mathbb{1}$. Note that in this case $\left[\begin{smallmatrix} bq \\ a_1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} bq \\ a \end{smallmatrix}\right]_2$ will commute with each other and we can assume that $\left[\begin{smallmatrix} bq \\ a_2 \end{smallmatrix}\right] = \mathbb{1}$ without loss of generality.

Following a proof by cases:

(1) $a_2 \equiv y^2 \bmod bqR$, for some $y \in R$.
(2) $a_1 \equiv y^2 \bmod bqR$, for some $y \in R$.
(3) $a_1 a_2 \equiv y^2 \bmod bqR$, for some $y \in R$.

To prove the first case, take $a_2' := y^2 \equiv a_2 \bmod bqR$. By Lemma III.29 there is an ideal $I' \subset I$, such that

$$\begin{bmatrix} xa_2' \\ z \end{bmatrix} = \begin{bmatrix} x \\ z \end{bmatrix} \tag{5.7}$$

for any $(x, z) \in W_{I'}$. Furthermore, as $(bq, a_1a_2') \in W_I$, we have

$$bR + a_1a_2'R \supset bqR + a_1a_2R = R/I'.$$

The property $\mathrm{SR}_{1\frac{1}{2}}$ (or more precisely SR_1 for R/I') ensures that there is an element $b' \equiv b \bmod a_1a_2'R$ with $b'R + I' = R$. This implies the existence of an element $t \in R$, such that

$$tb' = 1 \bmod I'. \tag{5.8}$$

Define $a_1' := a_1 - (1 - a_1)tb'$. This element satisfies $a_1' \equiv a_1 \bmod b'I$ and $a_1' \equiv 1 \bmod I'$ by (5.8). Note that this implies $(a_1' - 1) \in I'$. Let c, d be such that $\left(\begin{smallmatrix} a_2' & b'q \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R; I)$. Therefore

$$a_2d = 1 + cb \equiv 1 \bmod b \tag{5.9}$$

Using the properties of Mennicke symbols, now compute:

$$\begin{aligned}
\begin{bmatrix} bq \\ a_1a_2 \end{bmatrix} \begin{bmatrix} bq \\ a_2 \end{bmatrix}^{-1} &= \begin{bmatrix} bq \\ a_1a_2' \end{bmatrix} \begin{bmatrix} bq \\ a_2' \end{bmatrix}^{-1} = \begin{bmatrix} b'q \\ a_1a_2' \end{bmatrix} \begin{bmatrix} b'q \\ a_2' \end{bmatrix}^{-1} \\
&= \begin{bmatrix} b'q \\ a_1'a_2' \end{bmatrix} \begin{bmatrix} b'q \\ a_2' \end{bmatrix}^{-1} = \begin{pmatrix} a_1a_2 & bq \\ * & * \end{pmatrix} \begin{pmatrix} a_2 & bq \\ c & d \end{pmatrix}^{-1} \\
&= \begin{pmatrix} a_1a_2 & bq \\ * & * \end{pmatrix} \begin{pmatrix} d & -bq \\ -c & a_2 \end{pmatrix} \\
&= \begin{pmatrix} a_1a_2d - bqc & -a_1a_2bq + bqa_2 \\ * & * \end{pmatrix} \\
&= \begin{pmatrix} 1 - a_2d(1 - a_1) & a_2bq(1 - a_2) \\ * & * \end{pmatrix} \\
&= \begin{bmatrix} a_2'b'q(1 - a_1') \\ 1 - a_2'd(1 - a_1') \end{bmatrix} \overset{(5.7)}{=} \begin{bmatrix} b'q(1 - a_1') \\ 1 - a_2'd(1 - a_1') \end{bmatrix} \\
&\overset{(5.9)}{=} \begin{bmatrix} b'q(1 - a_1') \\ a_1' \end{bmatrix} = \begin{bmatrix} b'q \\ a_1' \end{bmatrix} = \begin{bmatrix} bq \\ a_1 \end{bmatrix}
\end{aligned} \tag{5.10}$$

This proves the statement in the first case.

The proof for the second case is immediately obtained from the first case, due to the commutativity of $\left[\begin{smallmatrix} bq \\ a_1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} bq \\ a_2 \end{smallmatrix}\right]$.

Now assume $a_1a_2 = y^2 \bmod bqR$ for some $y \in R$. Under the condition (5.2) it follows :

$$\begin{bmatrix} bq \\ a_2 \end{bmatrix} = \mathbb{1} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mathbb{1} \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \begin{bmatrix} bq \\ a_2 \end{bmatrix} \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \begin{bmatrix} -bq \\ a_2 \end{bmatrix} \tag{5.11}$$

Take again $c, d \in R$ satisfying $\left(\begin{smallmatrix} a_2 & -bq \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R; I)$. From the fact that $\left(\begin{smallmatrix} a_2 & -bq \\ c & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} d & bq \\ -c & a_2 \end{smallmatrix}\right)$ compute:

$$\begin{bmatrix} bq \\ a_2 \end{bmatrix}^{-1} \overset{(5.11)}{=} \begin{bmatrix} -bq \\ a_2 \end{bmatrix}^{-1} = \begin{bmatrix} bq \\ d \end{bmatrix} \tag{5.12}$$

Now use the result from the first case to compute:

$$\begin{bmatrix} bq \\ a_1a_2 \end{bmatrix} \begin{bmatrix} bq \\ a_2 \end{bmatrix}^{-1} \overset{(5.12)}{=} \begin{bmatrix} bq \\ a_1a_2 \end{bmatrix} \begin{bmatrix} bq \\ d \end{bmatrix} = \begin{bmatrix} bq \\ a_1a_2d \end{bmatrix} = \begin{bmatrix} bq \\ a_1 \end{bmatrix}$$

The last equality makes use of $1 = a_2d - bqc \equiv a_2d \bmod bqR$.

It still has to be proved that at least one of the three cases occurs for any choice of the elements a_1 and a_2. This is where the few generator property $\mathrm{Gen}(2, 1)$ will be used.

Because of $(bq, a_1a_2) \in W_I$, it follows

$$bR + a_1a_2R \supset bqR + a_1a_2R = R$$

and by $\mathrm{SR}_{1\frac{1}{2}}$ find $\tilde{b} \in R$ with

$$\begin{aligned} \tilde{b} &= b \bmod a_1a_2R \quad \text{ and} \\ \tilde{b}R + qR &= R. \end{aligned} \tag{5.13}$$

It remains $(a_1a_2, \tilde{b}q) \in W_I$ and

$$a_1a_2R + \tilde{b}R = R. \tag{5.14}$$

(5.13) and (5.14) together give:

$$\tilde{b}R + a_1a_2qR = R \tag{5.15}$$

It is now possible to apply the few generator property. Hence, there is an element $b' \in R$, such that

$$\begin{gathered} b' \equiv \tilde{b} \bmod qa_1a_2R \quad \text{ and} \\ (R/b'R)^\times/((R/b'R)^\times)^2 \text{ is cyclic.} \end{gathered}$$

Because $\tilde{b}$ was only changed by an element of the ideal qR, it remains $b'R + qR = R$, i.e. b' and q are coprime. Furthermore $(a_1a_2, b'q) \in W_I$ and $a_1a_2R + b'qR = R$, implying that a_1a_2 is a unit in $R/b'R$. The same holds for the elements a_1 and a_2. So they can be considered as elements of $(R/b'R)^\times/((R/b'R)^\times)^2$. Because this group is cyclic and has order 2, at least one of the elements a_1, a_2, a_1a_2 has to be trivial in this group. In other words, there is at least one element that is a square modulo $b'R$. Without loss of generality it can be assumed $a_1 \equiv y^2 \bmod b'R$. Remember that $(a_1, bq) \in W_I$ implies $a_1 \equiv 1 \bmod qR$.

b' and q are coprime, so according to the Chinese remainder theorem $R/b'qR$ is isomorphic to $R/b'R \times R/qR$. This means that

$$y' = (y, 1) \in R/b'R \times R/qR \cong R/bqR$$

is an element that satisfies $y'^2 \equiv a_1 \bmod bqR$. This finishes the proof in the case of a principal ideal.

It remains to prove that the assumption of the ideal being principal is not a restriction. So let I be arbitrary and take $(a_1, b), (a_2, b) \in W_I$. As above $c, d \in R$ are such that $\left(\begin{smallmatrix} a_2 & -bq \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R; I)$.

$$\begin{bmatrix} b \\ a_1 a_2 \end{bmatrix} \begin{bmatrix} b \\ a_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_2(1-a_1) \\ 1 - a_2 d(1-a_1) \end{bmatrix} \underbrace{\begin{bmatrix} 1-a_1 \\ 1 - a_2 d(1-a_1) \end{bmatrix}}_{=\mathbb{1}}$$

$$= \begin{bmatrix} a_2 b(1-a_1)^2 \\ 1 - a_2 d(1-a_1) \end{bmatrix} \tag{5.16}$$

$$= \underbrace{\begin{bmatrix} a_2(1-a_1) \\ 1 - a_2 d(1-a_1) \end{bmatrix}}_{=\mathbb{1}} \begin{bmatrix} b(1-a_1) \\ 1 - a_2 d(1-a_1) \end{bmatrix} \tag{5.17}$$

$$= \begin{bmatrix} b(1-a_1) \\ a_1 - bc(1-a_1) \end{bmatrix} = \begin{bmatrix} b \\ a_1 \end{bmatrix}$$

The first equation follows from a computation that was part of equation 5.10. In the steps (5.16) and (5.17) we used that the restriction of $[\ ]$ to the principal ideal $(1-a_1)R \subset I$ is a Mennicke symbol.

This completes the last step of the proof. □

6. Number rings

Up until now, the existence of rings satisfying the ring theoretic properties of Section 3 is not described. However, there are concrete examples of such rings, which will be shortly presented in this section. For simplicity, we will not verify the desired properties in detail, but instead refer to the article [**Mor07**], where all the proofs can be found.

The following definitions will be necessary.

Definition III.30. Let K be an algebraic extension of $\mathbb{Q}$. An order in K is a subring $\mathcal{O}$ with the following properties:

(1) $\mathbb{Q}\mathcal{O} = K$
(2) $\mathcal{O}$ is a lattice in K

Example. The set $\mathcal{O}_K$ of algebraic integers in K is an order in K. Recall that $\mathcal{O}_K$ is the set of all elements $a \in K$, which are a root of some monic polynomial f with coefficients in $\mathbb{Z}$.

Definition III.31. Let R be a ring and S a multiplicative subset. The localization of R at S is a ring denoted by $S^{-1}R$ together with a map $f : R \to S^{-1}R$, such that the following universal property holds: If R' is any ring and there is a map $f' : R \to R'$, such that every element of S is mapped to a unit, then there is a unique map $g : R \to R'$, making the following diagram commutative:

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[dr, "f'"'] & R \arrow[d, "g"'] \\
 & R'
\end{tikzcd}$$

Remark III.32. If the ring R has no zero divisors then the localization at a subset S that does not contain 0 is easily constructed as the ring of fractions: $S^{-1}R = \{\frac{r}{s} | r \in R, s \in S\}$.

Now let K be an algebraic number field of degree $k < \infty$ over $\mathbb{Q}$. Take an order B in K and a multiplicative subset $S \subset B$. Define the ring A to be the localization $A = S^{-1}B$ of B at S.

Theorem III.33 ([**Mor07**]). *Let A be a ring as above and assume that A has infinitely many units. Then A satisfies the properties $\mathrm{SR}_{1\frac{1}{2}}$, $\mathrm{Gen}(2,1)$, $\mathrm{Gen}(t,r)$, $\mathrm{Exp}(t,l)$, $\mathrm{Unit}(1,x)$ and $\mathrm{Conj}(z)$ for positive integers r, x, l, t and z.*

In the following, only rings of the form $A = S^{-1}B$ will be considered.

7. Bounded Generation in $\mathrm{SL}_2(A)$

In this section we will finally prove the main theorem of this chapter. We will start by recalling the compactness theorem of first order logic.

7.1. The Compactness Theorem of first order logic. For the formulation of the compactness theorem the following definitions are required.

Definition III.34. A *first-order language* $\mathcal{L}$ consists of the following data:

The alphabet of $\mathcal{L}$, which is the disjoint union of the following sets:

(1) V, the set of variables,
(2) a set of logical symbols,
(3) $\{=\}$, the equal symbol,
(4) $\{(,)\}$, a set of parentheses,
(5) and the symbol set S, containing
    (a) a set $\mathcal{R}_n$ of n-ary relation symbols for every $n \in \mathbb{N}$,
    (b) a set $\mathcal{F}_n$ of n-ary function symbols for every $n \in \mathbb{N}$,
    (c) a set $\mathcal{C}$ of constant symbols.

The terms of $\mathcal{L}$ is the set that contains:

(1) any $v \in V$,
(2) any constant symbol $c \in C$,
(3) any $f(x_1, \ldots, x_n)$, for a n-ary function $f \in F_n$ and terms $x_1, \ldots, x_n$.

Formulas of $\mathcal{L}$ are:

(1) $(x_1 = x_2)$, if x_1 and x_2 are terms of the language,
(2) $(R(x_1, \ldots, x_n))$, for a n-ary relation R and terms x_i,
(3) $(\neg\varphi)$, for a formula φ,
(4) $(\varphi \vee \psi)$, for formulas φ and ψ,
(5) $(\exists x \varphi(x))$, for a formula φ and a variable x.

Example (The language of rings)**.** The language of rings has the binary function symbols $+, -, \times$, representing the binary operations, and two constant symbols $0, 1$, representing zero and the identity of a ring.

To be able to assign a meaning to the formulas of a language $\mathcal{L}$ we need the notion of an interpretation, given in the next definition.

Definition III.35. An *interpretation* of a first order language is a tuple $(D, \mathcal{I})$, where D is a non-empty set and $\mathcal{I}$ is a function that assigns

(1) an element of D to every constant symbol,
(2) a n-ary function $D^n \to D$ to every function symbol and
(3) a n-ary relation (i.e. a subset of D^n) to every n-ary relation symbol.

It can be shown that this allows the assignment of a truth value (i.e. the value $true$ or $false$) to any formula of the language. A formula is said to be satisfied in the interpretation, if its assigned value is $true$.

Definition III.36. If a formula φ is satisfied in an interpretation $\mathcal{I}$, we say that $\mathcal{I}$ is a model for φ and write $\mathcal{I} \models \varphi$. The same applies if Φ is a set of formulas: $\mathcal{I} \models \Phi \Leftrightarrow \mathcal{I} \models \varphi \ \forall \varphi \in \Phi$

Φ is said to imply ψ, if every model for Φ is also a model for ψ. This is denoted by $\Phi \models \psi$.

Now all the requirements for the formulation of the compactness theorem are fulfilled.

Theorem III.37 (The Compactness Theorem of first-order logic)**.** *Let Φ be a set of first-order formulas. Then Φ has a model if and only if every finite subset $\Phi_0 \subset \Phi$ has a model.*

For a proof of the compactness theorem we just refer to the introductory text [**EFT07**], as a full proof would go beyond the scope of this thesis. We conclude this subsection with the following remark.

Remark III.38. The name of the compactness theorem has the following origin: For any set of first-order formulas Φ, which has a model, choose a model $\mathcal{M}_\Phi$. Let $X = \{\mathcal{M}_\Phi | \Phi \text{ has a model}\}$ be the set of all such models and set $X_\varphi = \{\mathcal{M} \in X | \mathcal{M} \models \varphi\}$ for any formula φ.

Then the collection of all X_φ defines a basis for a topology on X. The statement of the compactness-theorem is precisely that X, endowed with this topology, is a compact space.

7.2. Bounded Generation in $\mathrm{SL}_2(A)$. The theorem of bounded generation in the group $\mathrm{SL}_2(A)$ stated later on is a consequence of the following more general theorem.

Theorem III.39 ([**Mor07**, Cor. 2.8])**.** *Let $\mathcal{L}$ be a first-order language containing:*

(1) the language of rings $(+,-,\times,0,1)$;
(2) variables x_{ij}, $1 \leq i,j \leq n$;
(3) two relation symbols $G(x_{ij})$ and $H(x_{ij})$;
(4) constant symbols C_k, $k \in \mathbb{N}$;
(5) additional variables, constant symbols and relation symbols.

Let $\mathcal{T}$ be a collection of first-order expressions, such that every model $(D,\mathcal{I})$ of $\mathcal{T}$ has the following properties:

(1) D is a commutative ring, and
(2) with the definitions

$$\begin{aligned} G_D &= \{(x_{ij})|x_{ij} \in D, G(x_{ij})\}, \quad \text{and} \\ E_D &= \{(x_{ij})|x_{ij} \in D, H(x_{ij})\}, \end{aligned}$$

G_D is a subgroup of $\mathrm{SL}_n(D)$ and E_D generates a finite-index subgroup in G_D.

Then for any model $(D,\mathcal{I})$ the set E_D boundedly generates the subgroup $\langle E_D\rangle$ of G_D.

Proof. To the set $\mathcal{T}$ add for every $i,j,r \in \mathbb{N}$, $j \neq i$, expressions that specify

$$\begin{aligned} C_i &\in G_D, \\ C_i^{-1}C_j &\notin \langle E_D\rangle_r. \end{aligned}$$

This extension of $\mathcal{T}$ is not consistent: The condition $C_i^{-1}C_j \notin \langle E_D\rangle$ for any $r \in \mathbb{N}$ implies that $C_i^{-1}C_j$ is not in the set $\langle E_D\rangle$. Therefore, the subgroup $\langle E_D\rangle$ has infinitely many cosets in G, in contradiction to the assumption that this subgroup is of finite index.

Application of the compactness Theorem III.37 therefore yields an inconsistent finite subset of these expressions. This means that there is a number $r \in \mathbb{N}$, such that for any $C_1, C_2, \ldots C_r \in G_D$ there are $i,j \in \mathbb{N}$ with $i \neq j$ and $C_i^{-1}C_j \in \langle E_D\rangle_{r-1}$.

Now assume the existence of elements $C_i \in G_D$ $i \leq r$ that are a product of exactly $i \cdot r$ elements of E_D, i.e.:

$$C_i \in \langle E_D\rangle_{ir} \setminus \langle E_D\rangle_{ir-1}$$

This implies, that the word length of the C_i differ by at least r and hence:

$$C_i^{-1}C_j \notin \langle E_D\rangle_{r-1}$$

By the statement above, it is impossible to find elements with this property and therefore there is a $k \leq r$ such that

$$\langle E_D \rangle_{kr} = \langle E_D \rangle_{kr-1}$$

This implies $\langle E_D \rangle_{kr} = \langle E_D \rangle$ and the subgroup is boundedly generated. □

We now would like to apply Theorem III.39 to the situation where $G_D = \mathrm{SL}_2(A; I)$ and $E_D = \mathrm{E}_2^{\triangleleft}(I)$. Therefore, the only thing left to prove is that the elementary matrices generate a finite index subgroup in $\mathrm{SL}_2(A; I)$. This of course requires the ring R be of a special type.

In the following, denote by $A = S^{-1}B$ a ring like in Section 6, i.e. A is a ring that satisfies:

(1) $\mathrm{SR}_{1\frac{1}{2}}$,
(2) $\mathrm{Gen}(2,1)$ and $\mathrm{Gen}(t,r)$ for some $t, r \in \mathbb{N}_{>0}$,
(3) $\mathrm{Exp}(t,l)$ for $t, l \in \mathbb{N}_{>0}$,
(4) $\mathrm{Unit}(1,x)$ for $x \in \mathbb{N}_{>0}$ and
(5) $\mathrm{Conj}(z)$ for $z \in \mathbb{N}_{>0}$.

The proof of the next lemma is now easily obtained by just combining all the results from above.

Lemma III.40 ([**Mor07**, Thm. 5.13];[**CKP92**])**.** *Let A be a ring as above and let $I \subset A$ be an arbitrary ideal. Then $\mathrm{E}_2^{\triangleleft}(I)$ is of finite index in $\mathrm{SL}_2(A; I)$.*

Proof. The lemma can be proved using the results on Mennicke symbols from the foregoing sections. Theorem III.23 states that the quotient $\mathrm{SL}_2(A; I)/\mathrm{E}_2^{\triangleleft}(I)$ is the image of a Mennicke symbol. Hence, by the universal property (III.7) it is a quotient of the universal Mennicke group. The finiteness of the universal Mennicke group, proved in Theorem III.21, thus implies the finiteness of $\mathrm{SL}_2(A; I)/\mathrm{E}_2^{\triangleleft}(I)$. □

Finally, the chapter can be concluded with the central result.

Theorem III.41 ([**Mor07**, Thm.5.26];[**CKP92**])**.** *Let A be a ring as above. Then $\mathrm{E}_2^{\triangleleft}(I)$ is boundedly generated by $\mathrm{e}_2^{\triangleleft}(I)$ for any ideal I in A.*

Proof. In the notation of Theorem III.39 add to the language $\mathcal{T}$ formulas to ensure the following conditions for any model $(D, \mathcal{I})$:

(1) the ring D satisfies the properties $\mathrm{SR}_{1\frac{1}{2}}$, $\mathrm{Gen}(2,1)$, $\mathrm{Gen}(t,r)$, $\mathrm{Exp}(t,l)$, $\mathrm{Unit}(1,x)$ and $\mathrm{Conj}(z)$.
(2) $G_D = \mathrm{SL}_2(D; J)$ and $E_D = \mathrm{e}_2^{\triangleleft}(J)$ for some ideal $J \subset D$.

Application of Theorem III.39, which is now possible by Lemma III.40 completes the proof. □

IV

Ulam Stability of $\mathrm{SL}_2(A)$

Throughout this section A will denote a ring as in in section 6. Thus A is of the form $A = BS^{-1}$, with B being an order in the ring of algebraic integers in an algebraic number field K and $S \subset B$ a multiplicative subset. It will be assumed that A has an infinite number of units. As stated above, a ring A has the property that the elementary matrices $\mathrm{e}_2^{\triangleleft}(I)$ boundedly generate the group $\mathrm{E}_2^{\triangleleft}(I)$ in $\mathrm{SL}_2(R)$ for any ideal $I \subset R$.

1. Preliminaries

The proofs of the following well known lemmas are required for proving Ulam stability of $\mathrm{SL}_2(A)$. The first two lemmas concern properties of the ring A and will be used in the proofs of Lemma IV.6 and the main theorem (Theorem IV.7).

Lemma IV.1. *The ring A has a unit of infinite order.*

Proof. As the ring A has an infinite number of units, Dirichlet's unit theorem implies the existence of a unit that is not a root of unity. This already completes the proof. □

The second important property of A is proved in the next lemma.

Lemma IV.2. *Let I be an arbitrary ideal in A. Then $\mathrm{E}_2^{\triangleleft}(I)$ is of finite index in $\mathrm{SL}_2(A)$.*

Proof. As A is the localization of a number ring, any ideal I of A has finite index: $|A/I| < \infty$. This implies that the congruence subgroup $\mathrm{SL}_2(A;I)$ is of finite index in $\mathrm{SL}_2(A)$, i.e.

$$|\mathrm{SL}_2(A)/\mathrm{SL}_2(A;I)| = |\mathrm{SL}_2(A/I)| < \infty.$$

The conclusion of the lemma now follows from Lemma III.40:

$$\left|\frac{\mathrm{SL}_2(A)}{\mathrm{E}_2^{\triangleleft}(I)}\right| \leq |\mathrm{SL}_2(A/I)| \cdot \left|\frac{\mathrm{SL}_2(A;I)}{\mathrm{E}_2^{\triangleleft}(I)}\right| < \infty$$

□

Further, the character of a representation will be defined followed by the proof of a lemma for characters, which will be used in the sequel.

Definition IV.3. Let π be a finite-dimensional representation of a group G. The character χ of π is defined as:

$$\chi(g) = \mathrm{tr}(\pi(g))$$

If the representation is of dimension d, the character is also said to be d-dimensional.

The next lemma treats an important property of characters implying that a character is essentially unique.

Lemma IV.4. *One-dimensional characters of a group G are linearly independent in the space of functions of G.*

Proof. The objective is to show that if $\Phi_i, i = 1, \dots n$, are n different characters, then one has:

$$\sum_{i=1}^{n} a_i \Phi_i = 0 \Leftrightarrow a_i = 0 \ \forall i = 1, \dots n \tag{1.1}$$

This is done by induction on the number of summands. The claim holds for one summand, therefore, in order to do a proof by contradiction, assume that 1.1 holds for all $k \leq n$ and that there is a relation $\sum_{i=1}^{n+1} a_i \Phi_i = 0$, such that the Φ_i are pairwise different and not all of the a_i are zero. Observe that according to the inductive assumption $a_i \neq 0$ for every $i \leq n+1$.

Take a $g \in G$ with the property $\Phi_1(g) \neq \Phi_2(g)$, which exists because $\Phi_1 \neq \Phi_2$. Since one-dimensional characters are multiplicative the relation $\sum_{i=1}^{n+1} a_i \Phi_i = 0$ can be transformed into a new relation:

$$\sum_{i=1}^{n+1} a_i \Phi_i(g) \Phi_i(h) = \sum_{i=1}^{n+1} a_i \Phi_i(gh) = 0 \quad \forall h \in G \tag{1.2}$$

These two relations together now give:

$$\sum_{i=1}^{n+1} (\Phi_i(g) - \Phi_1(g)) a_i \Phi_i = \sum_{i=2}^{n+1} (\Phi_i(g) - \Phi_1(g)) a_i \Phi_i = 0 \tag{1.3}$$

But this is now a non-trivial relation $((\Phi_1(g) - \Phi_2(g)) a_2 \neq 0)$ with n summands in contradiction to the inductive assumption. □

2. Johnson's Theorem

In this section an important theorem by Johnson will be presented. The theorem will be used to prove Ulam stability of $\mathrm{SL}_2(A)$, but it is also interesting in that it implies that the representation close to a ε-representation is unique if the group is amenable.

Theorem IV.5 ([**Joh86**])**.** *If Γ is an amenable group, then every two unitary representations $\pi, \mu : \Gamma \to U(n)$ with $\|\pi - \mu\| < 1$ are unitarily conjugate.*

Proof. Let π and μ be such representations. Denote by $\int_\Gamma \mathrm{d}g$ the mean of the amenable group Γ. Define the following element $a \in U(n)$

$$a = \int_\Gamma \pi(g)\mu(g^{-1})\mathrm{d}g \tag{2.1}$$

Then a satisfies $\pi a = a\mu$:

$$\pi(g)a = \int_\Gamma \pi(gh)\mu(h^{-1})\mathrm{d}h = \int_\Gamma \pi(\hat{h})\mu(\hat{h}^{-1}g)\mathrm{d}\hat{h} = a\mu(g) \tag{2.2}$$

Furthermore a is non-zero and invertible, since:

$$\|a - 1\| \leq \int_\Gamma \|\pi(g)\mu(g^{-1}) - 1\|\mathrm{d}g = \int_\Gamma \|\pi(g) - \mu(g)\|\mathrm{d}g < 1 \tag{2.3}$$

Therefore the unitary part u of the polar decomposition $a = u|a|$ is a unitary that conjugates the representations. This finishes the proof. □

3. Ulam stability of $\mathrm{SL}_2(A)$

Now we have all the ingredients that are required to proof the Ulam stability of $\mathrm{SL}_2(A)$. The first step of the proof is to show that if π is a representation of A that satisfies a certain condition then there is an ideal I on which π is trivial. This will allow us to conclude that the elementary matrices $\mathrm{E}_2^{\triangleleft}(I)$ with entries in this ideal act almost trivial. The precise statement is the following:

Lemma IV.6. *Let $a \in A$ be a unit of infinite order. Let $\pi : A \to \mathrm{U}(n)$ be finite dimensional representation whose character is invariant under multiplication with a. Then there exists some $0 \neq q \in A$ such that $\pi|_{qA}$ is the trivial representation.*

Proof. As A is abelian, every irreducible representation is one-dimensional. This implies that the character $\Phi = \mathrm{tr}(\pi)$ of a d-dimensional representation is a sum of d one-dimensional characters

$$\Phi = \sum_{i=1}^{d} \Phi_i \qquad \text{for } \Phi_i : A \to \mathrm{U}(1) \quad 1 \leq i \leq d.$$

These characters Φ_i are unique up to permutation as this follows from Lemma IV.4.

By invariance of the character, multiplication by a therefore only permutes the summands Φ_i of the character Φ. As the permutation group of a finite set is finite, there exists a power a^n of a which leaves every single summand invariant:

$$\Phi_i(a^n b) = \Phi_i(b) \quad \forall b \in A$$

Dividing by the right hand-side gives:

$$\Phi_i((a^n - 1)b) = 1 \ \ \forall b \in A$$

With setting $q = a^n - 1 \neq 0$, the proof is completed. □

This allows proving the following theorem.

Theorem IV.7. $\mathrm{SL}_2(A)$ *is Ulam stable.*

PROOF. Let $\mu : \mathrm{SL}_2(A) \to \mathrm{U}(n)$ be a ε-:representation into a Hilbert space with finite dimension n. Denote by A' the copy of A in $\mathrm{SL}_2(A)$ consisting of the upper triangular matrices with ones on the diagonal, i.e. in the notation of the previous chapter $A' = \{e_u(a) | a \in A\}$. As A is an abelian group it is amenable and the restriction of μ to A' is 2ε-close to a representation $\pi : A' \to \mathrm{U}(n)$ (Theorem II.5):

$$\|\pi - \mu_{|_{A'}}\| \leq 2\varepsilon$$

Now let $u \in A$ be a unit with infinite order (which exists by Lemma IV.1). Define $U := \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right)$. Note that conjugation of A' by U descends into multiplication by u^2:

$$U^{-1}a'U = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix} = \begin{pmatrix} 1 & u^2a \\ 0 & 1 \end{pmatrix} = (u^2a)'$$

Denote by $\pi^u : A' \to \mathrm{U}(n)$ the representation that is obtained by conjugating the argument of π with U: $\pi^u(a') = \pi(U^{-1}a'U)$. The following computation holds:

$$\begin{aligned} \pi^u(a) = \pi(U^{-1}aU) \sim_{2\varepsilon} \mu(U^{-1}aU) \sim_{2\varepsilon} \mu(U^{-1})\mu(a)\mu(U) \\ \sim_{2\varepsilon} \mu(U^{-1})\pi(a)\mu(U) \sim_{\varepsilon} \mu(U)^{-1}\pi(a)\mu(U) \end{aligned} \tag{3.1}$$

This means that the representation π^u is 7ε-close to a representation conjugate to π. Applying Johnson's Theorem IV.5, which is possible as A is amenable, yields that the two representations π and π^u are conjugate (if $\varepsilon \leq \frac{1}{7}$). Characters of conjugate representations are equal, thus we can deduce that the character of μ is invariant under multiplication with u^2.

By Lemma IV.6, the restriction of π to qA is trivial, where q is of the form $q = (u^2)^n - 1$ for some $n \in \mathbb{N}$. Conclude that the restriction of μ to qA is 2ε-close to the trivial representation:

$$\|\mathbb{1} - \mu|_{qA}\| \leq \|\mathbb{1} - \pi|_{qA}\| + 2\varepsilon = 2\varepsilon$$

As the same argument applies to the lower triangular matrices, it follows that μ maps every elementary matrix with entries in qA, that is every element of $\mathrm{e}_2(qA)$, 2ε-close to the identity. The next computation will show that then any conjugate of an element of $\mathrm{e}_2(I)$ will be mapped 5ε-close to the identity:

$$\begin{aligned} \left\|\mu\left(b(qa)'b^{-1}\right) - \mathbb{1}\right\| \leq & \left\|\mu(b)\underbrace{\mu((qa)')}_{\sim_{2\varepsilon}}\mu(b^{-1}) - \mathbb{1}\right\| + 2\varepsilon \\ \leq & \left\|\mu(b)\mu(b^{-1}) - \mathbb{1}\right\| + 4\varepsilon \\ \leq & 5\varepsilon \end{aligned}$$

This implies that any element of $\mu(\mathrm{e}_2^{\triangleleft}(qA))$ has distance at most 5ε from the identity. Application of the theorem on bounded generation III.39 allows to conclude that the subgroup $\mathrm{E}_2^{\triangleleft}(A;qA)$ generated by the elementary matrices with entries in qA is $r(q,A)\cdot 5\varepsilon$- close to the identity. $r(q,A)$ denotes in this case the maximal number of elementary matrices needed to write an element of $\mathrm{E}_2^{\triangleleft}(qA)$ as a product of elements of $\mathrm{e}_2^{\triangleleft}(qA)$.

As the group $\mathrm{E}_2^{\triangleleft}(qA)$ is of finite index in $\mathrm{SL}_2(A)$ by Lemma IV.2 application of Lemma II.24 proves that μ is $15\varepsilon r(A,q)+5\varepsilon$ close to some representation π'. □

4. Discussion

Two observations are worth mentioning.

The first is that the condition that $\mathrm{E}_2^{\triangleleft}(I)$ is boundedly generated is a real necessity. A counterexample is provided by the group $\mathrm{SL}_2(\mathbb{Z})$. This group contains the free group with two generators as a finite index subgroup, so according to Corollary II.23 it has finite dimensional non-trivial ε-representations.

The second interesting fact is that, as mentioned in Chapter II, the group $\mathrm{SL}_2(A)$ is no example of a strongly Ulam stable group. This follows from Lemma II.17, as this group contains a free subgroup with two generators (but this free group is of course not of finite index).

This means further studies are necessary to identify an example of a non-amenable strongly Ulam stable group. However, in order to find such a group, infinite dimensional ε-representations will have to be considered.

Bibliography

[Bas64] H. Bass, *K-theory and stable algebra*, Publications Mathématiques de l'IHES **22** (1964), no. 1, 5–60.

[Bas68] ———, *Algebraic k-theory*, WA Benjamin New York, 1968.

[BHV08] M.B. Bekka, P.L. Harpe, and A. Valette, *Kazhdan's property (T)*, New mathematical monographs, Cambridge University Press, 2008.

[BMS67] H. Bass, J. Milnor, and J.P. Serre, *Solution of the congruence subgroup problem for $SL_n(n \geq 3)$ and $Sp_{2n}(n \geq 2)$*, Publications mathematiques de l'IHES **33** (1967), no. 1, 59–137.

[BOT10] M. Burger, N. Ozawa, and A. Thom, *On Ulam stability*, to appear in Israel Journal of Mathematics (2010).

[Cal09] D. Calegari, *scl*, World Scientific Pub Co, June 2009.

[CKP92] D. Carter, G. Keller, and E. Paige, *Bounded expressions in SL(n, A)*, preprint (1992).

[EFT07] H.D. Ebbinghaus, J. Flum, and W. Thomas, *Einführung in die mathematische Logik*, 5. ed., Spektrum Akademischer Verlag, September 2007.

[Fuj00] K. Fujiwara, *The second bounded cohomology of an amalgamated free product of groups*, Transaction-American Mathmatical Society **352** (2000), no. 3, 1113–1130.

[Joh86] B.E. Johnson, *Approximately multiplicative functionals*, Journal of the London Mathematical Society **2** (1986), no. 3, 489–510.

[Kaz82] D. Kazhdan, *On ε-representations*, Israel J. Math **43** (1982), no. 4, 315–323.

[Men65] J.L. Mennicke, *Finite factor groups of the unimodular group*, The Annals of Mathematics **81** (1965), no. 1, 31–37.

[Mor07] D. Witte Morris, *Bounded generation of SL(n,A) (after D. Carter, G. Keller and E. Paige)*, New York Journal of Mathematics (2007), 383–421.

[Rol09] Pascal Rolli, *Quasi-morphisms on Free Groups*, arXiv:0911.4234 (2009).

[Ula60] S. M. Ulam, *A collection of mathematical problems*, Interscience Tracts in Pure and Applied Mathematics, vol. 8, Interscience Publishers, New York, NY, USA, 1960.