Master Thesis

# $L^{2}$-Betti numbers and profinite completions of groups 

Nico Stucki

January 23, 2018

First Supervisor: Dr. Holger Kammeyer<br>Second Supervisor: Prof. Dr. Roman Sauer

Institute for Algebra and Geometry
Karlsruhe Institute of Technology

## Contents

1 Introduction ..... 5
$2 \quad L^{2}$-Betti numbers ..... 7
$2.1 \quad L^{2}$-Betti numbers of Hilbert chain complexes ..... 7
2.2 Cellular $L^{2}$-Betti numbers ..... 9
2.3 Classifying spaces and $L^{2}$-Betti numbers of groups ..... 13
3 Profinite completion ..... 15
3.1 Projective limits and its properties ..... 15
3.2 Profinite groups and profinite completion of groups ..... 22
$4 \quad L^{2}$-Betti numbers and profinite invariance ..... 33
4.1 The first $L^{2}$-Betti number is a profinite invariant ..... 33
4.2 The $L^{2}$-Betti numbers in general are no profinite invariant ..... 38

## 1 Introduction

In 1970 Alexander Grothendieck published an article (see Grothendieck, 1970), where he asked if a homomorphism $u: G \longrightarrow H$ between discrete groups needs to be an isomorphism, if its profinite completion $\widehat{u}: \widehat{G} \longrightarrow \widehat{H}$ is an isomorphism. To be more precise, he asked about conditions $G$ and $H$ have to provide in order to conclude that $u$ itself is an isomorphism if $\widehat{u}$ is. A first answer was given by Bridson and Grunewald (see Bridson and Grunewald, 2004), who constructed a group $\Gamma$ as direct product of two residually finite, hyperbolic (i.e. finitely presented) groups and a finitely presented subgroup $P$ of infinite index in $\Gamma$, such that the inclusion $u: P \hookrightarrow \Gamma$ induces an isomorphism $\widehat{u}: \widehat{P} \longrightarrow \widehat{\Gamma}$, but $P$ and $\Gamma$ are not abstractly isomorphic.
This might be a good motivation to ask about (weaker) similiarities between abstract groups $G$ and $H$, which have isomorphic profinite completions $\widehat{G}$ and $\widehat{H}$, so in particular we ask about profinite invariants. That is where Betti numbers and $L^{2}$-Betti numbers come into play. Alan Reid showed in his article (see Reid, 2013) that the first Betti number is a profinite invariant for finitely generated groups and concluded, by using Lück's Approximation Theorem, that the first $L^{2}$-Betti number is a profinite invariant for finitely presented residually finite groups.
Naturally this result arises the question about $L^{2}$-Betti numbers being a profinite invariant in higher dimensions as well, at least for finitely presented residually finite groups. Menny Aka discussed in his paper (see Aka, 2010) a similar question. He showed that Kazhdan's property (T), which was introduced in the mid 60's by D. Kazhdan for locally compact groups in order to show that a large class of lattices is finitely generated, is no profinite invariant. For this purpose he constructed two groups $\Gamma_{0} \leq \operatorname{Spin}(1, n)\left(\mathcal{O}_{K}\right)$ and $\Lambda_{0} \leq \operatorname{Spin}(5, n-4)\left(\mathcal{O}_{K}\right)\left(\mathcal{O}_{K}\right.$ denotes the ring of integers of the number field $K:=\mathbb{Q}(\sqrt{d}), d \in \mathbb{N}$ square free) with isomorphic profinite completions $\widehat{\Gamma_{0}} \cong \widehat{\Lambda_{0}}$ and showed that $\Lambda_{0}$ admits Property $(T)$ while $\Gamma_{0}$ does not. Actually we will use the same groups to show that the $L^{2}$-Betti numbers in every even dimension $\geq 6$ are no profinite invariant.
This work is organized as follows. In Chapter 2 we introduce $L^{2}$-Betti numbers of Hilbert chain complexes, $G$-CW-complexes and groups which are countable, discrete and have a finite type model for $E G$. Chapter 3 provides a review about projective limits and its basic properties in order to introduce the profinite completion of a group. In Chapter 4 we eventually prove the main results of this work. The first part of this chapter deals with the first $L^{2}$-Betti numbers and is a more detailed elaboration of Reid's observation. To be more precise we will show the following ...
1.0.1 Theorem. Let $G$ and $H$ be finitely presented residually finite groups with isomorphic profinite completions $\widehat{G} \cong \widehat{H}$. Then $b_{1}^{(2)}(G)=b_{1}^{(2)}(H)$.

The second part deals with $L^{2}$-Betti numbers in higher dimensions and will make use of the groups constructed by Aka to show...
1.0.2 Theorem. For every natural number $p \geq 6$ there are finitely presented residually finite groups $G_{p}$ and $H_{p}$ with $\widehat{G_{p}} \cong \widehat{H_{p}}$ but $b_{p}^{(2)}\left(G_{p}\right) \neq b_{p}^{(2)}\left(H_{p}\right)$.

## Notation

In this work we rely on the following notation. The category of (topological) groups with (continuous) group homomorphisms as morphisms is denoted by Grp (resp. TGrp) and the category of $G$-spaces with $G$-maps as morphisms by $G T o p$.
 subgroup of $G$ we write $H \leq G$ (resp. $H<G$ ). In order to express that $H$ is additionally of finite index (resp. open) in $G$ we write $H \leq_{f} G$ (resp. $H \leq_{o} G$ ). The direct sum is denoted by $\oplus$, the tensor product by $\otimes$, the product by $\Pi$ (resp. $\times$ ), the coproduct by $\amalg$, and the disjoint union of sets by $\sqcup$.
Of course we use the common notation for the natural numbers $\mathbb{N}$, the rational integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$. Additionally we denote the set of prime numbers by $\mathbb{P} \subset \mathbb{N}$, the $p$-adic integers by $\mathbb{Z}_{p}$ and the unique field with $p^{d}$ elements by $\mathbb{F}_{p^{d}}$ for any $p \in \mathbb{P}$ and $d \in \mathbb{N}$. Furthermore the units of a ring $R$ are denoted by $R^{\times}$.

## 2 L$^{2}$-Betti numbers

The goal of this chapter is the introduction of $L^{2}$-Betti numbers of a countable discrete group $G$ with finite type model for $E G$, where $E G$ denotes the classifying space of $G$. Recall that the $p$-th Betti number $b_{p}(X)$ of a finite CW-complex $X$ is defined by $\operatorname{dim}_{\mathbb{C}}\left(H_{p}(X ; \mathbb{C})\right)$, which is a homotopy invariant of $X$. Now the $L^{2}$-Betti numbers can be seen as a refined version of the ordinary Betti numbers, which take the universal covering $\widetilde{X}$ and the action of the fundamental group $\pi_{1}(X)$ on $\widetilde{X}$ into account.

## 2.1 $L^{2}$-Betti numbers of Hilbert chain complexes

In this section, which is mainly based on Chapter 1.1 of Lück, 2013, we introduce the necessary input about Hilbert modules in order to define the von Neumann dimension of a Hilbert module $V$ as the von Neumann trace of the identity $\mathrm{id}_{V}$. This allows us to define the $p$-th $L^{2}$-Betti number of a Hilbert chain complex $C_{*}$ as the von Neumann dimension of the reduced $p$-th $L^{2}$-Homology of $C_{*}$.

We assume in this section that $G$ is a countable discrete group.

### 2.1.1 Definition. (Hilbert module)

a) A Hilbert $\mathcal{N}(G)$-module is a Hilbert space $V$ with a linear isometric $G$-action, such that there is a Hilbert space $H$ together with an isometric linear $G$-embedding of $V$ into the tensor product of Hilbert spaces $H \otimes l^{2}(G)$ whose $G$-action is defined by

$$
g_{0} \cdot\left(h \otimes \sum_{g \in G} c_{g} g\right):=h \otimes \sum_{g \in G} c_{g} g_{0} g
$$

b) Let $V, W$ be Hilbert $\mathcal{N}(G)$-modules. A bounded $G$-equivariant operator $f: V \longrightarrow W$ is called map of Hilbert $\mathcal{N}(G)$-modules.
c) A Hilbert $\mathcal{N}(G)$-module V is said to be finitely generated, if there is some $n \in \mathbb{N}_{0}$ and a surjective map $\bigoplus_{i=1}^{n} l^{2}(G) \longrightarrow V$ of Hilbert $\mathcal{N}(G)$-modules.

### 2.1.2 Definition. (von Neumann trace)

Let $V$ be a Hilbert $\mathcal{N}(G)$-module and $f: V \longrightarrow V$ a positive (i.e. $\langle f(v), v\rangle \geq 0$ ) endomorphism. By Definition 2.1.1 we can choose a Hilbert space $H$ with isometric linear $G$-embedding $V \hookrightarrow H \otimes l^{2}(G)$, a $G$-equivariant projection $p: H \otimes l^{2}(G) \longrightarrow H \otimes l^{2}(G)$ and an isometric $G$-isomorphism $u: \operatorname{Im}(p) \xrightarrow{\sim} V$. We define the positive operator $\bar{f}: H \otimes l^{2}(G) \longrightarrow H \otimes l^{2}(G)$ by the composition

$$
\bar{f}: H \otimes l^{2}(G) \xrightarrow{p} \operatorname{Im}(p) \xrightarrow{u} V \xrightarrow{f} V \xrightarrow{u^{-1}} \operatorname{Im}(p) \hookrightarrow H \otimes l^{2}(G) .
$$

Now let $\left\{b_{i}\right\}_{i \in I}$ be a Hilbert basis of $H$. Then the von Neumann trace of $f$ is given by

$$
\operatorname{tr}_{\mathcal{N}(G)}(f):=\sum_{i \in I}\left\langle\bar{f}\left(b_{i} \otimes 1\right), b_{i} \otimes 1\right\rangle \quad \in[0, \infty]
$$

where $1 \in l^{2}(G)$ is the unit element. Note that this definition is independent of the choice of $H,\left\{b_{i}\right\}_{i \in I}, p$ and $u$ (c.f. Lück, 2013).

### 2.1.3 Definition. (von Neumann dimension)

Let $V$ be a Hilbert- $\mathcal{N}(G)$-module. The von Neumann dimension of $V$ is defined by

$$
\operatorname{dim}_{\mathcal{N}(G)}(V):=\operatorname{tr}_{\mathcal{N}(G)}\left(\operatorname{id}_{V}\right) \quad \in[0, \infty] .
$$

### 2.1.4 Definition. (Hilbert chain complex)

A Hilbert $\mathcal{N}(G)$-chain complex $C_{*}$ is a sequence of maps of Hilbert $\mathcal{N}(G)$-modules

$$
\cdots \xrightarrow{c_{p+2}} C_{p+1} \xrightarrow{c_{p+1}} C_{p} \xrightarrow{c_{p}} C_{p-1} \xrightarrow{c_{p-1}} \cdots
$$

such that $c_{n} \circ c_{n+1}=0$ for every $n \in \mathbb{Z} . C_{*}$ is said to be positive if $C_{n}=0$ for $n<0$.

### 2.1.5 Definition. ( $L^{2}$-homology and $L^{2}$-Betti numbers)

If $C_{*}$ is a Hilbert $\mathcal{N}(G)$-chain complex, we define the (reduced) p-th $L^{2}$-homology of $C_{*}$ by

$$
H_{p}^{(2)}\left(C_{*}\right):=\operatorname{ker}\left(c_{p}\right) / \overline{\operatorname{Im}\left(c_{p+1}\right)}
$$

and the p-th $L^{2}$-Betti number of $C_{*}$ by

$$
b_{p}^{(2)}\left(C_{*}\right):=\operatorname{dim}_{\mathcal{N}(G)}\left(H_{p}^{(2)}\left(C_{*}\right)\right) .
$$

Note that we divide by the closure of the image in order to ensure that $H_{p}^{(2)}\left(C_{*}\right)$ is a Hilbert space and inherits the $G$-action from $C_{p}$.

### 2.2 Cellular $\mathrm{L}^{2}$-Betti numbers

Now we want to define $L^{2}$-Betti numbers for a free $G$-CW-complex $X$ of finite type. A special case of a $G$-CW-complex is a regular covering of an ordinary CW-complex. In order to apply Section 1, we need to assign a suitable Hilbert chain complex to a given $G$-CW-complex $X$. This section is mainly based on Chapter 1.1, 1.2 in ibid. and Chapter 2 in Kammeyer, 2015.

Let us assume again that $G$ is a countable discrete group in this section.

### 2.2.1 Definition. (G-CW-complex)

A $G$-CW-complex is a $G$-space $X$ together with a $G$-invariant filtration

$$
\emptyset=X_{-1} \subseteq X_{0} \subseteq X_{1} \subseteq \ldots \subseteq X_{n} \subseteq \ldots \subseteq \bigcup_{n \geq 0} X_{n}=X
$$

such that

- $X$ carries the colimit topology with respect to this filtration.
- for each $n \geq 0$ there is a pushout

in $\underline{G T o p}$ with stabiliser subgroups $H_{i}$ in $G$ for every $i$ in the index set $I_{n}$.
The space $X_{n}$ is called the $n$-skeleton of $X$. An equivariant open $n$-dimensional cell is a $G$-component of $X_{n} \backslash X_{n-1}$, i.e. the preimage of a path component of $G \backslash\left(X_{n} \backslash X_{n-1}\right)$. Its closure is an equivariant closed $n$-dimensional cell.
2.2.2 Definition. A $G$-CW-complex $X$ is called
- finite, if it has finitely many equivariant cells.
- of finite type, if it has finitely many equivariant $n$-dimensional cells for every $n \geq 0$.
- proper, if all stabiliser groups $H_{i}$ are finite.
- free, if all stabiliser groups $H_{i}$ are trivial.
2.2.3 Proposition. If $X$ is a $G$-CW-complex, the cellular chain complex $\left(C_{*}^{C W}(X), d_{*}^{C W}\right)$ is canonically a chain complex of left $\mathbb{Z}[G]$-modules.

Proof. For every $g \in G$ the multiplication from left with $g$ induces a homeomoprhism

$$
m_{g}:\left(X_{n}, X_{n-1}\right) \xrightarrow{\sim}\left(X_{n}, X_{n-1}\right)
$$

and hence an automorphism

$$
H_{n}\left(m_{g}\right): C_{n}^{C W}(X) \xrightarrow{\sim} C_{n}^{C W}(X) .
$$

Furthermore we have

$$
H_{n}\left(m_{g}\right) \circ H_{n}\left(m_{h}\right)=H_{n}\left(m_{g} \circ m_{h}\right)=H_{n}\left(m_{g h}\right)
$$

for $g, h \in G$ and $H_{n}\left(m_{1}\right)=\operatorname{id}_{C_{n}^{C W}(X)}$, if $1 \in G$ is the neutral element. So $G$ acts on $C_{n}^{C W}(X)$ for every $n \geq 0$ and we found a $\mathbb{Z}[G]$-module structure. Since $d_{n}^{C W}$ is the boundary map in the triple sequence of ( $X_{n}, X_{n-1}, X_{n-2}$ ), we see by naturality of the boundary map that

commutes and hence that $d_{n}^{C W}$ is $\mathbb{Z}[G]$-linear for every $n \geq 0$.
2.2.4 Remark. In the following we consider $l^{2}(G)$ as $\mathbb{C}[G]-\mathbb{Z}[G]$-bimodule by

$$
g_{0} \cdot\left(\sum_{g \in G} c_{g} g\right):=\sum_{g \in G} c_{g}\left(g_{0} g\right)
$$

and

$$
\left(\sum_{g \in G} c_{g} g\right) \cdot g_{0}:=\sum_{g \in G} c_{g}\left(g g_{0}\right) .
$$

### 2.2.5 Definition. (cellular $L^{2}$-chain complex)

If $X$ is a proper $G$-CW-complex of finite type, then the cellular $L^{2}$-chain complex of $X$ is defined as

$$
C_{*}^{(2)}(X)=l^{2}(G) \otimes_{\mathbb{Z}[G]} C_{*}^{C W}(X)
$$

with differentials $d_{*}^{(2)}=\operatorname{id}_{l^{2}(G)} \otimes d_{*}^{C W}$.
2.2.6 Theorem. The cellular $L^{2}$-chain complex of a free $G$-CW-complex of finite type is a chain complex of Hilbert $\mathcal{N}(G)$-modules.

Proof. Let us fix pushouts

whose existence is required by Definition 2.2.1. Since $i_{n}$ is an embedding as a closed neighborhood deformation retract, we can use the Mayer-Vietoris theorem for pushouts and obtain

$$
\begin{aligned}
C_{n}^{C W}(X)=H_{n}\left(X_{n}, X_{n-1}\right) & \cong H_{n}\left(\coprod_{i \in I_{n}} G \times D^{n}, \coprod_{i \in I_{n}} G \times S^{n-1}\right) \\
& \cong \bigoplus_{i \in I_{n}} H_{n}\left(G \times D^{n}, G \times S^{n-1}\right) \\
& \cong \bigoplus_{i \in I_{n}} H_{n}\left(\coprod_{g \in G} D^{n}, \coprod_{g \in G} S^{n-1}\right) \\
& \cong \bigoplus_{i \in I_{n}} \bigoplus_{g \in G} H_{n}\left(D^{n}, S^{n-1}\right) \\
& \cong \bigoplus_{i \in I_{n}} \bigoplus_{g \in G} \mathbb{Z} \\
& \cong \bigoplus_{i \in I_{n}} \mathbb{Z}[G]
\end{aligned}
$$

for every $n \geq 0$, where " $\cong$ " means isomorphic as $\mathbb{Z}[G]$-modules. So the $n$-th cellular $L^{2}$-chain module is given by

$$
\begin{aligned}
C_{n}^{(2)}(X)=l^{2}(G) \otimes_{\mathbb{Z}[G]} C_{n}^{C W}(X) & \cong l^{2}(G) \otimes_{\mathbb{Z}[G]}\left(\bigoplus_{i \in I_{n}} \mathbb{Z}[G]\right) \\
& \cong\left(\bigoplus_{i \in I_{n}} l^{2}(G) \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]\right) \\
& \cong \bigoplus_{i \in I_{n}} l^{2}(G) .
\end{aligned}
$$

Hence we can pull back the inner product and the linear isometric $G$-action of $\bigoplus_{i \in I_{n}} \mathbb{Z}[G]$, which turns $C_{n}^{(2)}(X)$ into a Hilbert $\mathcal{N}(G)$-module. If we choose a different $G$-pushout, we obtain another $\mathbb{Z}[G]$-isomorphism, but the two differ only by the composition of an automorphism which becomes a $G$-equivariant unitary after applying the $L^{2}$-completion $l^{2}(G) \otimes_{\mathbb{Z}[G]}(\cdot)$. Furthermore the differentials $d_{n}^{(2)}=\operatorname{id}_{l^{2}(G)} \otimes d_{n}^{C W}$ are maps of Hilbert $\mathcal{N}(G)$-modules, which is shown in Proposition 2.19 of Kammeyer, 2015.
$2 L^{2}$-Betti numbers

### 2.2.7 Definition. ( $L^{2}$-homology and $L^{2}$-Betti numbers)

Let $X$ be a free $G$-CW-complex of finite type with cellular $L^{2}$-chain complex $\left(C_{*}^{(2)}(X), d_{*}^{(2)}\right)$.
a) The $p$-th (reduced) $L^{2}$-homology of $X$ is the Hilbert $\mathcal{N}(G)$-module

$$
H_{p}^{(2)}(X):=\operatorname{ker}\left(d_{p}^{(2)}\right) / \overline{\operatorname{Im}\left(d_{p+1}^{(2)}\right)}
$$

b) The $p$-th $L^{2}$-Betti number of $X$ is

$$
b_{p}^{(2)}(X):=\operatorname{dim}_{\mathcal{N}(G)} H_{p}^{(2)}(X) .
$$

### 2.3 Classifying spaces and $\mathrm{L}^{2}$-Betti numbers of groups

In this section we assign a classifying space $E G$ to a given countable and discrete group $G$, which can be seen as universal free $G$-CW-complex in some sense. So if $E G$ turns out to have a model of finite type, we can define the $L^{2}$-Betti numbers of $G$ as the $L^{2}$-Betti numbers of $E G$. This section is mainly based on Chapter 2.3 in Kammeyer, 2015.

We assume again, unless otherwise stated, that $G$ is a countable discrete group in this section.

### 2.3.1 Definition. (weakly contractible)

A space $X$ is called weakly contractible, if every map $f: S^{n-1} \longrightarrow X$ extends to a map $\bar{f}: D^{n} \longrightarrow X$ for all $n \in \mathbb{N}$.

### 2.3.2 Proposition. For a free $G$ - $C W$-complex $E$ the following are equivalent:

i) For every free $G$-CW-complex $X$ there exists a unique continuous map $X \longrightarrow E$ up to $G$-homotopy.
ii) $E$ is weakly contractible.

This statement is proven in Chapter 2.3 of ibid.

### 2.3.3 Definition. (classifying space)

A free $G$-CW-complex $E$ which satisfies i) or ii) in Proposition 2.3 .2 is called a model for $E G$ and the quotient space $B G:=G \backslash E G$ is called the classifying space of $G$.
2.3.4 Proposition. There is a model for $E G$ of $G$ and any two of them are $G$-homotopy equivalent.

A proof of this statement is given in Chapter 2.3 of ibid.
Finally we are able to define the $L^{2}$-Betti numbers for a countable discrete group with finite type model for $E G$.

### 2.3.5 Definition. ( $L^{2}$-Betti numbers)

Let $G$ have a finite type model for $E G$. Then we define the $p$-th $L^{2}$-Betti number of $G$ by

$$
b_{p}^{(2)}(G):=b_{p}^{(2)}(E G)
$$

for every $p \in \mathbb{N}_{0}$.
Let us recall for a moment the definition of ordinary Betti numbers of a group $G$.

### 2.3.6 Definition. (Betti numbers)

The $i$-th Betti number of a group $G$ is the $i$-th Betti number of its classifying space $B G$, so

$$
b_{i}(G):=b_{i}(B G)=\operatorname{dim}_{\mathbb{Q}}\left(H_{i}(B G ; \mathbb{Q})\right) .
$$

for every $i \in \mathbb{N}_{0}$.

The following theorem will be key in Chapter 4.1, where we want to prove that the first $L^{2}$-Betti numbers are a profinite invariant. It goes back to Wolfgang Lück, who showed that for finitely presented, residually finite groups, the $L^{2}$-Betti numbers are in fact an asymptotic invariant of towers of finite index subgroups.

### 2.3.7 Theorem. (Lück's Approximation Theorem)

Let $G$ be a finitely presented group with classifying space EG and

$$
G=G_{1}>G_{2}>\ldots>G_{m}>\ldots
$$

a sequence of finite index subgroups, which are normal in $G$ and satisfy $\bigcap_{m=1}^{\infty} G_{m}=1$. If $E G$ has a finite $(p+1)$-skeleton, then

$$
b_{p}^{(2)}(G)=\lim _{m \rightarrow \infty} \frac{b_{p}\left(G_{m}\right)}{\left[G: G_{m}\right]}
$$

for every $p \in \mathbb{N}_{0}$.
A proof of this theorem can be found in Lück, 1994.
Another result we need is the following Lemma, which helps us to find the nonvanishing $L^{2}$-Betti numbers of a lattice in a connected semisimple Lie group. It can be found in Kammeyer, 2014.
2.3.8 Lemma. Let $G$ be a connected semisimple Lie group, $K \leq G$ a maximal compact subgroup and $\Gamma \subseteq G$ any lattice. Then $b_{p}^{(2)}(\Gamma) \neq 0$ if and only if $\delta(G)=0$ and $\operatorname{dim}(G / K)=2 p$, where $\delta(G):=\operatorname{rank}_{\mathbb{C}}(G)-\operatorname{rank}_{\mathbb{C}}(K)$ denotes the deficiency of $G$.

## 3 Profinite completion

In this chapter we want to clarify the term 'profinite invariant'. For that purpose we need to describe the profinite completion, which gives a way to encode all finite quotients of a group. Furthermore we want to elaborate some basic properties about profinite groups and profinite completions for later purposes. Note that this chapter is based on Chapter 1 and 2 of Ribes, 2010.

### 3.1 Projective limits and its properties

Let us recall the definition and basic properties of projective limits. Although most of the time we will be dealing with topological groups, we will study projective limits in a more general category: the category of topological spaces. Replacing the word space by group (resp. ring), map by homomorphism of groups (resp. homomorphism of rings) and homeomorphism by isomorphism of topological groups (resp. isomorphism of topological rings), one obtains the corresponding definitions and statements for topological groups (resp. topological rings).

### 3.1.1 Definition. (Projective system and projective limit)

a) We call a partially ordered set $I$ directed if for any two elements $i, j \in I$ there is some $k \in I$ with $k \geq i$ and $k \geq j$.
b) A projective system of topological spaces is a tripel $\left(X_{i}, \varphi_{i j}, I\right)$ consisting of a partially ordered set $I$, a family of topological spaces $\left\{X_{i}\right\}_{i \in I}$ and a family of continuous maps $\varphi_{i j}: X_{i} \longrightarrow X_{j}$ whenever $i \geq j$, such that:

- $\varphi_{i i}=\operatorname{id}_{X_{i}}$ for every $i \in I$,
$-\varphi_{j k} \circ \varphi_{i j}=\varphi_{i k}$ whenever $i \geq j \geq k$.
c) A projective limit $\left(X, \Phi_{i}\right)$ of a projective system $\left(X_{i}, \varphi_{i j}, I\right)$ of topological spaces is a topological space $X$ with compatible continuous maps $\Phi_{i}: X \longrightarrow X_{i}$ for all $i \in I$, where compatible means $\varphi_{i j} \circ \Phi_{i}=\Phi_{j}$ for $i \geq j$, satisfying the following universal property:
For any topological space $Y$ and family of compatible continuous maps $\Psi_{i}: Y \longrightarrow X_{i}$ $(i \in I)$ there is a unique continuous map $\Psi: Y \longrightarrow X$ such that $\Phi_{i} \circ \Psi=\Psi_{i}$ for every $i \in I$.



## 3 Profinite completion

The maps $\Phi_{i}$ are called projections, although they are not necessarily surjective.
3.1.2 Proposition. If $\left(X_{i}, \varphi_{i j}, I\right)$ is a projective system of topological spaces, then
a) there exists a projective limit of $\left(X_{i}, \varphi_{i j}, I\right)$.
b) the projective limit of $\left(X_{i}, \varphi_{i j}, I\right)$ is unique up to a natural homeomorphism and we denote it by $\lim _{i \in I} X_{i}$ or just ${\underset{\mathrm{lim}}{\leftrightarrows}}^{\rightleftarrows} X_{i}$.

Proof. a) Consider

$$
X:=\left\{\left(x_{i}\right) \in \prod_{i \in I} X_{i} \mid \forall i \geq j: \varphi_{i j}\left(x_{i}\right)=x_{j}\right\}
$$

equipped with the subspace topology of the product topology. Then $X$ is a topological space and the restriction of the canonical projections $\prod_{i \in I} X_{i} \longrightarrow X_{j}$ to $X$ yield a continuous map $\Phi_{i}: X \longrightarrow X_{j}$ for every $j \in I$, which are compatible by definition of $X$. The universal property for $X$ is now a direct consequence of the universal property for the direct product and the fact that we consider families of compatible maps.
b) If $\left(X, \Phi_{i}\right)$ and $\left(Y, \Psi_{i}\right)$ are both projective limits of $\left(X_{i}, \varphi_{i j}, I\right)$, then the universal property gives us continuous maps $\Phi: X \longrightarrow Y$ and $\Psi: Y \longrightarrow X$ such that

$$
\Psi_{i} \circ \Phi=\Phi_{i} \text { and } \Phi_{i} \circ \Psi=\Psi_{i}
$$

for all $i \in I$. But then

$$
\Phi_{i} \circ(\Psi \circ \Phi)=\Phi_{i} \text { and } \Psi_{i} \circ(\Phi \circ \Psi)=\Psi_{i}
$$

for all $i \in I$. So by uniqueness of continuous maps with this property we conclude $\Psi \circ \Phi=\mathrm{id}_{X}$ and $\Phi \circ \Psi=\mathrm{id}_{Y}$.
3.1.3 Proposition. If $\left(X_{i}, \varphi_{i j}, I\right)$ is a projective system of totally disconnected compact Hausdorff spaces, then $\lim _{\leftrightarrows} X_{i}$ is a totally disconnected compact Hausdorff space.

Proof. First note that $\prod_{i \in I} X_{i}$ is compact by Tychonoff's theorem and recall the description of $\lim _{\leftrightarrows} X_{i}$ as

$$
\left\{\left(x_{i}\right) \in \prod_{i \in I} X_{i} \mid \forall i \geq j: \varphi_{i j}\left(x_{i}\right)=x_{j}\right\} .
$$

If $p_{j}: \prod_{i \in I} X_{i} \longrightarrow X_{j}$ is the projection for $j \in I$ we see that

$$
\lim _{\leftrightarrows} X_{i}=\bigcap_{i \geq j} E\left(\varphi_{i j} \circ p_{i}, p_{j}\right),
$$

where $E(-,-)$ denotes the equaliser of two maps. Since the equaliser of two continuous maps into a Hausdorff space is closed, we can conclude that $\lim _{\leftarrow} X_{i}$ is a closed subset
of the compact space $\prod_{i \in I} X_{i}$ and hence compact. The rest of the statement should be clear, since products of totally disconnected (resp. Hausdorff) spaces are totally disconnected (resp. Hausdorff) and subspaces of totally disconnected (resp. Hausdorff) spaces are totally disconnected (resp. Hausdorff) as well.
3.1.4 Proposition. If $\left(X_{i}, \varphi_{i j}, I\right)$ is a projective system of nonempty compact Hausdorff spaces, then $\varliminf_{\rightleftarrows} X_{i}$ is nonempty.

Proof. For $j \in I$ let us define

$$
Y_{j}:=\left\{\left(x_{i}\right) \in \prod_{i \in I} X_{i} \mid \forall k \leq j: \varphi_{j k}\left(x_{j}\right)=x_{k}\right\}
$$

and observe that

$$
\lim _{\leftrightarrows} X_{i}=\bigcap_{j \in I} Y_{j} .
$$

Since $\prod_{i \in I} X_{i}$ is compact by Tychonoff's theorem, it suffices to show that $\left\{Y_{j}\right\}_{j \in I}$ is a family of closed subsets which has the finite intersection property. First of all let us convince ourselves that $Y_{j}$ is nonempty for all $j \in I$. The axiom of choice guarantees the existence of $x_{j} \in X_{j}$ and $x_{i} \in X_{i}$ for $i \not \leq j$. Hence, we find $\left(y_{i}\right)$ as an element of $Y_{j}$, where

$$
y_{i}:= \begin{cases}x_{j} & \text { if } i=j, \\ x_{i} & \text { if } i \not \leq j, \\ \varphi_{j i}\left(x_{j}\right) & \text { if } i \leq j\end{cases}
$$

Furthermore each $Y_{j}$ is a closed subspace of $\prod_{i \in I} X_{i}$. To see this, let $\left(x_{i}\right) \in\left(\prod_{i \in I} X_{i}\right) \backslash Y_{j}$. Then there exists $k \leq j$ with $\varphi_{j k}\left(x_{j}\right) \neq x_{k}$. Since $X_{k}$ is Hausdorff, we can find disjoint open neighborhoods $U$ of $\varphi_{j k}\left(x_{j}\right)$ and $V$ of $x_{k}$ in $X_{k}$. So $W:=\prod_{i \in I} W_{i}$ is an open neighborhood of $\left(x_{i}\right)$ in $\prod_{i \in I} X_{i}$, where

$$
W_{i}:= \begin{cases}V & \text { if } i=k \\ \varphi_{j k}^{-1}(U) & \text { if } i=j, \\ X_{i} & \text { if } i \neq j, k\end{cases}
$$

But $W \cap Y_{j}=\emptyset$, since for $\left(y_{i}\right) \in W$ we have

$$
U \ni \varphi_{j k}\left(y_{j}\right) \neq y_{k} \in V
$$

by disjointness of $U$ and $V$. Now let $J \subset I$ determine an arbitrary finite subcollection $\left\{Y_{j}\right\}_{j \in J}$. Since $I$ is directed, we can find inductively some $l \in I$ with $j \leq l$ for all $j \in J$. Note that if $j \leq j^{\prime}$, the relation $\varphi_{j k} \circ \varphi_{j^{\prime} j}=\varphi_{j^{\prime} k}$ for $k \leq j$ implies $Y_{j^{\prime}} \subseteq Y_{j}$. Hence we obtain

$$
\emptyset \neq Y_{l} \subseteq \bigcap_{j \in J} Y_{j}
$$

and this finally shows the claim.
3.1.5 Remark. a) In fact $\varliminf_{\leftrightarrows}$ is a functor from the category of projective systems of topological spaces over a fixed directed set $I$ to the category of topological spaces. A morphim $\Theta:\left(X_{i}, \varphi_{i j}, I\right) \longrightarrow\left(Y_{i}, \psi_{i j}, I\right)$ in the category of projective systems is a family of continuous maps $\Theta_{i}: X_{i} \longrightarrow Y_{i}$, we call them components of $\Theta$, which satisfy $\psi_{i j} \circ \Theta_{i}=\Theta_{j} \circ \varphi_{i j}$ whenever $i \geq j$. If $\left(X, \Phi_{i}\right)=\lim _{\leftrightarrows} X_{i}$ and $\left(Y, \Psi_{i}\right)=\lim _{i} Y_{i}$ denote the projective limits, we obtain compatible continuous maps $\Theta_{i} \circ \Phi_{i}: X \longrightarrow Y_{i}$ which induce a continuous map

$$
\lim _{\underset{c}{ } \in I} \Theta_{i}=\lim \Theta: \lim _{\leftrightarrows}^{\leftrightarrows} X_{i} \longrightarrow \lim _{\leftrightarrows} Y_{i}
$$

by universal property of $\lim _{\rightleftarrows} Y_{i}$. Explicitly, $\lim _{\rightleftarrows} \Theta$ is given by $\varliminf_{\rightleftarrows} \Theta\left(\left(x_{i}\right)\right)=\left(\Theta_{i}\left(x_{i}\right)\right)$.

b) If $\Theta:\left(X_{i}, \varphi_{i j}, I\right) \longrightarrow\left(Y_{i}, \psi_{i j}, I\right)$ is a map of projective systems with embeddings $\Theta_{i}: X_{i} \hookrightarrow Y_{i}$, then $\varliminf_{\rightleftarrows} \Theta: \lim _{i} \longrightarrow X_{i} Y_{i}$ is an embedding as well. Continuity is given by construction and injectivity is obvious by its explicit description. So we have to see that $\lim \Theta$ sends open sets to open sets in $\operatorname{Im}(\lim \Theta)$. By definition of $\varliminf_{\rightleftarrows} X_{i}$ as subspace of $\prod_{i \in I} X_{i}$ a basis of $\lim _{\rightleftarrows} X_{i}$ is given by open sets like

$$
\lim _{幺} X_{i} \cap\left[\prod_{i \in S} U_{i} \times \prod_{j \in S^{c}} X_{j}\right]
$$

for any finite subset $S$ of $I$ and open subsets $U_{i}$ of $X_{i}(i \in S)$. So the equality

$$
\lim _{\hookleftarrow} \Theta\left(\lim _{\leftarrow} X_{i} \cap\left[\prod_{i \in S} U_{i} \times \prod_{j \in S^{c}} X_{j}\right]\right)=\operatorname{Im}\left(\varliminf_{\leftarrow} \Theta\right) \cap\left(\prod_{i \in S} \Theta_{i}\left(U_{i}\right) \times \prod_{j \in S^{c}} Y_{j}\right)
$$

implies the claim.
3.1.6 Lemma. Let $\Theta:\left(X_{i}, \varphi_{i j}, I\right) \longrightarrow\left(Y_{i}, \psi_{i j}, I\right)$ be a map of projective systems of compact Hausdorff spaces with surjective components $\Theta_{i}: X_{i} \longrightarrow Y_{i}$. Then

$$
\lim _{\leftrightarrows} \Theta: \lim _{\check{m}} X_{i} \longrightarrow \underset{\rightleftarrows}{\lim } Y_{i}
$$

is surjective.

Proof. Let $\left(y_{i}\right) \in \underset{\leftarrow}{\lim } Y_{i}$. Surjectivity of $\Theta_{i}$ tells us that $\widetilde{X}_{i}:=\Theta_{i}^{-1}\left(y_{i}\right)$ is a nonempty subspace of $X_{i}$ for every $i \in I$. Since $Y_{i}$ is Hausdorff, any point in $Y_{i}$ is closed. Therefore $\widetilde{X}_{i}$ is compact as closed subset of a compact space. In fact we found a projective system $\left(\widetilde{X}_{i},\left.\varphi_{i j}\right|_{\widetilde{X}_{i}}, I\right)$ of nonempty compact Hausdorff spaces, since $\varphi_{i j}\left(\widetilde{X}_{i}\right) \subseteq \widetilde{X}_{j}$. So Remark 3.1.5 b) allows us to identify $\lim \widetilde{X}_{i}$ with its image in $\lim _{\leftrightarrows} X_{i}$ under the embedding induced by the inclusions $\widetilde{X}_{i} \hookrightarrow X_{i}$ and Proposition 3.1.4 tells us that $\varliminf_{\leftrightarrows} \widetilde{X}_{i}$ is nonempty. Hence there is some $\left(x_{i}\right) \in \lim _{\rightleftarrows} \widetilde{X}_{i} \subseteq \lim _{\leftarrow} X_{i}$ with

$$
\lim _{\rightleftharpoons} \Theta\left(\left(x_{i}\right)\right) \stackrel{(3.1 .5 \mathrm{x})}{=}\left(\Theta_{i}\left(x_{i}\right)\right)=\left(y_{i}\right) .
$$

3.1.7 Corollary. Let $\left(X_{i}, \varphi_{i j}, I\right)$ be a projective system of compact Hausdorff spaces and $Y$ a compact Hausdorff space. If $\psi_{i}: Y \longrightarrow X_{i}$ are compatible continuous surjections $(i \in I)$, then the induced map $\Psi: Y \longrightarrow \not \varliminf_{\rightleftarrows} X_{i}$ is surjective.

Proof. We can consider the maps $\psi_{i}$ as components of a map $\psi:\left(Y, \mathrm{id}_{Y}, I\right) \longrightarrow\left(X_{i}, \varphi_{i j}, I\right)$ of projective systems. Then it is easy to verify that $\underset{\leftarrow}{\lim } \psi=\Psi$ and Lemma 3.1.6 gives the claim.
3.1.8 Lemma. Let $\left(X_{i}, \varphi_{i j}, I\right)$ be a projective system of topological spaces such that $\varliminf_{亡} X_{i} \neq \emptyset$ and $\Psi_{i}: Y \longrightarrow X_{i}$ a family of compatible continuous surjections from a topological space $Y(i \in I)$. Then the image of the induced map $\Psi: Y \longrightarrow \not \varliminf_{\longleftarrow} X_{i}$ is a dense subspace of $\varliminf_{\leftrightarrows} X_{i}$.

Proof. Consider a basic open subset

$$
V=\varliminf_{\leftarrow} X_{i} \cap\left(\prod_{i \in S} V_{i} \times \prod_{j \in S^{c}} X_{j}\right)
$$

of $\varliminf_{\longleftarrow} X_{i}$, where $S$ is any finite subset of $I$ and $V_{i}$ is an open subset of $X_{i}$ for every $i \in S$. Since $I$ is directed and $S$ is finite there is some $k \in I$ with $k \geq i$ for every $i \in S$. Now let $\left(x_{i}\right)$ some arbitrary element in $V$. By surjectivity of $\Psi_{k}$ we can find some $y \in Y$ with $\Psi_{k}(y)=x_{k}$. But then $\Psi(y)$ is in $V$ since for $i \in S$ we have

$$
\Psi(y)_{i}=\Psi_{i}(y)=\varphi_{k i} \circ \Psi_{k}(y)=\varphi_{k i}\left(x_{k}\right)=x_{i} \in V_{i} .
$$

Hence we showed that $\operatorname{Im}(f) \cap V \neq \emptyset$ and since $V$ was an arbitrary basic open set in $\lim _{\rightleftarrows} X_{i}$ the claim follows.
3.1.9 Lemma. Let $\left(X_{i}, \varphi_{i j}, I\right)$ be a projective system of compact Hausdorff spaces, $X:=\varliminf_{\longleftarrow} X_{i}$ and $\Phi_{i}: X \longrightarrow X_{i}$ the projections.
a) If $Y \subseteq X$ closed, then $Y=\lim _{\leftrightarrows} \Phi_{i}(Y)$.

## 3 Profinite completion

b) If $Y \subseteq X$, then $\bar{Y}=\varliminf_{\lessdot} \Phi_{i}(Y)$.

Proof. The inclusions $\iota_{i}: \Phi_{i}(Y) \hookrightarrow X_{i}$ for $i \in I$ are the components of a map

$$
\iota:\left(\Phi_{i}(Y),\left.\varphi_{i j}\right|_{\Phi_{i}(Y)}, I\right) \longrightarrow\left(X_{i}, \varphi_{i j}, I\right)
$$

of projective systems. Remark 3.1 .5 b ) tells us that $\lim \iota: \lim _{\rightleftharpoons} \Phi_{i}(Y) \longrightarrow X$ is an embedding, which allows us to identify $\lim \Phi_{i}(Y)$ with its image in $X$. Moreover, restricting the projections $\Phi_{i}$ to $Y$ yields a family of compatible continuous maps $\left.\Phi_{i}\right|_{Y}: Y \longrightarrow \Phi_{i}(Y)$, which induce a continuous map $f: Y \longrightarrow \underset{\rightleftarrows}{\rightleftarrows} \Phi_{i}(Y)$. It is injective since

$$
f\left(\left(x_{j}\right)\right)=\left(\Phi_{i}\left(\left(x_{j}\right)\right)=\left(x_{i}\right) .\right.
$$

and it is easy to check that

$$
f\left(Y \cap\left[\prod_{i \in S} U_{i} \times \prod_{j \in S^{c}} X_{j}\right]\right)=\operatorname{Im}(f) \cap\left(\prod_{i \in S}\left[\Phi_{i}(Y) \cap U_{i}\right] \times \prod_{j \in S^{c}} \Phi_{j}(Y)\right)
$$

for any finite subset $S$ of $I$ and open subsets $U_{i}$ of $X_{i}(i \in S)$. So we found another embedding $f: Y \hookrightarrow \varliminf_{亡} \Phi_{i}(Y)$. Observe that the composition of these embeddings is the natural inclusion of $Y$ into $X$ which means that $Y$ is a subspace of $\varliminf_{¿} \Phi_{i}(Y)$ under this identification.
a) Note that $Y$ is compact as closed subset of the compact space $X$. So $\Phi_{i}(Y)$ is compact for every $i \in I$ as image of a compact space under a continuous map. On top of that $Y$ and $\Phi_{i}(Y)$ are Hausdorff spaces for every $i \in I$ as subspaces of the Hausdorff spaces $X$ and $X_{i}$. Using Corollary 3.1.7 we see that $f$ is surjective and we conclude $Y=\lim _{\ddagger} \Phi_{i}(Y)$.
b) First of all note that the case $Y=\emptyset$ is trivial. In order to see that $\bar{Y} \subseteq \lim _{\leftrightarrows} \Phi_{i}(Y)$ we show that $\underset{\lim }{\leftrightarrows} \Phi_{i}(Y)$ is a closed subset of $X$. Let $\left(x_{i}\right) \in X \backslash \lim \Phi_{i}(Y)$, which means that there is some $k \in I$ such that $x_{k} \notin \Phi_{k}(Y)$. Since $X_{k}$ is Hausdorff, there are disjoint open neighborhoods $U$ of $x_{k}$ and $V$ of $\Phi_{k}(Y)$. Then

$$
\left(U \times \prod_{j \neq k} X_{j}\right) \cap X
$$

is an open neighborhood of $\left(x_{i}\right)$ in $X$ which does not intersect $\lim _{\leftrightarrows} \Phi_{i}(Y)$. By assumption $\emptyset \neq Y \subseteq \lim _{幺} \Phi_{i}(Y)$, so we can apply Lemma 3.1 .8 to $f$ and see that $Y$ is a dense subspace of $\lim _{\leftrightarrows} \Phi_{i}(Y)$. Therefore the closure of $Y$ in $\lim _{\leftrightarrows} \Phi_{i}(Y)$ is all of $\lim _{\leftrightarrows} \Phi_{i}(Y)$ and the same holds for the closure $\bar{Y}$ in $X$.

### 3.1.10 Definition. (cofinal)

For a directed set $I$ we call a subset $J \subseteq I$ cofinal in $I$ if for any $i \in I$ there is some $j \in J$ with $j \geq i$.
3.1.11 Lemma. Let $\left(X_{i}, \varphi_{i j}, I\right)$ a projective system of compact Hausdorff spaces and $J$ cofinal in $I$. Then $\left(X_{i}, \varphi_{i j}, J\right)$ is as well a projective system of compact Hausdorff spaces and

$$
\varliminf_{亡}{ }_{i \in I} X_{i} \cong \lim _{j \in J} X_{j} .
$$

Proof. First of all observe that $J$ is as well directed since it is cofinal in $I$ and therefore $\left(X_{i}, \varphi_{i j}, J\right)$ is obviously a projective system. On top of that we can find $j_{i} \in J$ for any $i \in I$ such that $j_{i} \geq i$. Let us denote the projections $\lim _{i \in I} X_{i} \longrightarrow X_{i}$ by $\Phi_{i}$ for $i \in I$. So the compatible family of continuous maps $\psi_{i}: \lim _{\rightleftarrows}^{\rightleftarrows} X_{j} \longrightarrow X_{i}$ for $i \in I$, which are defined as the composition

$$
\lim _{j \in J} X_{j} \xrightarrow{\Phi_{j_{i}}} X_{j_{i}} \xrightarrow{\varphi_{j_{i} i}} X_{i},
$$

induce a continuous map

$$
\Phi: \lim _{\ddagger} j \in J X_{j} \longrightarrow \lim _{i \in I} X_{i} .
$$

Note that the definition of $\psi_{i}$ does not depend on the chosen index $j_{i}$ since the maps $\varphi_{i j}$ are compatible. $\Phi$ is injective since

$$
\Phi\left(\left(x_{j}\right)\right)=\left(y_{i}\right) \Longrightarrow y_{j}=x_{j} \forall j \in J
$$

and it is surjective since $\left(x_{j}\right) \in \varliminf_{j \in J} X_{j}$ is a preimage for $\left(x_{i}\right) \in \lim _{i \in I} X_{i}$. So $\Phi$ is a homeomorphism as continuous bijection between compact Hausdorff spaces.
Observe that the inverse of $\Phi$ is given by the map $\Psi: \varliminf_{\underset{~}{~}}^{i \in I}$ $X_{i} \longrightarrow \varliminf_{\ddagger} \lim _{j \in J} X_{j}$ which is induced by the family of projections $\Phi_{j}: \varliminf_{\ddagger} \lim _{i \in I} X_{i} \longrightarrow X_{j}$ for $j \in J$.

### 3.2 Profinite groups and profinite completion of groups

The preliminary work of the last section enables us to introduce profinite groups as projective limit of finite groups. Later we will see some further characterisations of them, for example as totally disconnected, compact groups. So there are many topological groups which are not profinite, but we will find a profinite completion of an arbitrary group by taking the profinite limit of all finite quotients of it.

### 3.2.1 Definition. (Profinite group)

If $\left(G_{i}, \varphi_{i j}, I\right)$ is a projective system of finite groups endowed with the discrete topology, then we call $\lim _{\rightleftarrows} G_{i}$ a profinite group.
3.2.2 Lemma. Let $\left(G_{i}, \varphi_{i j}, I\right)$ be a projective system of finite groups endowed with the discrete topology, $G=\not \lim _{i} G_{i}$ and $\Phi_{i}: G \longrightarrow G_{i}$ the projections for $i \in I$. Then $\left\{\operatorname{ker}\left(\Phi_{i}\right) \mid i \in I\right\}$ is a neighborhood basis of $1 \in G$.

Proof. By defintion of $G$ as subspace of $\prod_{i \in I} G_{i}$ a neighborhood basis of $1 \in G$ is given by sets of the form

$$
\left[\left(\prod_{i \in I \backslash\left\{i_{1}, \ldots, i_{n}\right\}} G_{i}\right) \times\left(\prod_{i \in\left\{i_{1}, \ldots, i_{n}\right\}}\left\{1_{G_{i}}\right\}\right)\right] \cap G
$$

for some $n \in \mathbb{N}$ and $i_{1}, \ldots, i_{n} \in I$. Since $I$ is directed there is $i_{0} \in I$ with $i_{0} \geq i_{1}, \ldots, i_{n}$ and by definiton of $G$ we see
$\operatorname{ker}\left(\Phi_{i_{0}}\right)=\left[\left(\prod_{i \in I \backslash\left\{i_{0}\right\}} G_{i}\right) \times\left\{1_{G_{i_{0}}}\right\}\right] \cap G \subseteq\left[\left(\prod_{i \in \backslash \backslash\left\{i_{1}, \ldots, i_{n}\right\}} G_{i}\right) \times\left(\prod_{i \in\left\{i_{1}, \ldots, i_{n}\right\}}\left\{1_{G_{i}}\right\}\right)\right] \cap G$
which implies the claim.

### 3.2.3 Definition. (Core)

Let $G$ be a group and $H \leq G$ a subgroup. We call

$$
\begin{equation*}
H_{G}:=\bigcap_{g \in G} g H g^{-1} \tag{1}
\end{equation*}
$$

the core of $H$ in $G$.
3.2.4 Lemma. Let $G$ be a group and $H \leq G$ a subgroup. Then the core $H_{G}$ of $H$ in $G$ is a normal subgroup of $G$ which is contained in $H$ and $H_{G}$ is of finite index in $G$ if and only if $H$ is of finite index in $G$. Furthermore if $G$ is a compact topological group and $H$ an open subgroup of $G$, then $H_{G}$ is open in $G$ as well.

Proof. The fact that $H_{G}$ is a normal subgroup in $G$ which is contained in $H$ should be obvious. So if $H$ is not of finite index in $G$, then $H_{G}$ can't be either. Therefore let us assume now that $H$ is of finite index in $G$ and observe that we have a surjection

$$
s: G / H \longrightarrow\left\{g H g^{-1} \mid g \in G\right\}, g H \longmapsto g H g^{-1} .
$$

Note that $s$ is well-defined since

$$
g_{1} H=g_{2} H \Longrightarrow g_{1} H g_{1}^{-1}=g_{1} H H^{-1} g_{1}^{-1}=g_{2} H H^{-1} g_{2}^{-1}=g_{2} H g_{2}^{-1}
$$

for any $g_{1}, g_{2} \in G$. So by finiteness of $G / H$ we see that the intersection in (11) is in fact finite and since $H$ is of finite index in $G$ every conjugate $g H^{-1}$ is of finite index as well. Hence $H_{G}$ is a finite intersection of finite index subgroups and therefore itself of finite index. Now let $H$ be open in the compact group $G$. Then $H$ is of finite index and again the intersection in (1) is finite. Furthermore $g \mathrm{Hg}^{-1}$ is open in $G$ for every $g \in G$ as homeomorphic image of $H$ under conjugation with $g$. This proves the claim.
3.2.5 Lemma. Let $X$ be a compact Hausdorff space. For every $x \in X$ the connected component $C(x)$ of $x$ is the intersection of all clopen (i.e. closed and open) neighborhoods of $x$.

Proof. Let $x \in X, \mathcal{U}$ be the set of all clopen neighborhoods of $x$ and $A:=\bigcap_{U \in \mathcal{U}} U$. Obviously every clopen neighborhood of $x$ contains its connected component $C(x)$, so $C(x) \subseteq A$. Hence it suffices to show that $A$ is connected. For that purpose let $A=U \cup V$ with $U \cap V=\emptyset$ and $U, V$ closed in $A$. Since $A$ is closed in $X$ we have that $U, V$ are also closed in $X$ and hence compact. Furthermore $X$ is Hausdorff, so by compactness and disjointness of $U$ and $V$ we can find open sets $\widetilde{U}, \widetilde{V}$ with $U \subseteq \tilde{U}, V \subseteq \tilde{V}$ and $\widetilde{U} \cap \widetilde{V}=\emptyset$. Therefore

$$
[X \backslash(\widetilde{U} \cup \widetilde{V})] \cap A=\emptyset
$$

and since $X \backslash(\widetilde{U} \cup \widetilde{V})$ is closed we can find a finite subset $\mathcal{V} \subseteq \mathcal{U}$ such that

$$
\begin{equation*}
[X \backslash(\widetilde{U} \cup \tilde{V})] \cap B=\emptyset \tag{2}
\end{equation*}
$$

with $B:=\bigcap_{U \in \mathcal{V}} U$. Note that $B$ is a clopen neighborhood of $x$ since $\mathcal{V}$ is finite. Furthermore $x \in(B \cap \widetilde{U}) \cup(B \cap \widetilde{V}) \stackrel{\mid(2)}{=} B$, so w.l.o.g we can assume that $x \in B \cap \widetilde{U}$. Observe that $B \cap \widetilde{U}$ is clopen since $B \cap \widetilde{U}=[X \backslash(B \cap \widetilde{V})] \cap B$, so $(B \cap \widetilde{U}) \in \mathcal{U}$. Therefore $A \subseteq B \cap \widetilde{U} \subseteq \widetilde{U}$ and we can conclude that $A \cap V \subseteq A \cap \widetilde{V}=\emptyset$ by disjointness of $\widetilde{U}$ and $\widetilde{V}$. Thus $V=\emptyset$ and $A$ is connected.

### 3.2.6 Proposition. Every totally disconnected group $G$ is Hausdorff.

Proof. If $G$ is totally disconnected the connected component $C(e)$ of the neutral element $e \in G$ is $\{e\}$. So, as every connected component, $\{e\}$ is closed in $G$. Now consider the continuous map

$$
f: G \times G \longrightarrow G, \quad(g, h) \longmapsto g h^{-1}
$$

and observe that the diagonal $\Delta:=\{(g, g) \in G \times G \mid g \in G\}$ is the preimage of $\{e\}$ under $f$. Hence $\Delta$ is closed in $G \times G$ and therefore $G$ is Hausdorff.

Finally we are able to prove some further characterisations of profinite groups.
3.2.7 Theorem. For a topological group $G$ the following statements are equivalent.
a) $G$ is a profinite group.
b) $G$ is compact and totally disconnected.
c) $G$ is compact and $1 \in G$ admits a neighborhood basis $\mathcal{U}$ consisting of open normal subgroups of $G$ and $\bigcap_{U \in \mathcal{U}} U=1$.
d) $1 \in G$ admits a neighborhood basis $\mathcal{U}$ consisting of open normal subgroups of $G$ with finite index and $G \cong \lim _{U \in \mathcal{U}} G / U$.
Proof. a) $\Rightarrow \mathrm{b})$ : Let $G$ be profinite, so $G=\lim _{i} G_{i}$ for a projective system $\left(G_{i}, \varphi_{i j}, I\right)$ of finite discrete groups. So by assumption $G_{i}$ is compact and totally disconnected for every $i \in I$ and so is $G$ by Proposition 3.1.3.
$\mathrm{b}) \Rightarrow \mathrm{c})$ : Let $G$ be a compact and totally disconnected group and $U$ an open neighborhood of $1 \in G$. First we want to find some clopen neighborhood $V$ of 1 which is contained in $U$. For that purpose consider the set $\mathcal{U}$ of all clopen neighborhoods of 1 . Then Lemma 3.2.5 tells us that

$$
\{1\}=\bigcap_{X \in \mathcal{U}} X
$$

since $G$ is totally disconnected. Furthermore $G \backslash U$ is closed and $(G \backslash U) \cap\left(\bigcap_{X \in \mathcal{U}} X\right)=\emptyset$, so by compactness of $G$ we can conclude that there is some finite subset $\mathcal{V} \subseteq \mathcal{U}$ such that $(G \backslash U) \cap\left(\bigcap_{X \in \mathcal{V}} X\right)=\emptyset$. Hence $V:=\bigcap_{X \in \mathcal{V}} X$ does the job. Now we show that there is some open normal subgroup $W$ of $G$ which is contained in $V$. Consider $C:=(G \backslash V) \cap V^{2}$ and note that $C$ is closed in $G$ and hence compact. Now let $x \in V$ arbitrary, so $x \in G \backslash C$. Since multiplication in $G$ is continuous and $G \backslash C$ is open in $G$, we can find open neighborhoods $V_{x}$ of $x$ and $S_{x}$ of 1 such that $V_{x}, S_{x} \subseteq V$ and $V_{x} S_{x} \subseteq G \backslash C$. Now compactness of $V$ tells us, that we can find finitely many $x_{1}, \ldots, x_{n}$ such that $\bigcup_{i=1}^{n} V_{x_{i}}=V$. Let $S:=\bigcap_{i=1}^{n} S_{x_{i}}$ and consider $T:=S \cap S^{-1}$, which is a symmetric (i.e. $T=T^{-1}$ ) open neighborhood of 1 , contained in $V$ and satisfies $V T \subseteq G \backslash C$. On the other hand we have $V T \subseteq V^{2}$, so we can conclude that $V T \cap(G \backslash V)=\emptyset$ which means that $V T \subseteq V$. So by induction we see that $V T^{n} \subseteq V$ for every $n \in \mathbb{N}$ and since $T$ is symmetric we find $R:=\bigcup_{n \in \mathbb{N}} T^{n}$ as an open subgroup of $G$ which is contained in $V$. Now let $W:=\bigcap_{q \in G} g R g^{-1}$ be the core of $R$ in $G$. Since $R$ is open and $G$ compact we see by Lemma 3.2.4 that $W$ is an open normal subgroup of $G$ which satisfies

$$
W \subseteq R \subseteq V R \subseteq \bigcup_{n \in \mathbb{N}} V T^{n} \subseteq V
$$

c) $\Rightarrow$ d): Let $\mathcal{U}$ be as in $c$ ) and note that by compactness of $G$ every $U \in \mathcal{U}$ is of finite index. We find a projective system $\left(G / U, \pi_{U V}, \mathcal{U}\right)$ of finite discrete groups using the partial order

$$
U \geq V: \Longleftrightarrow U \subseteq V
$$

on $\mathcal{U}$ and the natural projections $\pi_{U V}: G / U \longrightarrow G / V$ for $U \geq V$. Since the canonical projections $\pi_{U}: G \longrightarrow G / U$ for $U \in \mathcal{U}$ are compatible, we obtain an induced continuous homomorphism

$$
\Phi: G \longrightarrow \lim _{U \in \mathcal{U}} G / U, g \longmapsto(g U)_{U \in \mathcal{U}} .
$$

By assumption $G$ and $G / U$ are compact Hausdorff spaces for every $U \in \mathcal{U}$ so we can use Corollary 3.1 .7 to see that $\Phi$ is surjective. Furthermore

$$
\operatorname{ker}(\Phi)=\bigcap_{U \in \mathcal{U}} U=1
$$

so $\Phi$ is a continuous bijection between compact Hausdorff spaces and hence a homeomorphism. Therefore it is an isomorphism of topological groups.
d) $\Rightarrow$ a): Trivial.

Now let $G$ be an abstract group. In the following we will construct a profinite group which is closely related to $G$. For that purpose let $\mathcal{N}_{G}$ be the set of all normal finite index subgroups of $G$. We can define a partial order on $\mathcal{N}_{G}$ by

$$
M \geq N: \Longleftrightarrow M \subseteq N
$$

which turns $\mathcal{N}_{G}$ into a directed set, since two normal finite index subgroups $N$ and $M$ have $M \cap N$ as common upper bound. So we can use $\mathcal{N}_{G}$ as index set of a projective system of topological groups $\left(G / N, \pi_{M N}, \mathcal{N}_{G}\right)$, where $\pi_{M N}: G / M \longrightarrow G / N$ are the canonical projections for $M \geq N$ and the finite groups $G / N$ are equipped with the discrete topology for every $N \in \mathcal{N}_{G}$.

### 3.2.8 Definition. (Profinite completion)

The profinite group $\varliminf_{\mathrm{K}}^{\mathrm{N} \in \mathcal{N}_{G}} G / N$ is called the profinite completion of $G$ and denoted by $\widehat{G}$.

In order to make sense of the term profinite completion, we have to find a suitable topology on $G$ which turns it into a topological group and yields a natural continuous homomorphism $G \longrightarrow \widehat{G}$. So it would be helpful to have compatible continuous homomorphisms $\pi_{N}: G \longrightarrow G / N$ for $N \in \mathcal{N}_{G}$, since then the universal property of the projective limit does the rest.

### 3.2.9 Definition. (Profinite topology)

The initial topology on $G$ with respect to the family of canonical projections $\left\{\pi_{N}\right\}_{N \in \mathcal{N}_{G}}$ is called the profinite topology on $G$.
3.2.10 Proposition. A neighborhood basis of 1 in the profinite topology of $G$ is given by $\mathcal{N}_{G}$ and it turns $G$ into a topological group.

Proof. By definition as initial topology of $\left\{\pi_{N}\right\}_{N \in \mathcal{N}_{G}}$ a basis of the profinite topology is given by finite intersections of sets like $\pi_{N}^{-1}(g N)=g N$ for $N \in \mathcal{N}_{G}$. If such a finite intersection wants to contain $1 \in G$, it has to be a finite intersection of elements in $\mathcal{N}_{G}$. But $\mathcal{N}_{G}$ is closed under taking finite intersections, so it is again an element of $\mathcal{N}_{G}$. This shows that $\mathcal{N}_{G}$ is a neighborhood basis of 1 in the profinite topology. The fact that this topology turns $G$ into a topological group is shown in Proposition 1 of Chapter 3 in Bourbaki, 1989.

Now we have a topological group $G$ and a family of compatible continuous homomorphisms $\pi_{N}: G \longrightarrow G / N$ for every $N \in \mathcal{N}_{G}$, which induce a continuous homomorphism $i: G \longrightarrow \underset{\rightleftarrows}{\lim } G / N=\widehat{G}$ with

$$
\operatorname{ker}(i)=\bigcap_{N \in \mathcal{N}_{G}} N
$$

So the map $i$ is injective if and only if $\bigcap_{N \in \mathcal{N}_{G}} N=1$, which is equivalent to $G$ being Hausdorff with respect to its profinite topology. Hence we want to define...

### 3.2.11 Definition. (Residually finite)

An abstract group $G$ is called residually finite if $\bigcap_{N \in \mathcal{N}_{G}} N=1$.
In the following, if we talk about an abstract group $G$ as topological group, we always think of it equipped with its profinite topology.
3.2.12 Lemma. The natural continuous homomorphism $i: G \longrightarrow \widehat{G}$ maps $G$ onto a dense subgroup of $\widehat{G}$ and satisfies the following universal property:
If $H$ is a profinite group and $\phi: G \longrightarrow H$ is a continuous homomorphism, then there is a unique continuous homomorphism $\Phi: \widehat{G} \longrightarrow H$ such that $\Phi \circ i=\phi$.


Proof. Note that by Lemma 3.1.8 we have that $i(G)$ is a dense subgroup of $\widehat{G}$. So let $\phi: G \longrightarrow H$ be a continuous homomorphism to a profinite group $H$. By Theorem 3.2.7 we find a neighborhood basis $\mathcal{U}$ of $1 \in H$ consisting of open normal subgroups in $H$ with finite index such that $H=\varliminf_{\zeta} \operatorname{li\mathcal {U}} H / U$. Observe that for every $U \in \mathcal{U}$ we find $N_{U}:=\phi^{-1}(U)$ as normal subgroup of finite index in $G$ and the fundamental theorem of homomorphisms gives an homomorphism $\phi_{U}: G / N_{U} \longrightarrow H / U$ induced by $\phi$. Denoting the projections $\underset{\rightleftarrows}{\varliminf} G / N \longrightarrow G / N$ by $\Phi_{N}$ we obtain a compatible family of continuous homomorphisms $\Psi_{U}: \lim _{\rightleftarrows} G / N \longrightarrow H / U$ defined as the composition

$$
\underset{\rightleftarrows}{\lim } G / N \xrightarrow{\Phi_{N_{U}}} G / N_{U} \xrightarrow{\phi_{U}} H / U .
$$

and they induce a continuous homomorphism

$$
\Phi: \widehat{G}=\lim _{\check{ }} G / N \longrightarrow \varliminf_{\check{ }} H / U \cong H .
$$

Explicitly, it is given by $\Phi\left(\left(g_{N} N\right)\right)=\left(\phi\left(g_{N_{U}}\right) U\right)$, so it should be obvious that $\Phi \circ i=\phi$, if we remember that the isomorphism $H \xrightarrow{\sim} \underset{\rightleftarrows}{\lim } H / U$ is given by $h \longmapsto(h U)$. In order to see that the extension $\Phi$ is unique, let us assume that $\Phi_{1}$ and $\Phi_{2}$ are continuous homomorphisms $\widehat{G} \longrightarrow H$ with $\Phi_{j} \circ i=\phi$ for $j=1,2$. Then the equaliser

$$
E:=\left\{x \in \widehat{G} \mid \Phi_{1}(x)=\Phi_{2}(x)\right\}
$$

is a closed subset of $\widehat{G}$ since the maps $\Phi_{j}$ are continuous and $H$ is a Hausdorff space. On top of that, we have by assumption $i(G) \subseteq E$. So $i(G)$ being dense in $\widehat{G}$ implies $E=\widehat{G}$ and hence $\Phi_{1}=\Phi_{2}$.
3.2.13 Proposition. Let $G$ be a residually finite group, so that we can identify $G$ with its image under the natural continuous monomorphism (i.e. injective homomorphism) $i: G \longrightarrow \widehat{G}$.
a) There is a bijection

$$
\Phi:\left\{U \mid U \leq_{o} G\right\} \longrightarrow\left\{V \mid V \leq_{o} \widehat{G}\right\}, U \longmapsto \bar{U}
$$

with inverse

$$
\Psi:\left\{V \mid V \leq_{o} \widehat{G}\right\} \longrightarrow\left\{U \mid U \leq_{o} G\right\}, V \longmapsto V \cap G .
$$

b) If $H, K \in\left\{U \mid U \leq \leq_{o} G\right\}$ and $H \leq K$ then $[K: H]=[\bar{K}: \bar{H}]$. Moreover $H \unlhd K$ if and only if $\bar{H} \unlhd \bar{K}$ and in this case $K / H \cong \bar{K} / \bar{H}$.

Proof. a) First of all note that $\Phi$ is well-defined since by compactness a subgroup $U$ of $\widehat{G}$ is open if and only if it is closed and of finite index. So if $U$ is an open subgroup of $G$ by Proposition 3.2 .10 there is some normal subgroup of finite index in $G$ contained in $U$ which implies that $U$ itself has finite index in $G$. Hence we find $g_{1}, \ldots, g_{n} \in G$ for some $n \in \mathbb{N}$ such that $\coprod_{i=1, \ldots, n} g_{i} U=G$. Since $G$ is dense in $\widehat{G}$ we can conclude

$$
\widehat{G}=\bar{G}=\bigcup_{i=1, \ldots, n} g_{i} \bar{U}
$$

by taking the closure and see that $\bar{U}$ has finite index in $\widehat{G}$. To see that $\Psi$ is welldefined observe that $V \cap G=i^{-1}(V)$ for any open subgroup $V$ of $\widehat{G}$ and use that $i$ is a continuous homomorphism. If $V$ is an open subgroup of $\widehat{G}$ we know that $V$ is closed in $\widehat{G}$ and $V \cap G$ is dense in $V$ since $G$ is dense in $\widehat{G}$. So

$$
\Phi \circ \Psi(V)=\overline{V \cap G}=V .
$$

Conversely if $U$ is an open subgroup of $G$, we see that

$$
U \subseteq \bar{U} \cap G=\Psi \circ \Phi(U)
$$

So let $x \in \bar{U} \cap G$. Recall that the identification of $G$ in $\widehat{G}$ is given by

$$
g \longmapsto(g N) \in \varliminf_{\longleftarrow}{ }_{N \in \mathcal{N}} G / N .
$$

Lemma 3.1.9 tells us that $\bar{U}=\lim _{N \in \mathcal{N}(G)} U N / N$. Thus $x \in U N$ for every $N \in \mathcal{N}_{G}$. Since $U$ is an open subgroup of $G$, Proposition 3.2 .10 guarantees the existence of a normal subgroup $N_{U}$ of $G$ contained in $U$ and with finite index in $G$. For example the core

$$
U_{G}:=\bigcap_{g \in G} g U g^{-1} \subseteq U
$$

of $U$ in $G$ does the job. Hence we can conclude $x \in U U_{G}=U$.
b) Since $[K: H]=[G: H] /[G: K]$ and $[\bar{K}: \bar{H}]=[\widehat{G}: \bar{H}] /[\widehat{G}: \bar{K}]$ we only have to show that $[G: U]=[\widehat{G}: \bar{U}]$ for any open subgroup $U$ of $G$. First of all let us convince ourselves that $G \bar{U}=\widehat{G}$. Note that

$$
G \bar{U}=\bigcup_{g \in G} g \bar{U}
$$

where the right hand side is in fact a finite union since $\bar{U}$ has finite index in $\widehat{G}$. Furthermore $g \bar{U}$ is closed in $\widehat{G}$ as homeomorphic image under left-multiplication with $g$ of $\bar{U}$, so we see that $G \bar{U}$ is closed in $\widehat{G}$. Thus $G$ being dense in $\widehat{G}$ and contained in $G \bar{U}$ implies $G \bar{U}=\widehat{G}$. Hence, if $n$ denotes the index of $\bar{U}$ in $\widehat{G}$, we can find $x_{1}, \ldots, x_{n} \in G$ as system of representatives for the left cosets of $\bar{U}$ in $\widehat{G}$. By a) we see that for any $x \in G$ we have $x \bar{U} \cap G=x U$ and conclude $n=[G: U]$ by

$$
G=\widehat{G} \cap G=\bigsqcup_{i=1}^{n}\left(x_{i} \bar{U} \cap G\right)=\bigsqcup_{i=1}^{n} x_{i} U .
$$

Now let $H \unlhd K$. Then $H N / N \unlhd K N / N$ for every $N \in \mathcal{N}_{G}$, since the image of normal subgroups under surjective homomorphisms are normal and hence

$$
\bar{H}=\lim _{\check{c}} N \in \mathcal{N} H N / N \unlhd \varliminf_{幺} H \in \mathcal{N} K N / N=\bar{K} .
$$

Conversely, if $\bar{H} \unlhd \bar{K}$, a) tells us that

$$
H=\bar{H} \cap G \unlhd \bar{K} \cap G=K .
$$

To see that $K / H \cong \bar{K} / \bar{H}$ consider the homomorphism $\phi: K \longrightarrow \bar{K} / \bar{H}$ given by the composition

$$
K \xrightarrow{\left.i\right|_{K}} \bar{K} \xrightarrow{\pi} \bar{K} / \bar{H},
$$

where $\pi$ denotes the canonical projection. Applying the fundamental theorem of homomorphisms to $\phi$ and using that

$$
\operatorname{ker}(\phi)=\bar{H} \cap K=H,
$$

we see that $\phi$ factors through $K / H$ by a monomorphism $K / H \longrightarrow \bar{K} / \bar{H}$ which has to be surjective since $[K: H]=[\bar{K}: \bar{H}]$.
3.2.14 Remark. a) If $G$ is a residually finite group, then we can identify $G$ with its image under $i: G \longrightarrow \widehat{G}$ as topological groups since Proposition 3.2.13 implies that $i$ is an embedding of topological spaces.
b) If we assume additionally that $G$ is finitely generated in Proposition 3.2.13, then we can use the result of Nikolov, Segal, and Nikolav, 2007 in order to replace the set $\left\{V \mid V \leq_{o} \widehat{G}\right\}$ by $\left\{V \mid V \leq_{f} \widehat{G}\right\}$, since they showed that in a finitely generated profinite group every subgroup of finite index is open.

Now let us assume that $\phi: G \longrightarrow H$ is a homomorphism of groups. Note that $\phi$ is continuous, if we equip both groups with their profinite topology. Our next goal is to find a canonical continuous homomorphism $\widehat{\phi}: \widehat{G} \longrightarrow \widehat{H}$ in such a way that $\widehat{(\cdot)}$ is functorial. So for $N \in \mathcal{N}_{H}$ consider the embeddings $\Theta_{N}: G / \phi^{-1}(N) \longrightarrow H / N$ of topological groups induced by

$$
G \xrightarrow{\phi} H \xrightarrow{\pi_{N}} H / N,
$$

where $\pi_{N}$ are the canonical projections. In fact, these $\Theta_{N}$ are components of a map $\Theta:\left(G / \phi^{-1}(N), \varphi_{M N}, \mathcal{N}_{H}\right) \longrightarrow\left(H / N, \psi_{M N}, \mathcal{N}_{H}\right)$ of projective systems where

$$
\varphi_{M N}: G / \phi^{-1}(M) \longrightarrow G / \phi^{-1}(N), \psi_{M N}: H / M \longrightarrow H / N
$$

are the canonical projections for $M \subseteq N$. Using functoriality of $\varliminf_{\leftarrow}$. we obtain a continuous homomorphism

$$
\lim \Theta: \lim _{\rightleftarrows} G / \phi^{-1}(N) \longrightarrow \lim _{\rightleftharpoons} H / N .
$$

On top of that, since $\left\{\phi^{-1}(N) \mid N \in \mathcal{N}_{H}\right\}$ is a directed subset of $\mathcal{N}_{G}$, we have a continuous homomorphism

$$
\Lambda: \lim _{\leftrightarrows} G / M \longrightarrow \underset{\leftrightarrows}{\lim } G / \phi^{-1}(N)
$$

induced by the surjective projections $\underset{\leftarrow}{\lim } G / M \longrightarrow G / \phi^{-1}(N)$ for $N \in \mathcal{N}_{H}$. So we can define $\widehat{\phi}$ as the composition

$$
\widehat{G}=\lim _{\leftrightarrows} G / M \xrightarrow{\Lambda} \varliminf_{\doteqdot} G / \phi^{-1}(N) \xrightarrow{\text { lim } \Theta} \underset{\leftrightarrows}{\varliminf} H / N=\widehat{H} .
$$

Explicitly, this map is given by $\widehat{\phi}\left(\left(g_{M} M\right)\right)=\left(\phi\left(g_{\phi^{-1}(N)}\right) N\right)$, which explains the commutativity of the following diagram:


Observe that $\lim \Theta$ is an embedding of topological groups by Remark 3.1.5 and $\Lambda$ is an epimorphism (i.e. surjective homomorphism) by Corollary 3.1.7.
3.2.15 Lemma. The profinite completion $\widehat{(\cdot)}$ is a functor from the category of groups to the category of profinite groups with continuous homomorphisms.

Proof. Using the explicit description of $\widehat{\phi}$ it is easy to verify that

$$
\widehat{\mathrm{id}_{G}}=\operatorname{id}_{\widehat{G}} \text { and } \widehat{\phi_{2} \circ \phi_{1}}=\widehat{\phi_{2}} \circ \widehat{\phi_{1}}
$$

for homomorphisms $\phi_{1}: G \longrightarrow H$ and $\phi_{2}: H \longrightarrow K$.
3.2.16 Lemma. If $\phi: G \longrightarrow H$ is a homomorphism of groups and $i_{H}: H \longrightarrow \widehat{H}$ the canonical continuous homomorphisms to its profinite completion, then

$$
\operatorname{Im}(\widehat{\phi})=\overline{\operatorname{Im}\left(i_{H} \circ \phi\right)} .
$$

Proof. Let $i_{G}: G \longrightarrow \widehat{G}$ be the canonical continuous homomorphism for $G$. In the discussion above we convinced ourselves that $\widehat{\phi} \circ i_{G}=i_{H} \circ \phi$, so $\operatorname{Im}\left(i_{H} \circ \phi\right) \subseteq \operatorname{Im}(\widehat{\phi})$. Since $\widehat{G}$ is compact and $\widehat{H}$ is Hausdorff we know that $\operatorname{Im}(\widehat{\phi})$ is closed in $\widehat{H}$ and therefore

$$
\overline{\operatorname{Im}\left(i_{H} \circ \phi\right)} \subseteq \operatorname{Im}(\widehat{\phi}) .
$$

Furthermore $i_{G}(G)$ is dense in $\widehat{G}$ which implies that $\operatorname{Im}\left(i_{H} \circ \phi\right)=\widehat{\phi}\left(i_{G}(G)\right)$ is dense in $\widehat{\phi}(\widehat{G})$. Hence

$$
\overline{\operatorname{Im}\left(i_{H} \circ \phi\right)} \supseteq \operatorname{Im}(\widehat{\phi})
$$

and we obtain equality.
3.2.17 Lemma. Let $K$ be a subgroup of $G$ and $\iota: K \hookrightarrow G$ the inclusion. Then the induced map $\widehat{\iota}: \widehat{K} \longrightarrow \widehat{G}$ is injective if and only if the profinite topology of $G$ induces on $K$ its profinite topology.

Proof. We defined $\hat{\iota}$ as the composition

$$
\widehat{K} \xrightarrow{\Lambda} \underset{\longrightarrow}{\lim } K /(K \cap N) \stackrel{\lim \Theta}{\rightleftarrows} \widehat{G}
$$

and observed that $\Lambda$ is an epimorphism and $\varliminf \gg \Theta$ is an embedding. Hence $\widehat{\iota}$ is injective if and only if the epimorphism $\Lambda: \varliminf_{\longleftarrow} K / M \longrightarrow \not \varliminf_{\subsetneq} K /(K \cap N)$ is injective. So let us assume that the profinite topology on $G$ induces the profinite topology on $K$. Then $\left\{K \cap N \mid N \in \mathcal{N}_{G}\right\}$ is a neighborhood basis of $1 \in K$ and hence it is cofinal in $\mathcal{N}_{K}$. Lemma 3.1.11 tells us now that $\Lambda$ is an isomorphism of topological groups and hence injective. Conversely if we assume that $\Lambda$ is injective, then it is an isomorphism of topological groups as continuous bijection between compact Hausdorff spaces. If we denote by $\Phi_{K \cap N}: \varliminf_{幺} K /(K \cap N) \longrightarrow K /(K \cap N)$ the corresponding projections, Lemma 3.2 .2 gives us

$$
\left\{\operatorname{ker}\left(\Phi_{K \cap N}\right) \mid N \in \mathcal{N}_{G}\right\}
$$

as neighborhood basis of $1 \in \lim K /(K \cap N)$. Using that $\Lambda$ is an isomorphism of topological groups and the fact that the profinite topology on $K$ is the coarsest topology, such that the canonical homomorphism $i: K \longrightarrow \widehat{K}$ is continuous, we find

$$
\left\{(\Lambda \circ i)^{-1}\left(\operatorname{ker}\left(\Phi_{K \cap N}\right)\right) \mid N \in \mathcal{N}_{G}\right\}
$$

as neighborhood basis of $1 \in K$. But this means that the profinite topology on $G$ induces on $K$ its profinite topology, since

$$
(\Lambda \circ i)^{-1}\left(\operatorname{ker}\left(\Phi_{K \cap N}\right)\right)=\operatorname{ker}\left(\Phi_{K \cap N} \circ \Lambda \circ i\right)=K \cap N
$$

for every $N \in \mathcal{N}_{G}$.
3.2.18 Corollary. If $K$ is a subgroup of the residually finite group $G$ and $\iota: K \hookrightarrow G$ denotes the inclusion, then $\widehat{\iota} \widehat{K} \longrightarrow \bar{K}$ is an isomorphism of topological groups if and only if the profinite topology on $G$ induces on $K$ its profinite topology.

Proof. By Lemma 3.2 .16 we have $\operatorname{Im}(\hat{\iota})=\overline{\operatorname{Im}(i \circ \iota)}=\bar{K}$, where we identify $G$ with its image in $\widehat{G}$ under the natural embedding $i: G \hookrightarrow \widehat{G}$. By Lemma 3.2.17 we know that $\widehat{\iota}$ is injective if and only if the profinite topology on $G$ induces the profinite topology on $K$. So the claim follows from the fact that $\widehat{\iota}: \widehat{K} \longrightarrow \bar{K}$ is an isomorphism of topological groups if and only if it is bijective, since $\widehat{\iota}$ is continuous and $\widehat{K}, \bar{K}$ are compact Hausdorff spaces.
3.2.19 Lemma. Let $H$ be a subgroup of $G$, which is open in the profinite topology of $G$. Then the profinite topology on $G$ induces on $H$ its profinite topology.

Proof. Since $H$ is open in the profinite topology on $G$ by assumption, we know that $H$ is of finite index in $G$. Now we want to show that for any normal subgroup $N \unlhd H$ with finite index we can find a normal subgroup $M \unlhd G$ with finite index, such that $M \leq N$. So let $M:=N_{G}$ be the core of $N$ in $G$. Since $N$ has finite index in $H$ and $H$ has finite index in $G$, we see that $N$ has finite index in $G$ as well and by Lemma 3.2.4 we can conclude that $M$ satisfies everything we wanted.

## $4 L^{2}$-Betti numbers and profinite invariance

In Chapter 2 we introduced the $L^{2}$-Betti numbers of a group $G$ and in Chapter 3 we defined its profinite completion. So for the $p$-th $L^{2}$-Betti number to be a profinite invariant, we require that $b_{p}^{(2)}(G)=b_{p}^{(2)}(H)$ for any two groups $G$ and $H$ which have isomorphic profinite completions $\widehat{G} \cong \widehat{H}$. Chapter 4.1 will show that this is actually true for the first $L^{2}$-Betti number if we consider finitely presented residually finite groups, but in Chapter 4.2 we construct explicit counterexamples for every even dimension greater or equal to 6 .

### 4.1 The first $L^{2}$-Betti number is a profinite invariant

In this section, which is based on Reid, 2013, we want to show that the first $L^{2}$-Betti number is a profinite invariant for finitely presented residually finite groups (cf. Theorem 1.0.1).

The following observation will be key for this section.
4.1.1 Proposition. Let $G$ be a finitely generated group and $F$ a finite discrete group. Then every group homomorphism $\Phi: \widehat{G} \longrightarrow F$ is continuous, which means that

$$
\operatorname{Hom}_{\underline{T G r p}}(\widehat{G}, F)=\operatorname{Hom}_{\underline{G r p}}(\widehat{G}, F) .
$$

Proof. It suffices to show that $\Phi^{-1}\left(1_{F}\right)=\operatorname{ker}(\Phi)$ is open in $\widehat{G}$. But $\operatorname{ker}(\Phi)$ is of finite index in $\widehat{G}$ and hence open by Remark 3.2 .14 b ), since $G$ is finitely generated by assumption.
4.1.2 Lemma. Let $G$ be a finitely generated group, $i: G \longrightarrow \widehat{G}$ the natural map to its profinite completion and $F$ any finite group. Then the map

$$
i^{*}: \operatorname{Hom}_{\underline{G r p}}(\widehat{G}, F) \longrightarrow \operatorname{Hom}_{\underline{G r p}}(G, F), \Phi \longmapsto \Phi \circ i
$$

is a bijection and the restriction to $\operatorname{Epi}(\widehat{G}, F)$ yields a bijection

$$
\operatorname{Epi}(\widehat{G}, F) \xrightarrow{\sim} \operatorname{Epi}(G, F)
$$

Proof. Note that $F$ endowed with its discrete topology is profinite, so we know that

$$
i^{*}: \operatorname{Hom}_{\underline{T G r p}}(\widehat{G}, F) \xrightarrow{\sim} \operatorname{Hom}_{\underline{T G r p}}(G, F)
$$

is a bijection by Lemma 3.2.12. Furthermore, $\operatorname{Hom}_{T G r p}(G, F)=\operatorname{Hom}_{G r p}(G, F)$ since every homomorphism is continuous if the groups carry their profinite topology and $\operatorname{Hom}_{\widehat{T G r p}}(\widehat{G}, F)=\operatorname{Hom}_{\underline{G r p}}(\widehat{G}, F)$ by Proposition 4.1.1. Of course the restriction of $i^{*}$ to $\operatorname{Epi}(\widehat{\widehat{G}}, F)$ is still injective and its image is contained in $\operatorname{Epi}(G, F)$. To see this, let us assume that $\Phi: \widehat{G} \longrightarrow F$ is surjective. Note that $\Phi$ is continuous by Proposition 4.1.1,
if $F$ carries its discrete topology. Since $i(G)$ is dense in $\widehat{G}$ we see that $\Phi(i(G))$ is dense in $\Phi(\widehat{G})=F$. Hence we can conclude

$$
\operatorname{Im}(\Phi \circ i)=\overline{\operatorname{Im}(\Phi \circ i)}=F,
$$

since $F$ is discrete. Furthermore the image of $\left.i^{*}\right|_{\operatorname{Epi}(\widehat{G}, F)}$ has to be all of $\operatorname{Epi}(G, F)$ since $\Phi$ needs to be surjective if $\Phi \circ i$ wants to have a chance to be surjective.
4.1.3 Corollary. Let $G_{1}$ and $G_{2}$ be finitely generated groups with $\widehat{G}_{1} \cong \widehat{G}_{2}$. Then for any finite group $F$ we have

$$
\left|\operatorname{Hom}_{\underline{G r p}}\left(G_{1}, F\right)\right|=\left|\operatorname{Hom}_{\underline{G r p}}\left(G_{2}, F\right)\right| .
$$

4.1.4 Lemma. Let $G$ be a finitely generated group. Then

$$
b_{1}(G)=\operatorname{dim}_{\mathbb{Q}}\left[(G /[G, G]) \otimes_{\mathbb{Z}} \mathbb{Q}\right],
$$

so the first Betti number of $G$ is the greatest integer $b \in \mathbb{N}_{0}$ such that $G$ surjects onto $\left(\mathbb{Z} / p^{k} \mathbb{Z}\right)^{b}$ for every $k \in \mathbb{N}$ and every $p \in \mathbb{P}$.

Proof. Note that the quotient map $E G \longrightarrow B G=G \backslash E G$ is a covering map and $E G$ is (weakly) contractible. So $E G$ is the universal cover of $B G$ and $\pi_{1}(B G)=G$. Hence Hurewicz gives us

$$
H_{1}(B G ; \mathbb{Z})=\pi_{1}(B G)^{a b}=G^{a b}=G /[G, G]
$$

since $B G$ is path-connected and we conclude

$$
b_{1}(G)=\operatorname{dim}_{\mathbb{Q}}\left(H_{1}(B G ; \mathbb{Q})\right)=\operatorname{dim}_{\mathbb{Q}}\left[(G /[G, G]) \otimes_{\mathbb{Z}} \mathbb{Q}\right]
$$

by using the universal coefficient theorem for homology.
4.1.5 Corollary. Let $G$ and $H$ be finitely generated groups. If $H$ is isomorphic to a dense subgroup of $\widehat{G}$, then $b_{1}(H) \geq b_{1}(G)$.

Proof. Recall that for a finitely generated group $X$ we can characterise $b_{1}(X)$ as the greatest integer $b$ such that $X$ surjects onto $\left(\mathbb{Z} / p^{k} \mathbb{Z}\right)^{b}$ for every $k \in \mathbb{N}$ and every $p \in \mathbb{P}$ by Lemma 4.1.4. Let us denote by $i: G \longrightarrow \widehat{G}$ the natural continuous homomorphism of $G$ to its profinite completion and by $j: H \hookrightarrow \widehat{G}$ the embedding of $H$ into $\widehat{G}$. The same argumentation as in the proof of Lemma 4.1 .2 shows that for any epimorphism $\Phi: \widehat{G} \longrightarrow F$ onto a finite group $F$, the restriction $\Phi \circ j$ is an epimorphism as well. So the map

$$
j^{*}: \operatorname{Epi}(\widehat{G}, F) \longrightarrow \operatorname{Epi}(H, F), \Phi \longmapsto \Phi \circ j
$$

is well defined. Hence any epimorphism $f \in \operatorname{Epi}\left(G,\left(\mathbb{Z} / p^{k} \mathbb{Z}\right)^{b}\right)$ yields an epimorphism $j^{*} \circ\left(i^{*}\right)^{-1}(f) \in \operatorname{Epi}\left(H,\left(\mathbb{Z} / p^{k} \mathbb{Z}\right)^{b}\right)$, where we use Lemma 4.1.2 in order to invert

$$
i^{*}: \operatorname{Epi}(\widehat{G}, F) \longrightarrow \operatorname{Epi}(G, F), \Phi \longmapsto \Phi \circ i
$$

4.1.6 Definition. We introduce the following notation for a group $G$ and $d \in \mathbb{N}$ :

- $\mathcal{N}_{G}^{d}:=\{N \unlhd G \mid[G: N] \leq d\}$
- $M_{G}^{d}:=\bigcap_{N \in \mathcal{N}_{G}^{d}} N$
4.1.7 Corollary. Let $G$ be a finitely generated residually finite group. Then

$$
M_{\overparen{G}}^{d}=\overline{M_{G}^{d}} .
$$

Proof. For normal subgroups $N_{1}$ and $N_{2}$ of finite index in $G$ we can find epimorphisms $\phi_{i}: G \longrightarrow F_{i}$ onto finite groups $F_{i}$ such that $\operatorname{ker}\left(\phi_{i}\right)=N_{i}(i=1,2)$. By Lemma 4.1.2 there are extensions $\Phi_{i}: \widehat{G} \longrightarrow F_{i}$. Note that $\operatorname{ker}\left(\Phi_{i}\right)$ is of finite index in $\widehat{G}$ and hence open by Remark 3.2 .14 b). So Proposition 3.2 .13 tells us that $\operatorname{ker}\left(\Phi_{i}\right)=\overline{N_{i}}$ since

$$
\operatorname{ker}\left(\Phi_{i}\right) \cap G=\operatorname{ker}\left(\phi_{i}\right)=N_{i} .
$$

Furthermore we can consider the product $\phi_{1} \times \phi_{2}: G \longrightarrow F_{1} \times F_{2}$ and extend it to a $\operatorname{map} \Phi: \widehat{G} \longrightarrow F_{1} \times F_{2}$. Then Lemma 4.1.2 implies that $\Phi=\Phi_{1} \times \Phi_{2}$ since extensions are unique by Lemma 4.1.2 and hence

$$
\overline{N_{1} \cap N_{2}}=\operatorname{ker}(\Phi)=\operatorname{ker}\left(\Phi_{1} \times \Phi_{2}\right)=\overline{N_{1}} \cap \overline{N_{2}} .
$$

So by induction we can show that

$$
\overline{\bigcap_{i=1, \ldots, n} N_{i}}=\bigcap_{i=1, \ldots, n} \overline{N_{i}}
$$

for $n \in \mathbb{N}$ and normal subgroups $N_{1}, \ldots, N_{n}$ of finite index in $G$. The fact that there are only finitely many subgroups of given index $d \in \mathbb{N}$ in a finitely generated group gives us

$$
\overline{M_{G}^{d}}=\overline{\bigcap_{N \in \mathcal{N}_{G}^{d}} N}=\bigcap_{N \in \mathcal{N}_{G}^{d}} \bar{N} \stackrel{\overline{3.2 .13}}{=} \bigcap_{M \in \mathcal{N}_{G}^{d}} M=M_{\widehat{G}}^{d} .
$$

### 4.1.8 Definition. ( $H$-separable)

A group $G$ is called $H$-separable for a subgroup $H \leq G$, if for every $g \in G \backslash H$ there is some subgroup $K$ of finite index in $G$ such that $H \subseteq K$ but $g \notin K$. Obviously this is equivalent to

$$
\bigcap_{H \subseteq K \leq{ }_{f} G} K=H
$$

4.1.9 Lemma. Let $G$ be a residually finite group and $H$ a finitely generated subgroup of $G$. If $G$ is $U$-separable for every finite index subgroup $U$ of $H$, then the natural homomorphism $\widehat{\iota}: \widehat{H} \longrightarrow \bar{H}$ induced by the inclusion $\iota: H \hookrightarrow G$ is an isomorphism of topological groups.

Proof. By Corollary 3.2.18 we have to show that the profinite topology on $G$ induces the profinite topology on $H$. Let $U$ be a subgroup of finite index in $H$. By assumption $G$ is $U$-separable, so we have

$$
\bigcap_{U \subseteq K \leq_{f} G} K=U
$$

and intersecting both sides with $H$ yields

$$
\begin{equation*}
\bigcap_{U \subseteq K \leq_{f} G}(K \cap H)=U \cap H=U \tag{3}
\end{equation*}
$$

Since $U$ is of finite index in the finitely generated group $H$, there are only finitely many subgroups of $H$ which contain $U$. Hence we find finitely many subgroups $K_{1}, \ldots, K_{n}$ of finite index in $G$ such that

$$
\bigcap_{i=1, \ldots, n}\left(K_{i} \cap H\right)=\bigcap_{U \subseteq K \leq_{f} G}(K \cap H) \stackrel{\sqrt[33]{=}}{=} U
$$

So the finite index subgroup $V:=\bigcap_{i=1, \ldots, n} K_{i}$ of $G$ satisfies $V \cap H=U$. This shows that the profinite topology on $H$ is induced by the profinite topology on $G$.
4.1.10 Corollary. Let $G$ be a finitely generated residually finite group and $H$ a subgroup of finite index in $G$. Then the natural homomorphism $\widehat{\iota}: \widehat{H} \longrightarrow \bar{H}$ induced by the inclusion $\iota: H \hookrightarrow G$ is an isomorphism of topological groups.

Proof. First of all note that $H$ is finitely generated as finite index subgroup of a finitely generated group and every finite index subgroup $U$ of $H$ is of finite index in $G$ as well. Hence $G$ is obviously $U$-separable for every finite index subgroup $U$ of $H$ and we can use Lemma 4.1.9 to see that $\widehat{\iota}$ is an isomorphism of topological groups.
4.1.11 Proposition. Let $G$ and $H$ be finitely presented residually finite groups and $H$ a dense subgroup of $\widehat{G}$. Then $b_{1}^{(2)}(G) \leq b_{1}^{(2)}(H)$.

Proof. First of all note that

$$
\bigcap_{d \in \mathbb{N}} \overline{M_{G}^{d}} \stackrel{4.1 .7}{=} \bigcap_{d \in \mathbb{N}} M_{\widehat{G}}^{d} \stackrel{(3.2 .7}{=} 1 .
$$

So for $L_{d}:=H \cap \overline{M_{G}^{d}} \subseteq \widehat{G}$ we find

$$
\bigcap_{d \in \mathbb{N}} L_{d}=\bigcap_{d \in \mathbb{N}} H \cap \overline{M_{G}^{d}}=H \cap \bigcap_{d \in \mathbb{N}} \overline{M_{G}^{d}}=1 .
$$

Since $G$ and $H$ are dense in $\widehat{G}$, the same argumentation as in the proof of Lemma 4.1.2 shows that the restriction of the natural projection $p_{d}: \widehat{G} \longrightarrow \widehat{G} / M_{G}^{d}$ to $G$ resp. $H$ are still surjective for every $d \in \mathbb{N}$. Furthermore

$$
\operatorname{ker}\left(\left.p_{d}\right|_{H}\right)=H \cap \overline{M_{G}^{d}}=L_{d}
$$

and

$$
\operatorname{ker}\left(\left.p_{d}\right|_{G}\right)=G \cap \overline{M_{G}^{d}} \stackrel{\sqrt[3.2 .13]{=}}{=} M_{G}^{d} .
$$

Note that $M_{G}^{d}$ is open in $G$ since it is of finite index as finite intersection of finite index subgroups. So we obtain

$$
\left[H: L_{d}\right]=\left[\widehat{G}: \overline{M_{G}^{d}}\right]=\left[G: M_{G}^{d}\right] .
$$

Since $H$ is dense in $\widehat{G}$ and $\overline{M_{G}^{d}}$ is open in $\widehat{G}$, we can conclude that that $L_{d}$ is dense in $\overline{M_{G}^{d}} \stackrel{4.1 .10}{\cong} \widehat{M_{G}^{d}}$. Now Corollary 4.1.5 implies that $b_{1}\left(L_{d}\right) \geq b_{1}\left(M_{G}^{d}\right)$, where we use that both $L_{d}$ and $M_{G}^{d}$ are finitely generated as finite index subgroups of finitely generated groups $H$ and $G$. Finally we can use Lück's Approximation Theorem (cf. Theorem 2.3.7) to compare the $L^{2}$-Betti numbers of $G$ and $H$ by

$$
b_{1}^{(2)}(G)=\lim _{d \rightarrow \infty} \frac{b_{1}\left(M_{G}^{d}\right)}{\left[G: M_{G}^{d}\right]} \leq \lim _{d \rightarrow \infty} \frac{b_{1}\left(L_{d}\right)}{\left[H: L_{d}\right]}=b_{1}^{(2)}(H) .
$$

Now the main theorem of this section (cf. Theorem 1.0.1) is a direct consequence of the previous Proposition.

### 4.2 The $\mathrm{L}^{2}$-Betti numbers in general are no profinite invariant

The goal of this section is to show Theorem 4.2.35, which states that there are finitely presented residually finited groups with isomorphic profinite completions and different $L^{2}$-Betti numbers. The construction of these groups and hence most of this section is based on Aka, 2010.
Later we will need the existence of a square root of -7 in $\mathbb{Z}_{2}$, whose existence is guaranteed by Hensel's Lemma. For that purpose we start by introducing the basic notions for this tool.

### 4.2.1 Definition. (Number field and ring of integers)

a) A number field $K \subseteq \mathbb{C}$ is a finite extension of the field $\mathbb{Q}$.
b) If $K$ is a number field we denote by $\mathcal{O}_{K}$ its ring of integers, which consists of all elements $k \in K$ such that there is a monic polynomial $p \in \mathbb{Z}[X]$ with $p(k)=0$.

### 4.2.2 Definition. (Absolute value and valuation)

Let $K$ be a field.
a) An absolute value on $K$ is a map $|\cdot|: K \longrightarrow \mathbb{R}_{\geq 0}$ which satisfies the following conditions for alle $k, l \in K$ :

1) $|k|=0 \Longleftrightarrow k=0$,
2) $|k l|=|k||l|$,
3) $|k+l| \leq|k|+|l|$.

It is called non-archimedean if we can replace condition 3) by the stronger condition $\left.3^{\prime}\right)|k+l| \leq \max \{|k|,|l|\}$.
Otherwise we call it archimedean.
b) A valuation on $K$ is a map $v: K \longrightarrow \mathbb{R} \cup\{\infty\}$ which satisfies the following conditions for all $k, l \in K$ :

1) $v(k)=\infty \Longleftrightarrow k=0$,
2) $v(k l)=v(k)+v(l)$,
3) $v(k+l) \geq \min \{v(k), v(l)\}$.

It is called discrete if there is some natural number $s \in \mathbb{R}_{\geq 0}$ with $v\left(K^{\times}\right)=s \mathbb{Z}$.
4.2.3 Remark. If $|\cdot|: K \longrightarrow \mathbb{R}_{\geq 0}$ is a non-archimedean absolute value, then we find a valuation by

$$
v: K \longrightarrow \mathbb{R} \cup\{\infty\}, k \mapsto \begin{cases}-\log |k| & \text { if } x \neq 0 \\ \infty & \text { if } x=0\end{cases}
$$

Also every valuation $v: K \longrightarrow \mathbb{R} \cup\{\infty\}$ defines a corresponding non-archimedean absolute value by

$$
|\cdot|: K \longrightarrow \mathbb{R}_{\geq 0}, k \mapsto \begin{cases}q^{-v(k)} & \text { if } x \neq 0 \\ 0 & \text { if } x=0\end{cases}
$$

where $q \in \mathbb{R}$ is some real number with $q>1$.
Obviously every absolute value on $K$ yields a metric if we define the distance between $x, y \in K$ by

$$
d(x, y):=|x-y| .
$$

Hence we are able to define Cauchy sequences in $K$ and convergence of sequences in $K$ in the usual way if $K$ is equipped with an absolute value or a valuation.

### 4.2.4 Definition. (Completeness)

A field $K$ is said to be complete with respect to an absolute value $|\cdot|$ on $K$, if every Cauchy sequence $\left\{a_{n}\right\}_{n \in \mathbb{N}}$ in $K$ converges to an element $a \in K$, i.e.

$$
\lim _{n \rightarrow \infty}\left|a_{n}-a\right|=0
$$

If the field $K$ is not complete with respect to an absolute value $|\cdot|$ on $K$, at least there is a complete field $\widehat{K}$ which contains $K$ and the absolute value on $\widehat{K}$ is obtained by extending the absolute value on $K$. For more details we refer to section 4 of Chapter 2 in Neukirch, 1990.

### 4.2.5 Definition. (Valuation ring and residue field)

Let $v: K \longrightarrow \mathbb{R} \cup\{\infty\}$ be a valuation. We call

$$
\mathcal{O}:=\{x \in K \mid v(x) \geq 0\}
$$

the valuation ring of $v$. The units in $\mathcal{O}$ are given by

$$
\mathcal{O}^{\times}:=\{x \in K \mid v(x)=0\}
$$

and $\mathcal{O}$ contains only one maximal ideal, namely

$$
\wp:=\{x \in K \mid v(x)>0\} .
$$

The field $\mathcal{O} / \wp$ is called residue field of $v$.

### 4.2.6 Definition. (Primitive)

Let $K$ be field which is complete with respect to a non-archimedean absolute value $|\cdot|: K \longrightarrow \mathbb{R}_{\geq 0}, \mathcal{O}$ the corresponding valuation ring with its maximal ideal $\wp$ and residue field $\kappa:=\mathcal{O} / \wp$. A polynomial $f=a_{0}+a_{1} X+\ldots+a_{n} X^{n} \in \mathcal{O}[X]$ is called primitive if $f \not \equiv 0 \bmod \wp$.

Now we are able to formulate Hensel's Lemma. The statement together with a proof of it can be found in Theorem 4.8 of Chapter 2 in ibid.

### 4.2.7 Theorem. (Hensel's lemma)

Under the same conditions as in Definition 4.2.6 let $f \in \mathcal{O}[X]$ be a primitive polynomial. If there is some decomposition

$$
f \equiv \bar{g} \cdot \bar{h} \quad \bmod \wp
$$

into coprime polynomials $\bar{g}, \bar{h} \in \kappa[X]$, then there is a decomposition

$$
f=g \cdot h
$$

into polynomials $g, h \in \mathcal{O}[X]$ with $\operatorname{deg}(g)=\operatorname{deg}(\bar{g})$ and

$$
g \equiv \bar{g} \quad \bmod \wp \quad \text { and } h \equiv \bar{h} \quad \bmod \wp .
$$

4.2.8 Corollary. Let $p \in \mathbb{P}$ be a prime number, $f \in \mathbb{Z}_{p}[X]$ a polynomial and $\bar{f} \in \mathbb{F}_{p}[X]$ its reduced polynomial. If $\bar{f}$ has a simple root $\bar{a} \in \mathbb{F}_{p}\left(\right.$ i.e. $\bar{f}(\bar{a})=0$ and $\left.\bar{f}^{\prime}(\bar{a}) \neq 0\right)$, then there is a root $a \in \mathbb{Z}_{p}$ of $f$ and $a \equiv \bar{a} \bmod p$.

Proof. We obtain this statement as a direct consequence of Hensel's Lemma. First of all note that $f$ is primitive by assumption, otherwise no root of $\bar{f}$ could be simple. Since $\bar{a}$ is a simple root of $\bar{f}$ we have a decomposition

$$
\bar{f}=(X-\bar{a}) \cdot \bar{h}
$$

of $\bar{f}$ for some $\bar{h} \in \mathbb{F}_{p}[X]$ with $\bar{h}(\bar{a}) \neq 0$. So $\bar{h}$ and $\bar{g}:=(X-\bar{a}) \in \mathbb{F}_{p}[X]$ are coprime and Theorem 4.2.7 tells us that there is a decompositon

$$
f=g \cdot h
$$

into polynomials $g, h \in \mathbb{Z}_{p}[X]$ with $\operatorname{deg}(g)=\operatorname{deg}(\bar{g})=1$ and $g \equiv \bar{g} \bmod p$. Hence we can write

$$
g=a_{1} X+a_{0} \in \mathbb{Z}_{p}[X]
$$

with $a_{1} \equiv 1 \bmod p\left(\right.$ i.e. $\left.a_{1} \in \mathbb{Z}_{p} \backslash p \mathbb{Z}_{p}=\mathbb{Z}_{p}^{\times}\right)$and $a_{0} \equiv-\bar{a} \bmod p$. So for $a:=-\frac{a_{0}}{a_{1}} \in \mathbb{Z}_{p}$ we find

$$
f(a)=g(a) \cdot h(a)=0 \cdot h(a)=0
$$

and

$$
a \equiv-\frac{a_{0}}{a_{1}} \equiv-\frac{-\bar{a}}{1} \equiv \bar{a} \quad \bmod p .
$$

4.2.9 Lemma. There is $\sqrt{-7}$ in $\mathbb{Z}_{2}$.

Proof. First observe that we can't apply Corollary 4.2 .8 to $q:=X^{2}+7 \in \mathbb{Z}_{2}[X]$ since

$$
\bar{q}=X^{2}+\overline{7}=X^{2}+\overline{1}=(X-\overline{1})(X+\overline{1})=(X-\overline{1})^{2} \in \mathbb{F}_{2}[X]
$$

and hence its reduction has no simple root in $\mathbb{F}_{2}$. But $-7 \equiv 1 \bmod 2$, so -7 is a unit in $\mathbb{Z}_{2}$ and if there is a solution $a \in \mathbb{Z}_{2}$ of $X^{2}=-7$, then $a$ has to be a unit as well. Hence $a \equiv 1 \bmod 2$ and we can find $b \in \mathbb{Z}_{p}$ with $a=2 b+1$. So we can use the linear transformation $X \mapsto 2 X+1$ and try to find a root of

$$
r:=q(2 X+1)=(2 X+1)^{2}+7=4 X^{2}+4 X+8 \in \mathbb{Z}_{2}[X] .
$$

Equivalently we can try to find roots of

$$
p:=\frac{r}{4}=X^{2}+X+2 \in \mathbb{Z}_{2}[X],
$$

since 4 is not a zero divisor in $\mathbb{Z}_{2}$. The reduction of $p$ is given by

$$
\bar{p}=X^{2}+X=X(X+\overline{1}) \in \mathbb{F}_{2}[X] .
$$

So $\overline{0}$ and $\overline{1}$ are simple roots and both of them can be lifted by Corollary 4.2 .8 to roots $b_{1}, b_{2} \in \mathbb{Z}_{2}$.
4.2.10 Lemma. Let $K$ be a field. If $G$ is a finite subgroup of the multiplicative group $K^{\times}$, then $G$ is cyclic.

Proof. By assumption $G$ is a finite abelian group and hence in particular a finitely generated abelian group. So the fundamental theorem of finitely generated abelian groups tells us that

$$
G \cong \bigoplus_{i=1}^{d} \mathbb{Z} / e_{i} \mathbb{Z}
$$

for some $d \in \mathbb{N}$ and natural numbers $e_{1}, e_{2}, \ldots, e_{d}>2$, such that $e_{i}$ divides $e_{i+1}$ for every $i \in\{1, \ldots, d-1\}$. If we assume that $G$ is not cyclic, then $d \geq 2$ and

$$
\left\{(x, y, 0, \ldots, 0) \in \bigoplus_{i=1}^{d} \mathbb{Z} / e_{i} \mathbb{Z} \mid x \in \mathbb{Z} / e_{1} \mathbb{Z}, y \in \mathbb{Z} / e_{2} \mathbb{Z}\right\}
$$

corresponds to $e_{1} \cdot e_{2}$ elements in $G$, which are roots of $p=X^{e_{2}}-1 \in K[X]$. But this contradicts the fact that $p$ can only have $e_{2}$ roots in $K$, which is less than $e_{1} \cdot e_{2}$.
4.2.11 Corollary. Every element in a finite field $\mathbb{F}_{q}$ is the sum of two squares, i.e. for $a \in \mathbb{F}_{q}$ there are $b, c \in \mathbb{F}_{q}$ such that $a=b^{2}+c^{2}$.

Proof. First we want to treat the case $q=2^{n}$ for some $n \in \mathbb{N}$. Note that $\left|\mathbb{F}_{2^{n}}^{\times}\right|=2^{n}-1$. Hence for $a \in \mathbb{F}_{2^{n}}^{\times}$we find

$$
1=a^{2^{n}-1} \Longrightarrow a=a^{2^{n}}=\left(a^{2^{n-1}}\right)^{2}
$$

by Lagrange's theorem and actually $a$ itself is a square. Another way to treat this case is using surjectivity of the Frobenius automorphism

$$
\phi: \mathbb{F}_{2^{n}} \longrightarrow \mathbb{F}_{2^{n}}, x \longmapsto x^{2} .
$$

Now we can assume that $q=p^{n}$ for some odd prime $p \in \mathbb{P} \backslash\{2\}$ and $n \in \mathbb{N}$. We consider the two sets

$$
A:=\left\{x^{2} \mid x \in \mathbb{F}_{q}\right\} \text { and } B:=\left\{a-y^{2} \mid y \in \mathbb{F}_{q}\right\}
$$

for some fixed $a \in \mathbb{F}_{q}$. Our goal is to show that $|A|=|B| \geq \frac{q+1}{2}$, so we can conclude that $A$ and $B$ are not disjoint and hence the claim follows. The fact that $|A|=|B|$ is
obvious, so we have to see that $|A| \geq \frac{q+1}{2}$. Note that the group $\mathbb{F}_{q}^{\times}$is cyclic of order $q-1$ by Lemma 4.2.10. So there is a generator $g$ of $\mathbb{F}_{q}^{\times}$and can write $\mathbb{F}_{q}^{\times}=\left\{g, g^{2}, \ldots, g^{q-1}\right\}$. Since $q$ is odd, we have

$$
\{0\} \sqcup\left\{g^{2 n} \left\lvert\, n \in\left\{1, \ldots, \frac{q-1}{2}\right\}\right.\right\} \subseteq A
$$

and hence at least $\frac{q+1}{2}$ elements in $A$.
4.2.12 Lemma. The equation

$$
x_{1}^{2}+x_{2}^{2}+x_{3}^{2}+x_{4}^{2}=-1
$$

has a solution $\left(x_{p}, y_{p}, z_{p}, w_{p}\right) \in \mathbb{Z}_{p}^{4}$ for any prime $p \in \mathbb{P}$.
Proof. By Lemma 4.2 .9 we find $\sqrt{-7}$ in $\mathbb{Z}_{2}$, so $(2,1,1, \sqrt{-7}) \in \mathbb{Z}_{p}^{4}$ does the job for $p=2$. Hence we can assume that $p \neq 2$. Since we know that every element in $\mathbb{F}_{p}$ is a sum of two squares by Corollary 4.2.11, we can find elements $\bar{a}, \bar{b} \in \mathbb{F}_{p}$ with

$$
\bar{a}^{2}+\bar{b}^{2}=-1 .
$$

Without loss of generality we can assume that $\bar{a} \neq 0$. Hence the polynomial

$$
\bar{p}:=X^{2}+\bar{b}^{2}+1 \quad \in \mathbb{F}_{p}[X]
$$

has $\bar{a}$ as simple root which can be lifted by Corollary 4.2 .8 to a root $\tilde{a} \in \mathbb{Z}_{p}$ of the polynomial

$$
p:=X^{2}+b^{2}+1 \quad \in \mathbb{Z}_{p}[X] .
$$

So in this case $(\tilde{a}, b, 0,0) \in \mathbb{Z}_{p}^{4}$ does the job.
Now we want to introduce the group which is central for the rest of this section, namely the spin group $\operatorname{Spin}(V, Q)$ of a quadratic space $(V, Q)$. For that purpose, we need some basic notions and properties about quadratic spaces and their corresponding Clifford algebra. For a more detailed reading we refer to Chapter 2 and Chapter 10 of Cassels, 2008.

### 4.2.13 Definition. (Quadratic form and quadratic space)

Let $K$ be a field with $\operatorname{char}(K) \neq 2, I \subseteq K$ a subring and $n \in \mathbb{N}$.
a) A quadratic form over $K$ in $n$ variables is a homogeneous polynomial $q \in K\left[X_{1}, \ldots, X_{n}\right]$ of degree 2. Hence it can written as

$$
q(X):=q\left(X_{1}, \ldots, X_{n}\right)=\sum_{i, j=1}^{n} q_{i j} X_{i} X_{j}
$$

with $q_{i j}=q_{j i} \in K$ for $1 \leq i, j \leq n$. So $q$ can be seen as a map $K^{n} \longrightarrow K$ which maps $\left(k_{1}, \ldots, k_{n}\right)$ to $q\left(k_{1}, \ldots, k_{n}\right)$. Furthermore it corresponds to a symmetric matrix $A_{q}:=\left(q_{i j}\right)_{1 \leq i, j \leq n} \in K^{n \times n}$ which satisfies

$$
q(x)=x^{T} A_{q} x \quad \forall x \in K^{n} .
$$

b) Two quadratic forms $p, q \in K\left[X_{1}, \ldots, X_{n}\right]$ are said to be equivalent over $I$ if there is $C \in \mathrm{GL}_{n}(I)$ such that

$$
q(C x)=p(x) \quad \forall x \in K^{n} .
$$

This is equivalent to

$$
C^{T} A_{q} C=A_{p}
$$

if $A_{p}, A_{q} \in K^{n \times n}$ denote their corresponding matrices.
c) A quadratic space $(V, Q)$ over $K$ is a finite dimensional $K$-vector space $V$ with a symmetric bilinear form $Q: V \times V \longrightarrow K$. By abuse of notation we put

$$
Q(v):=Q(v, v)
$$

for every $v \in V$ and note that

$$
Q(u, v)=\frac{1}{4}(Q(u+v)-Q(u-v))
$$

The dimension of the quadratic space $(V, Q)$ is the dimension of the underlying vector space $V$.
d) Two quadratic spaces $\left(V_{1}, Q_{1}\right)$ and $\left(V_{2}, Q_{2}\right)$ over $K$ are called isometric if there is an isometry $\sigma: V_{1} \longrightarrow V_{2}$, which means that $\sigma$ is an isomorphism of $K$-vector spaces and satisfies

$$
Q_{2}(\sigma(v))=Q_{1}(v) \quad \forall v \in V_{1}
$$

e) The quadratic space $(V, Q)$ over $K$ is said to be regular, if the $K$-linear map

$$
\Phi: V \longrightarrow \operatorname{Hom}_{K}(V, K), v \longmapsto[\Phi(v): w \mapsto Q(v, w)]
$$

is an isomorphism.
4.2.14 Remark. a) Let $K$ be a field with $\operatorname{char}(K) \neq 2$ and $(V, Q)$ be a quadratic space over $K$ with basis $B:=\left\{v_{1}, \ldots, v_{n}\right\}$ of $V$. Then we find a quadratic form $q \in K\left[X_{1}, \ldots, X_{n}\right]$ corresponding to $(V, Q)$ by

$$
q\left(X_{1}, \ldots, X_{n}\right):=\sum_{i, j=1}^{n} Q\left(v_{i}, v_{j}\right) X_{i} X_{j}
$$

which satisfies

$$
q\left(k_{1}, \ldots, k_{n}\right)=Q\left(\sum_{i=1}^{n} k_{i} v_{i}\right) .
$$

Choosing another basis $C:=\left\{u_{1}, \ldots, u_{n}\right\}$ of $V$ we obtain another quadratic form

$$
\tilde{q}\left(X_{1}, \ldots, X_{2}\right):=\sum_{i, j=1}^{n} Q\left(u_{i}, u_{j}\right) X_{i} X_{j}
$$

but obviously $q$ and $\tilde{q}$ are equivalent over $K$ using the base change matrix $D_{C B}$. Furthermore every quadratic form $q=\sum_{i=1, \ldots, n} q_{i j} X_{i} X_{j} \in K\left[X_{1}, \ldots, X_{n}\right]$ with $q_{i j}=q_{j i}$ arises from a quadratic space $(V, Q)$ over $K$. To see this, let $V$ be any $n$-dimensional $K$-vector space with basis $\left\{v_{1}, \ldots, v_{n}\right\}$ and define a symmetric bilinear form $Q$ on $V$ by $Q\left(v_{i}, v_{j}\right)=q_{i j}$.
b) Let $\left(V_{1}, Q_{1}\right)$ and $\left(V_{2}, Q_{2}\right)$ be $n$-dimensional quadratic spaces over $K$. If there is an isometry $\sigma: V_{1} \longrightarrow V_{2}$, then obviously their corresponding quadratic forms $q_{1}$ with respect to a basis $B$ of $V_{1}$ and $q_{2}$ with respect to $\sigma(B)$ are equivalent over $K$. Conversely, if their corresponding equivalence classes of quadratic forms over $K$ are the same, then it is easy to find an isometry $\sigma: V_{1} \longrightarrow V_{2}$. Therefore two quadratic spaces over $K$ are isometric if and only if they correspond to the same equivalence class of quadratic forms over $K$.
c) If $U \leq V$ is a subspace, then $\left(U,\left.Q\right|_{U \times U}\right)$ is is quadratic space and we denote it by $(U, Q)$.

### 4.2.15 Definition. (Orthogonal complement and normal basis)

Let $(V, Q)$ be an $n$-dimensional quadratic space over $K$.
a) For a subspace $U \leq V$ we define the orthogonal complement of $U$ as

$$
U^{\perp}:=\{v \in V \mid Q(u, v)=0 \forall u \in U\} .
$$

Note that $U^{\perp}$ is a subspace of $V$.
b) A basis $\left\{v_{1}, \ldots, v_{n}\right\}$ of $V$ is said to be normal if $Q\left(v_{i}, v_{j}\right)=0$ for all $i, j \in\{1, \ldots, n\}$ with $i \neq j$.
4.2.16 Lemma. Let $(V, Q)$ be a quadratic space over $K$. If $U \leq V$ is a subspace such that $(U, Q)$ is regular, then $V=U \oplus U^{\perp}$.

Proof. Every $v \in V$ determines a $K$-linear map

$$
\lambda_{v}: U \longrightarrow K, u \mapsto Q(v, u) .
$$

By regularity of $(U, Q)$ we find some $w \in U$ with $\Phi(w)=[u \mapsto Q(w, u)]=\lambda_{v}$ which means that

$$
Q(w, u)=Q(v, u) \Longleftrightarrow Q(v-w, u)=0
$$

for every $u \in U$. Hence $v-w \in U^{\perp}$ and $v=w+(v-w)$. Furthermore $U \cap U^{\perp}=\{0\}$ since for every $0 \neq u \in U$ we find some $v \in U$ with $Q(u, v) \neq 0$ by regularity of $(U, Q)$.
4.2.17 Lemma. Every quadratic space has a normal basis.

Proof. We proceed by induction on the dimension of the quadratic space. Let $(V, Q)$ be a $n$-dimensional quadratic space over $K$. If $n=0$ the empty basis does the job, so we
can assume $n>0$. If $Q=0$ every basis is normal, so we can further assume that there are $v_{1}, v_{2} \in V$ with $Q\left(v_{1}, v_{2}\right) \neq 0$. Hence

$$
Q\left(v_{1}+v_{2}\right)=Q\left(v_{1}\right)+2 Q\left(v_{1}, v_{2}\right)+Q\left(v_{2}\right)
$$

and we can conclude that there is some $v \in V$ with $Q(v) \neq 0$. Now observe that $(\langle v\rangle, Q)$ is a regular quadratic space since the map $\Phi:\langle v\rangle \longrightarrow \operatorname{Hom}_{K}(\langle v\rangle, K)$ in Definition 4.2.13 e) is obviously an isomorphism. So by Lemma 4.2.16 we have $V=\langle v\rangle \oplus\langle v\rangle^{\perp}$ and $\operatorname{dim}_{K}\left(\langle v\rangle^{\perp}\right)=n-1$. Hence $\langle v\rangle^{\perp}$ admits a normal basis $\left\{v_{1}, \ldots, v_{n-1}\right\}$ by induction hypothesis and $\left\{v_{1}, \ldots, v_{n-1}, v\right\}$ is a normal basis of $(V, Q)$.

### 4.2.18 Definition. (Direct sum)

Let $\left(V, Q_{V}\right)$ and $\left(W, Q_{W}\right)$ be quadratic spaces over the same field $K$. The direct sum $\left(V, Q_{V}\right) \oplus\left(W, Q_{W}\right)$ is a quadratic space with underlying vector space $V \oplus W$ and the symmetric bilinear form is given by

$$
Q_{V \oplus W}\left(\left(v_{1}, w_{1}\right),\left(v_{2}, w_{2}\right)\right):=Q_{V}\left(v_{1}, v_{2}\right)+Q_{W}\left(w_{1}, w_{2}\right) .
$$

4.2.19 Remark. Under the same conditions as in Definition 4.2.18 let $A_{V}, A_{W}$ and $A_{V \oplus W}$ denote the corresponding matrices to the quadratic spaces. It is obvious that

$$
A_{V \oplus W}=\left(\begin{array}{cc}
A_{V} & 0 \\
0 & A_{W}
\end{array}\right)
$$

4.2.20 Definition. In the following we want to fix the quadratic forms

- $q_{1}:=X_{1}^{2}+X_{2}^{2}+X_{3}^{2}+X_{4}^{2}$,
- $q_{2}:=-q_{1}=-X_{1}^{2}-X_{2}^{2}-X_{3}^{2}-X_{4}^{2}$,
- $q_{m, n}:=\sum_{i=1}^{m} X_{i}^{2}-\sum_{i=m+1}^{m+n} X_{i}^{2} \quad\left(m, n \in \mathbb{N}_{0}\right)$
and corresponding quadratic spaces $\left(V_{1}, Q_{1}\right),\left(V_{2}, Q_{2}\right),\left(V_{m, n}, Q_{m, n}\right)$ over a given field $K$.
4.2.21 Lemma. The quadratic forms $q_{1}$ and $q_{2}$ are equivalent over $\mathbb{Z}_{p}$ for any prime $p \in \mathbb{P}$.

Proof. Let us fix some prime $p \in \mathbb{P}$ and a solution $\left(x_{p}, y_{p}, z_{p}, w_{p}\right) \in \mathbb{Z}_{p}^{4}$ of the equation $x_{1}^{2}+x_{2}^{2}+x_{3}^{2}+x_{4}^{2}=-1$, which exists by Lemma 4.2.12. Then the matrix

$$
C_{p}:=\left(\begin{array}{cccc}
x_{p} & y_{p} & z_{p} & w_{p} \\
-y_{p} & x_{p} & -w_{p} & z_{p} \\
-z_{p} & w_{p} & x_{p} & -y_{p} \\
-w_{p} & -z_{p} & y_{p} & x_{p}
\end{array}\right) \in \mathbb{Z}_{p}^{4 \times 4}
$$

satisfies

$$
C_{p}^{T} \cdot I_{4} \cdot C_{p}=C_{p}^{T} \cdot C_{p}=-I_{4} .
$$

Hence $C_{p} \in \mathrm{GL}_{4}\left(\mathbb{Z}_{p}\right)$ and $q_{1}$ and $q_{2}$ are equivalent, since $I_{4}$ and $-I_{4}$ are the corresponding matrices to the quadratic forms $q_{1}$ and $q_{2}$.
4.2.22 Corollary. Let $m, n \in \mathbb{N}_{0}$ and $m \geq 4$. Then the quadratic forms $q_{m, n}$ and $q_{m-4, n+4}$ are equivalent over $\mathbb{Z}_{p}$ for every prime $p \in \mathbb{P}$. Hence, if $K$ is any number field and $v$ a discrete valuation on $K$ with valuation ring $\mathcal{O}_{v}$ in the completion $K_{v}$ of $K$ with respect to $v$, then $q_{m, n}$ and $q_{m-4, n+4}$ are equivalent over $\mathcal{O}_{v}$.

Proof. Let $\left(V_{i}, Q_{i}\right)$ be a quadratic space associated with $q_{i}$ over $K_{v}(i=1,2)$ and ( $V_{m, n}, Q_{m, n}$ ) a quadratic space associated to $q_{m, n}$ over $K_{v}$. For the corresponding matrices $A_{i}$ of $\left(V_{i}, Q_{i}\right)$ and $A_{m, n}$ of $\left(V_{m, n}, Q_{m, n}\right)$ we find $A_{1}=I_{4}, A_{2}=-I_{4}$ and

$$
A_{m, n}=\left(\begin{array}{cc}
I_{m} & 0 \\
0 & -I_{n}
\end{array}\right) .
$$

By assumption we have $m \geq 4$ and using Remark 4.2.19 we see that

$$
\begin{aligned}
\left(V_{m, n}, Q_{m, n}\right) & \cong\left(V_{1}, Q_{1}\right) \oplus\left(V_{m-4, n}, Q_{m-4, n}\right) \quad \text { and } \\
\left(V_{m-4, n+4}, Q_{m-4, n+4}\right) & \cong\left(V_{2}, Q_{2}\right) \oplus\left(V_{m-4, n}, Q_{m-4, n}\right),
\end{aligned}
$$

where " $\cong$ " means isometric as quadratic spaces. Furthermore $\left(V_{1}, Q_{1}\right) \cong\left(V_{2}, Q_{2}\right)$ over $\mathbb{Z}_{p}$ since their corresponding quadratic forms are equivalent over $\mathbb{Z}_{p}$ by Lemma 4.2.21. Hence we can conclude that $\left(V_{m, n}, Q_{m, n}\right) \cong\left(V_{m-4, n+4}, Q_{m-4, n+4}\right)$ over $\mathbb{Z}_{p}$.

### 4.2.23 Definition. (Clifford algebra)

a) Let $(V, Q)$ be a quadratic space of dimension $n \in \mathbb{N}$ over a field $K$. We consider the category $\mathcal{C}(V, Q)$ of associative unital $K$-algebras $A$ in which $V$ is embedded by a $K$-linear map $j: V \longrightarrow A$, such that for every $v \in V$ we have

$$
j(v) \cdot j(v)=Q(v) \cdot 1_{A} .
$$

So the objects of our category are such pairs $(A, j)$ and morphisms between $\left(A_{1}, j_{1}\right)$ and $\left(A_{2}, j_{2}\right)$ are given by $K$-algebra homomorphisms $\phi: A_{1} \longrightarrow A_{2}$ such that the embeddings of $V$ are identified, which means that

$$
\phi \circ j_{1}=j_{2} .
$$

b) Any initial object $(C, c)$ of $\mathcal{C}(V, Q)$ is called Clifford algebra of $(V, Q)$ and we identify $V$ with its image under $c$. Furthermore since every initial object is unique up to unique isomorphisms, we will denote it by $\mathrm{Cl}(V, Q)$.
4.2.24 Lemma. Let $(V, Q)$ be a quadratic space of dimension $n \in \mathbb{N}$ over a field $K$ and $\left\{v_{i}\right\}_{i=1}^{n}$ a normal basis of $V$ with respect to $Q$. Then there is a Clifford algebra ( $C, c$ ) of $(V, Q)$ and if $e_{i}:=c\left(v_{i}\right)$ for every $i=1, \ldots, n$ we find

$$
B:=\left\{e_{I}:=e_{i_{1}} \cdot e_{i_{2}} \cdot \ldots \cdot e_{i_{k}} \mid I=\left\{i_{1}<i_{2}<\ldots<i_{k}\right\} \subseteq\{1,2, \ldots, n\}\right\}
$$

as $K$-basis of $C$. Hence it is of dimension $2^{n}$ as vector space over $K$.

Proof. Let

$$
T(V):=\bigoplus_{n \geq 0} V^{\otimes n}
$$

be the tensor algebra of $V$ and $(A, j)$ an arbitrary object in the category $\mathcal{C}(V, Q)$. The universal property of $T(V)$ gives us a unique $K$-algebra homomorphism $\phi: T(V) \longrightarrow A$ induced by the $K$-linear map $j: V \longrightarrow A$, which satisfies $\phi \circ i=j$ for the canonical $K$-linear embedding $i: V \longrightarrow T(V)$. Now observe that the kernel of $\phi$ contains the two-sided ideal

$$
I(V, Q):=\langle\{v \otimes v-Q(v) \mid v \in V\}\rangle,
$$

so it factorises over the canonical projection $p: T(V) \longrightarrow T(V) / I(V, Q)=: C$ and induces a $K$-algebra homomorphism $\bar{\phi}: C \longrightarrow A$ with $\bar{\phi} \circ p=\phi$. Note that the $K$-linear map

$$
c: V \xrightarrow{i} T(V) \xrightarrow{p} C
$$

is still injective and satisfies

$$
c(v) \cdot c(v)=(v \otimes v)+I(V, Q)=Q(v)+I(V, Q)
$$

so $(C, c)$ is an object in $\mathcal{C}(V, Q)$. Furthermore $\bar{\phi}$ is a morphism in $\mathcal{C}(V, Q)$, since

$$
\bar{\phi} \circ c=\bar{\phi} \circ p \circ i=\phi \circ i=j .
$$

To see that $\bar{\phi}$ is unique, note that the requirement $\psi \circ c=j$ gives $\psi(v+I(V, Q))=j(v)$ for every $v \in V$ and since $\{v+I(V, Q) \mid v \in V\}$ generates $C$ as $K$-algebra, we can conclude that $\psi=\bar{\phi}$. Now let us choose a normal basis $\left\{v_{1}, \ldots, v_{n}\right\}$ of $V$ with respect to $Q$. So we can define

- $e_{i}:=c\left(v_{i}\right)=v_{i}+I(V, Q) \in C$ for $i=1, \ldots, n$,
- $e_{I}:=e_{i_{1}} \cdot \ldots \cdot e_{i_{k}}$ for $I=\left\{i_{1}<i_{2}<\ldots i_{k}\right\} \subseteq\{1,2, \ldots, n\}$ with $e_{\emptyset}=1$.

By construction of $C$ we find for $i, j=1, \ldots, n$ the relations

$$
\begin{gather*}
e_{i} \cdot e_{i}=Q\left(v_{i}\right)  \tag{4}\\
e_{i} \cdot e_{j}+e_{j} \cdot e_{i}=0 \quad(i \neq j) \tag{5}
\end{gather*}
$$

since

$$
e_{i} e_{j}+e_{j} e_{i}=\left(e_{i}+e_{j}\right)^{2}-e_{i}^{2}-e_{j}^{2}=Q\left(v_{i}+v_{j}\right)-Q\left(v_{i}\right)-Q\left(v_{j}\right)=0 .
$$

We already convinced ourselves, that $C$ is generated by $\left\{e_{i}\right\}_{i=1}^{n}$ as $K$-algebra. Hence, every element in $C$ can be expressed as finite sum of finite products of those $e_{i}$ 's. Now we can use the relations (4) and (5) to see that $C$ is generated by $B=\left\{e_{I} \mid I \subseteq\{1, \ldots, n\}\right\}$ as $K$-vector space, since relation (5) allows us to arrange the generators in a product in increasing order and relation (4) allows us to reduce their power to 1 . It remains to show $B$ is linearly independent over $K$. A proof of this can be found in Chapter 19 of Lang, 2004 (see Theorem 4.1).
4.2.25 Remark. Let $(V, Q)$ be a quadratic space over a field $K$. Then the antiautomorphism

$$
\alpha: T(V) \longrightarrow T(V), v_{1} \otimes v_{2} \otimes \cdots \otimes v_{n} \longmapsto v_{n} \otimes \cdots \otimes v_{2} \otimes v_{1}
$$

of the tensor algebra $T(V)$ keeps the two-sided ideal $I(V, Q)=\langle\{v \otimes v-Q(V) \mid v \in V\}$ invariant, so it descends to an anti-automorphism ' $: ~ \mathrm{Cl}(V, Q) \longrightarrow \mathrm{Cl}(V, Q)$ which makes the following diagram commute, where $p: T(V) \longrightarrow \mathrm{Cl}(V, Q)$ is the canonical projection factoring out $I(V, Q)$ as in the proof of Lemma 4.2.24.


### 4.2.26 Definition. (Even Clifford algebra and spin group)

Let $(V, Q)$ be a quadratic space of dimension $n \in \mathbb{N}$ over a field $K$.
a) If $\left\{e_{I} \mid I \subseteq\{1, \ldots, n\}\right\}$ is the basis of $\mathrm{Cl}(V, Q)$ corresponding to a normal basis $\left\{e_{1}, \ldots, e_{n}\right\}$ of $(V, Q)$, then the even Clifford algebra of $(V, Q)$ is the subalgebra of $\mathrm{Cl}(V, Q)$ generated by

$$
\left\{e_{I}|I \subseteq\{1, \ldots, n\},|I| \text { even }\}\right.
$$

and we denote it by $\mathrm{Cl}^{0}(V, Q)$.
b) The spin group of $(V, Q)$ is the subgroup

$$
\operatorname{Spin}(V, Q):=\left\{x \in \mathrm{Cl}^{0}(V, Q)^{\times} \mid x x^{\prime}=1, x V x^{\prime} \subseteq V\right\}
$$

in the group of invertible elements of the even Clifford algebra $\mathrm{Cl}^{0}(V, Q)$.
c) Let $m, n \in \mathbb{N}_{0}$. For a given field $K$ and corresponding quadratic space $\left(V_{m, n}, Q_{m, n}\right)$ we want to introduce the notation

$$
C_{m, n}:=\mathrm{Cl}\left(V_{m, n}, Q_{m, n}\right), C_{m, n}^{0}:=\mathrm{Cl}^{0}\left(V_{m, n}, Q_{m, n}\right) \text { and } G_{m, n}:=\operatorname{Spin}\left(V_{m, n}, Q_{m, n}\right) .
$$

4.2.27 Remark. Let $(V, Q)$ be a quadratic space of dimension $n \in \mathbb{N}$ over a field $K \subseteq \mathbb{C}$.
a) For every $y \in \operatorname{Spin}(V, Q)$ we find the $K$-linear map

$$
r_{y}: \mathrm{Cl}^{0}(V, Q) \longrightarrow \mathrm{Cl}^{0}(V, Q), x \longmapsto x y
$$

whose inverse is given by $r_{y^{-1}}$. Hence we obtain a group homomorphism

$$
\tilde{\rho}: \operatorname{Spin}(V, Q) \longrightarrow \operatorname{GL}\left(\mathrm{Cl}^{0}(V, Q)\right), y \longmapsto r_{y}
$$

which turns out to be a faithful irreducible linear representation of $\operatorname{Spin}(V, Q)$. Using the basis $E:=\left\{e_{I}|I \subseteq\{1, \ldots, n\},|I|\right.$ even $\}$ of $\mathrm{Cl}^{0}(V, Q)$ corresponding to a normal basis $\left\{e_{1}, \ldots, e_{n}\right\}$ of $(V, Q)$, we obtain another faithful irreducible linear representation

$$
\rho: \operatorname{Spin}(V, Q) \xrightarrow{\tilde{\rho}} \mathrm{GL}\left(\mathrm{Cl}^{0}(V, Q)\right) \xrightarrow{\Phi_{E}} \mathrm{GL}_{2^{n-1}}(\mathbb{C}),
$$

if $\Phi_{E}$ assigns to each automorphism $\alpha$ its transformation matrix $D_{E E}(\alpha)$ corresponding to $E$.
b) In case that $(V, Q)=\left(V_{m, n}, Q_{m, n}\right)$ for some $m, n \in \mathbb{N}_{0}$ we fix a normal basis $\left\{e_{1}, \ldots, e_{m+n}\right\}$ of $\left(V_{m, n}, Q_{m, n}\right)$ throughout this chapter, which satisfies

$$
Q_{m, n}\left(e_{i}\right)= \begin{cases}1 & \text { if } 1 \leq i \leq m \\ -1 & \text { if } m+1 \leq i \leq m+n\end{cases}
$$

so that we obtain a corresponding fixed basis $E_{m, n}$ of $C_{m, n}^{0}$ over $K$. Now a) tells us that we actually fixed a faithful irreducible linear representation

$$
\rho_{m, n}: G_{m, n} \xrightarrow{\tilde{\rho}_{m, n}} \mathrm{GL}\left(C_{m, n}^{0}\right) \xrightarrow{\Phi_{E_{m, n}}} \mathrm{GL}_{2^{m+n-1}}(\mathbb{C})
$$

and we want to identify $G_{m, n}$ with its image under $\rho_{m, n}$.

### 4.2.28 Definition. (Algebraic group and group of $R$-points)

a) An algebraic group is a subgroup of $\mathrm{GL}_{n}(\mathbb{C})$ which is closed in the Zariski topology. We consider $\mathrm{GL}_{n}(\mathbb{C})$ as Zariski closed subset of $\mathbb{C}^{(n+1) \times(n+1)}$ using the embedding

$$
\mathrm{GL}_{n}(\mathbb{C}) \longrightarrow \mathbb{C}^{(n+1) \times(n+1)}, g \longmapsto\left(\begin{array}{cc}
g & 0 \\
0 & \operatorname{det}(g)^{-1}
\end{array}\right)
$$

and see that its image can be described as the zero-locus of

$$
S:=\left\{X_{i, n+1}\right\}_{i=1, \ldots, n} \cup\left\{X_{n+1, i}\right\}_{i=1, \ldots, n} \cup\left\{X_{n+1, n+1} \cdot \operatorname{det}\left(\left(X_{i, j}\right)_{i, j=1, \ldots, n}\right)-1\right\}
$$

and hence the coordinate ring of $\mathrm{GL}_{n}(\mathbb{C})$ is given by

$$
A:=\mathbb{C}\left[\left\{X_{i, j}\right\}_{i, j=1, \ldots, n+1}\right] /\langle S\rangle \cong \mathbb{C}\left[X_{1,1}, X_{1,2}, \ldots, X_{n, n}, \operatorname{det}\left(\left(X_{i, j}\right)_{i, j=1, \ldots, n}\right)^{-1}\right]
$$

b) We say an algebraic group $G \leq \mathrm{GL}_{n}(\mathbb{C})$ is defined over a subfield $K \subseteq \mathbb{C}$, if the ideal $I(G):=\{p \in A \mid p(g)=0 \forall g \in G\}$ is generated by $I(G)_{K}:=I(G) \cap A_{K}$, where $A_{K}:=K\left[X_{1,1}, X_{1,2}, \ldots, X_{n, n}, \operatorname{det}\left(\left(X_{i, j}\right)_{i, j=1, \ldots, n}\right)^{-1}\right]$.
c) Let $G \leq \mathrm{GL}_{n}(\mathbb{C})$ an algebraic group and $R \subseteq \mathbb{C}$ a subring. Then we call

$$
G(R):=G \cap \mathrm{GL}_{n}(R)
$$

the group of $R$-points of $G$.
4.2.29 Corollary. Let $m>4$ and $n>0$ natural numbers, $K$ be a number field and $v$ a discrete valuation on $K$ with corresponding valuation ring $\mathcal{O}_{v}$ in the completion $K_{v}$ of $K$ with respect to $v$. Then

$$
G_{m, n}\left(\mathcal{O}_{v}\right) \cong G_{m-4, n+4}\left(\mathcal{O}_{v}\right)
$$

Proof. Let $\tilde{m}:=m-4, \tilde{n}:=n+4$ and $E:=\left\{e_{1}, \ldots, e_{m+n}\right\}$ be our fixed basis of the quadratic space $\left(V_{m, n}, Q_{m, n}\right)$ associated with $q_{m, n}$ over $K_{v}$ which satisfies

$$
Q_{m, n}\left(e_{i}\right)= \begin{cases}1 & \text { if } 1 \leq i \leq m \\ -1 & \text { if } m+1 \leq i \leq m+n\end{cases}
$$

By Corollary 4.2.22 we know that there is a normal basis $F:=\left\{f_{i}\right\}_{i=1}^{m+n}$ of $\left(V_{m, n}, Q_{m, n}\right)$ with

$$
Q_{m, n}\left(f_{i}\right)= \begin{cases}1 & \text { if } 1 \leq i \leq \tilde{m}  \tag{6}\\ -1 & \text { if } \tilde{m}+1 \leq i \leq \tilde{m}+\tilde{n}\end{cases}
$$

and the base change matrix $D_{F E}$ and its inverse $D_{E F}$ have entries in $\mathbb{Z}_{p}$. Note that the two normal bases $E$ and $F$ give rise to two bases $\widetilde{E}, \widetilde{F}$ of $C_{m, n}^{0}$ and induce two embeddings

$$
\Phi_{\widetilde{E}}, \Phi_{\widetilde{F}}: \mathrm{GL}\left(C_{m, n}^{0}\right) \hookrightarrow \mathrm{GL}_{2^{m+n-1}}(\mathbb{C})
$$

Furthermore the base change matrices $D_{F E}$ and $D_{E F}$ induce base change matrices $D_{\widetilde{F} \widetilde{E}}, D_{\widetilde{E} \widetilde{F}} \in \mathrm{GL}_{m+n}\left(K_{v}\right)$. Using relation (4) and (5) in the proof of Lemma 4.2.24. the fact that $D_{F E}, D_{E F}$ have entries in $\mathbb{Z}_{p}$ and that $q_{m, n}, q_{\tilde{m}, \tilde{n}}$ have coefficients in $\mathbb{Z}_{p}$, one sees that $D_{\widetilde{F} \widetilde{E}}$ and $D_{\widetilde{E} \widetilde{F}}$ actually have entries in $\mathbb{Z}_{p}$ as well. Now let

$$
\kappa: \mathrm{GL}_{2^{m+n-1}}(\mathbb{C}) \longrightarrow \mathrm{GL}_{2^{m+n-1}}(\mathbb{C}), A \longmapsto D_{\widetilde{F} \widetilde{E}} A D_{\widetilde{E} \widetilde{F}}
$$

and observe that $\kappa\left(\mathrm{GL}_{2^{m+n-1}}\left(\mathcal{O}_{v}\right)\right) \subseteq \mathrm{GL}_{2^{m+n-1}}\left(\mathcal{O}_{v}\right)$ since $D_{\widetilde{\tilde{F}} \widetilde{ }}, D_{\widetilde{E} \widetilde{F}} \in \mathrm{GL}_{2^{m+n-1}}\left(\mathbb{Z}_{p}\right)$. Furthermore $\kappa$ is an automorphism and for $\tilde{\rho}_{m, n}$ as in Remark 4.2 .27 b ), commutativity of

tells us that

$$
\left.\kappa\right|_{G_{m, n}\left(\mathcal{O}_{v}\right)}: G_{m, n}\left(\mathcal{O}_{v}\right) \xrightarrow{\sim} \Phi_{\widetilde{F}}\left(\tilde{\rho}_{m, n}\left(G_{m, n}\right)\right) \cap \operatorname{GL}_{2^{m+n-1}}\left(\mathcal{O}_{v}\right)
$$

is an isomorphism. Now let $G:=\left\{g_{i}\right\}_{i=1}^{\tilde{m}+\tilde{n}}$ be the fixed basis of $\left(V_{\tilde{m}, \tilde{n}}, Q_{\tilde{m}, \tilde{n}}\right)$ which satisfies

$$
Q_{\tilde{m}, \tilde{n}}\left(g_{i}\right)= \begin{cases}1 & \text { if } 1 \leq i \leq \tilde{m}  \tag{7}\\ -1 & \text { if } \tilde{m}+1 \leq i \leq \tilde{m}+\tilde{n}\end{cases}
$$

and $\widetilde{G}$ its corresponding basis on $C_{\tilde{m}, \tilde{n}}^{0}$. By comparing the equations (6) and (7) we can convince ourselves that

$$
\Phi_{\widetilde{G}}\left(\tilde{\rho}_{\tilde{m}, \tilde{n}}\left(G_{\tilde{m}, \tilde{n}}\right)\right)=\Phi_{\widetilde{F}}\left(\tilde{\rho}_{m, n}\left(G_{m, n}\right)\right),
$$

since the matrices obtained by these linear representations are only depending on the relations $f_{i}^{2}=Q_{m, n}\left(f_{i}\right)$ and $g_{i}^{2}=Q_{\tilde{m}, \tilde{n}}\left(g_{i}\right)$ for $i=1, \ldots, m+n$. So

$$
G_{\tilde{m}, \tilde{n}}\left(\mathcal{O}_{v}\right)=\Phi_{\widetilde{G}}\left(\tilde{\rho}_{\tilde{m}, \tilde{n}}\left(G_{\tilde{m}, \tilde{n}}\right)\right) \cap \operatorname{GL}_{2^{m+n-1}}\left(\mathcal{O}_{v}\right)=\Phi_{\widetilde{F}}\left(\tilde{\rho}_{m, n}\left(G_{m, n}\right)\right) \cap \mathrm{GL}_{2^{m+n-1}}\left(\mathcal{O}_{v}\right),
$$

which proves the claim.
4.2.30 Remark. Let $m, n \in \mathbb{N}_{0}, K \subseteq \mathbb{C}$ a number field and ( $V_{m, n}, Q_{m, n}$ ) its corresponding quadratic space. Then $G_{m, n} \leq \mathrm{GL}_{2^{m+n-1}}(\mathbb{C})$ is known to be an almost simple and absolutely simple algebraic group defined over $\mathbb{Q}$.

### 4.2.31 Definition. (Place)

a) Two absolute values $|\cdot|_{1},|\cdot|_{2}$ on a field $K$ are said to be equivalent if there is a real number $s>0$ with $|x|_{1}=|x|_{2}^{s}$ for every $x \in K$.
b) The equivalence class of an absolute value $|\cdot|$ on $K$ is called a place on $K$ and it is called non-archimedean (or finite) if $|\cdot|$ is non-archimedean. Otherwise it is called archimedean (or infinite).
4.2.32 Remark. Let $K \subseteq \mathbb{C}$ be a number field, $\mathcal{O}_{K}$ its ring of integers, $n \in \mathbb{N}$ a natural number, $G \subseteq \mathrm{GL}_{n}(K)$ an algebraic group over $K$ and consider $\Gamma:=G\left(\mathcal{O}_{K}\right)$. Besides its profinite topology we can consider the congruence topology on $\Gamma$, for which a fundamental system of neighborhoods of the identity is given by set

$$
\mathcal{M}:=\left\{\Gamma(\mathfrak{a}) \mid 0 \neq \mathfrak{a} \unlhd \mathcal{O}_{K}\right\}
$$

of congruence subgroups

$$
\Gamma(\mathfrak{a}):=\{g \in \Gamma \mid g \equiv I \quad \bmod \mathfrak{a}\}
$$

for nonzero ideals $\mathfrak{a} \unlhd \mathcal{O}_{K}$ (see section 5 in Chapter 9 of Platonov and Rapinchuk, 1992). They are normal and of finite index in $\Gamma$ as kernels of the group homomorphism $\Phi_{\mathfrak{a}}: \Gamma \longrightarrow \mathrm{GL}_{n}\left(\mathcal{O}_{K} / \mathfrak{a}\right)$ obtained by restricting the canonical group homomorphisms $\mathrm{GL}_{n}\left(\mathcal{O}_{K}\right) \longrightarrow \mathrm{GL}_{n}\left(\mathcal{O}_{K} / \mathfrak{a}\right)$ to $\Gamma$. So $\mathcal{M} \subseteq \mathcal{N}_{\Gamma}$ and we have $\bigcap_{0 \neq \mathfrak{a} \leq \mathcal{O}_{K}} \Gamma(\mathfrak{a})=I$. According to Humphreys, 2006 (see section 5 in Chapter 16) there is a completion $\bar{\Gamma}$ of $\Gamma$ with respect to this topology, which is given by

$$
\bar{\Gamma}=\lim _{\check{0}{ }_{0 \neq \mathfrak{a} \leq \mathcal{O}_{K}} \Gamma / \Gamma(\mathfrak{a}), ~}^{\text {, }}
$$

if we endow each $\Gamma / \Gamma(\mathfrak{a})$ with its discrete topology. Now we have a family of compatible continuous group homomorphisms $\widehat{\Gamma}=\lim _{\underset{\leftarrow}{ } \in \mathcal{N}_{\Gamma}} \Gamma / N \longrightarrow \Gamma / \Gamma(\mathfrak{a})$ which are all surjective, so by Corollary 3.1.7 the induced map $\pi: \widehat{\Gamma} \longrightarrow \bar{\Gamma}$ is surjective. The kernel of this map is called congruence kernel of $G$ and denoted by $C(G)$. Hence we obtain a short exact sequence

$$
1 \longrightarrow C(G) \longrightarrow \widehat{\Gamma} \longrightarrow \bar{\Gamma} \longrightarrow 1
$$

Now let $\Gamma\left(\mathcal{O}_{K} / \mathfrak{a}\right):=\operatorname{Im}\left(\Phi_{\mathfrak{a}}\right)$ and $\Gamma\left(\widehat{\mathcal{O}_{K}}\right):=\lim _{\underset{0}{ } \neq a \leq \mathcal{O}_{K}} \Gamma\left(\mathcal{O}_{K} / \mathfrak{a}\right)$. Then the maps $\Phi_{\mathfrak{a}}$ induce compatible isomorphisms $\Gamma / \Gamma(\mathfrak{a}) \xrightarrow{\sim} \Gamma\left(\mathcal{O}_{K} / \mathfrak{a}\right)$ and since lim is a functor we get $\bar{\Gamma} \cong \Gamma\left(\widehat{\mathcal{O}_{K}}\right)$. Using the fact that the profinite completion $\widehat{\mathcal{O}_{K}}:=\lim _{0 \neq \mathfrak{a} \unlhd_{f} \mathcal{O}_{K}} \mathcal{O}_{K} / \mathfrak{a}$ of $\mathcal{O}_{K}$ is isomorphic to $\prod_{v \in V_{f}^{K}} \mathcal{O}_{v}$ (see example 1.7 in Koch, 2013), where $V_{f}^{K}$ denotes the set of finite places of $K$ and $\mathcal{O}_{v}$ the ring of integers in the completion $K_{v}$ of $K$ with respect to $v$, one checks that $\Gamma\left(\widehat{\mathcal{O}_{K}}\right) \cong \prod_{v \in V_{f}^{K}} \Gamma\left(\mathcal{O}_{v}\right)$ and hence we obtain a short exact sequence

$$
1 \longrightarrow C(G) \longrightarrow \widehat{\Gamma} \longrightarrow \prod_{v \in V_{f}^{K}} \Gamma\left(\mathcal{O}_{v}\right) \longrightarrow 1
$$

In order to proof Theorem 4.2.35 we will need the fact that $G_{m, n}\left(\mathcal{O}_{v}\right)$ is residually finite, which is a direct consequence of Malcev's theorem. A proof of it can be found in Nica, 2013.

### 4.2.33 Definition. (Linear group)

A group $G$ is called linear if it is isomorphic to a subgroup of $\mathrm{GL}_{n}(K)$ for some field $K$ and some $n \in \mathbb{N}$.

### 4.2.34 Theorem. (Malcev's theorem)

A finitely generated linear group is residually finite.
4.2.35 Theorem. Let $K:=\mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{N}$ square free and $\mathcal{O}_{K}$ its ring of integers. For some fixed natural number $n \geq 6$ let

$$
\Gamma:=G_{1, n}\left(\mathcal{O}_{K}\right) \quad \text { and } \quad \Lambda:=G_{5, n-4}\left(\mathcal{O}_{K}\right)
$$

a) Then there are finite index subgroups $\Gamma_{0} \leq \Gamma$ and $\Lambda_{0} \leq \Lambda$ with isomorphic profinite completions $\widehat{\Gamma_{0}} \cong \widehat{\Lambda_{0}}$.
b) We have

$$
b_{p}^{(2)}\left(\Gamma_{0}\right) \neq 0 \Longleftrightarrow p=n \text { and } n \text { even }
$$

and

$$
b_{p}^{(2)}\left(\Lambda_{0}\right) \neq 0 \Longleftrightarrow p=5 n-20 \text { and } n \text { even } .
$$

Proof. a) Let $\sigma_{1}, \sigma_{2}: K \hookrightarrow \mathbb{R}$ be the two distinct embeddings of $K$ into $\mathbb{R}$. Furthermore, let $G_{1}:=G_{n, 1}$ and $G_{2}:=G_{n-4,5}$ over $K$ together with the fixed representations $\rho_{i}: G_{i} \longrightarrow \mathrm{GL}_{2^{n}}(K)$. Note that the embeddings $\sigma_{1}$ and $\sigma_{2}$ induce embeddings

$$
\widehat{\sigma}_{i, 1}, \widehat{\sigma}_{i, 2}: G_{i}\left(\mathcal{O}_{K}\right) \hookrightarrow G_{i}(\mathbb{R})
$$

for $i=1,2$. Now let us embed diagonally

$$
\widehat{\sigma}_{1,1} \times \widehat{\sigma}_{1,2}: \Gamma:=G_{1}\left(\mathcal{O}_{K}\right) \longrightarrow G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})
$$

and

$$
\widehat{\sigma}_{2,1} \times \widehat{\sigma}_{2,2}: \Lambda:=G_{2}\left(\mathcal{O}_{K}\right) \longrightarrow G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})
$$

By Corollary 4.2.29 we know that $G_{1}\left(\mathcal{O}_{v}\right) \cong G_{2}\left(\mathcal{O}_{v}\right)$ for any discrete valuation $v$ on $K$ with valuation ring $\mathcal{O}_{v}$ in the completion $K_{v}$ of $K$ with respect to $v$. So there is an isomorphism

$$
\Phi: \prod_{v \in V_{f}^{K}} G_{1}\left(\mathcal{O}_{v}\right) \xrightarrow{\sim} \prod_{v \in V_{f}^{K}} G_{2}\left(\mathcal{O}_{v}\right)
$$

where $V_{f}^{K}$ denotes the set of all finite places of $K$. In Kneser, 1979 it is shown that the congruence kernel of $G_{2}$ is trivial and the congruence kernel of $G_{1}$ is of size 1 or 2. Hence the discussion of Remark 4.2.32 implies that

$$
\widehat{\Lambda}=\widehat{G_{2}\left(\mathcal{O}_{K}\right)} \cong \prod_{v \in V_{f}^{K}} G_{2}\left(\mathcal{O}_{v}\right)
$$

with isomorphism $\pi_{2}: \widehat{\Lambda} \longrightarrow \prod_{v \in V_{f}^{K}} G_{2}\left(\mathcal{O}_{v}\right)$ and $\widehat{\Gamma}$ fits into a short exact sequence

$$
1 \longrightarrow C \longrightarrow \widehat{\Gamma} \xrightarrow{\pi_{1}} \prod_{v \in V_{f}^{K}} G_{1}\left(\mathcal{O}_{v}\right) \longrightarrow 1
$$

with a finite group $C$. We remember that the intersection of all normal open subgroups of a profinite group is trivial (cf. Theorem 3.2.7), so by finiteness of $C$ we can find a normal open subgroup of $\widehat{\Gamma}$ which intersects $C$ trivially and hence injects into $\prod_{v \in V_{f}^{K}} G_{1}\left(\mathcal{O}_{v}\right)$. As $\Gamma$ is finitely generated (see Theorem 5.1 in Chapter 5 of Platonov and Rapinchuk, 1992) and linear, Malcev's theorem (cf. Theorem 4.2.34) tells us that $\Gamma$ is residually finite and by Proposition 3.2 .13 the subgroup we found is of the form $\overline{\Gamma_{0}}$ for some open subgroup $\Gamma_{0} \leq \Gamma$. Since $\Gamma_{0}$ is open in $\Gamma$, Lemma 3.2.19 tells us that the profinite topology on $\Gamma_{0}$ is induced by the profinite topology on $\Gamma$ and by Corollary 3.2 .18 we conclude that $\widehat{\Gamma_{0}} \cong \overline{\Gamma_{0}}$. Now let

$$
\Psi:=\pi_{2}^{-1} \circ \Phi \circ \pi_{1}: \widehat{\Gamma} \longrightarrow \widehat{\Lambda} .
$$

and consider the subgroup $\Psi\left(\overline{\Gamma_{0}}\right) \leq \widehat{\Lambda}$, which is normal and of finite index by surjectivity of $\Psi$. Since $\overline{\Gamma_{0}}$ is closed in the compact group $\widehat{\Gamma}$, it is compact itself and its image under the continuous map $\Psi$ is compact as well. Therefore $\Psi\left(\overline{\Gamma_{0}}\right)$ is a compact subset of the Hausdorff space $\widehat{\Lambda}$ and hence closed. Together with the fact that it is of finite index, we can conclude that $\Psi\left(\overline{\Gamma_{0}}\right)$ is open in $\widehat{\Lambda}$. So, by the same argument as before, it is of the form $\overline{\Lambda_{0}}$ for some open subgroup $\Lambda_{0} \leq \Lambda$ and $\widehat{\Lambda_{0}} \cong \overline{\Lambda_{0}}$. Hence $\left.\Psi\right|_{\overline{\Gamma_{0}}}$ induces a continuous group homomorphism $\widehat{\Gamma_{0}} \longrightarrow \widehat{\Lambda_{0}}$ which has to be open, since $\widehat{\Gamma_{0}}$ and $\widehat{\Lambda_{0}}$ are compact Hausdorff spaces. This proves that $\widehat{\Gamma_{0}}$ and $\widehat{\Lambda_{0}}$ are isomorphic as topological groups and finally the claim.
b) Note that the embedding $\widehat{\sigma}_{1,1} \times \widehat{\sigma}_{1,2}$ (resp. $\widehat{\sigma}_{2,1} \times \widehat{\sigma}_{2,2}$ ) realises $\Gamma$ (resp. $\Lambda$ ) as lattice in the connected semisimple Lie group $G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\left(\right.$ resp. $\left.G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right)$. Since $\Gamma_{0} \leq \Gamma$ and $\Lambda_{0} \leq \Lambda$ are finite index subgroups, we can find $\Lambda_{0}$ (resp. $\Gamma_{0}$ ) as lattice in $G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\left(\right.$ resp. $\left.G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right)$ as well. Hence we can use Lemma 2.3.8 to find their non-vanishing $L^{2}$-Betti numbers. The maximal compact subgroup of $G_{1}(\mathbb{R})=$ $G_{1, n}(\mathbb{R})\left(\right.$ resp. $\left.G_{2}(\mathbb{R})=G_{5, n-4}(\mathbb{R})\right)$ is $K_{1}:=\mathrm{SO}(n)\left(\right.$ resp. $\left.K_{2}:=\mathrm{SO}(5) \times \mathrm{SO}(n-4)\right)$. So we can calculate

$$
\begin{aligned}
\operatorname{dim}\left(\left(G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\right) /\left(K_{1} \times K_{1}\right)\right) & =\operatorname{dim}\left(G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\right)-\operatorname{dim}\left(K_{1} \times K_{1}\right) \\
& =2 \operatorname{dim}\left(G_{1}(\mathbb{R})\right)-2 \operatorname{dim}\left(K_{1}\right) \\
& =2 \operatorname{dim}(\mathrm{SO}(n+1))-2 \operatorname{dim}(\mathrm{SO}(n)) \\
& =2 \frac{n(n+1)}{2}-2 \frac{(n-1) n}{2} \\
& =2 n, \\
\operatorname{dim}\left(\left(G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right) /\left(K_{2} \times K_{2}\right)\right) & =\operatorname{dim}\left(G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right)-\operatorname{dim}\left(K_{2} \times K_{2}\right) \\
& =2 \operatorname{dim}\left(G_{2}(\mathbb{R})\right)-2 \operatorname{dim}\left(K_{2}\right) \\
& =2 \operatorname{dim}(\mathrm{SO}(n+1))-2 \operatorname{dim}(\mathrm{SO}(5) \times \operatorname{SO}(n-4)) \\
& =2 \frac{n(n+1)}{2}-2\left(\frac{4 \cdot 5}{2}+\frac{(n-5)(n-4)}{2}\right) \\
& =10 n-40,
\end{aligned}
$$

and

$$
\begin{aligned}
\delta\left(G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\right) & =\operatorname{rank}_{\mathbb{C}}\left(G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\right)-\operatorname{rank}_{\mathbb{C}}\left(K_{1} \times K_{1}\right) \\
& =2 \operatorname{rank}_{\mathbb{C}}\left(G_{1}(\mathbb{R})\right)-2 \operatorname{rank}_{\mathbb{C}}\left(K_{1}\right) \\
& =2 \operatorname{rank}_{\mathbb{C}}(\mathrm{SO}(n+1))-2 \operatorname{rank}_{\mathbb{C}}(\mathrm{SO}(n)) \\
& =2\left\lfloor\frac{n+1}{2}\right\rfloor-2\left\lfloor\frac{n}{2}\right\rfloor, \\
\delta\left(G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right) & =\operatorname{rank}_{\mathbb{C}}\left(G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right)-\operatorname{rank}_{\mathbb{C}}\left(K_{2} \times K_{2}\right) \\
& =2 \operatorname{rank}_{\mathbb{C}}\left(G_{2}(\mathbb{R})\right)-2 \operatorname{rank}_{\mathbb{C}}\left(K_{2}\right) \\
& =2 \operatorname{rank}_{\mathbb{C}}(\mathrm{SO}(n+1))-2 \operatorname{rank}_{\mathbb{C}}(\mathrm{SO}(5) \times \mathrm{SO}(n-4)) \\
& =2\left\lfloor\frac{n+1}{2}\right\rfloor-2\left(\left\lfloor\frac{5}{2}\right\rfloor+\left\lfloor\frac{n-4}{2}\right\rfloor\right) \\
& =2\left\lfloor\frac{n+1}{2}\right\rfloor-2\left\lfloor\frac{n}{2}\right\rfloor .
\end{aligned}
$$

Thus $\delta\left(G_{1}(\mathbb{R}) \times G_{1}(\mathbb{R})\right)=\delta\left(G_{2}(\mathbb{R}) \times G_{2}(\mathbb{R})\right)$ is zero if and only if $n$ is even. Hence $\Gamma_{0}$ has a non-vanishing $p$-th $L^{2}$-Betti number if and only if $n$ is even and $p=\frac{2 n}{2}=n$, whereas $\Lambda_{0}$ has a non-vanishing $p$-th $L^{2}$-Betti number if and only if $n$ is even and $p=\frac{10 n-40}{2}=5 n-20$.
4.2 The $L^{2}$-Betti numbers in general are no profinite invariant

Now the main theorem of this section (cf. Theorem 1.0.2) is a direct consequence of the previous Theorem.

## References

Aka, Menny (2010). "Profinite completions and Kazhdan's property (T)". In: arXiv preprint arXiv:1005.4566.
Bourbaki, Nicolas (1989). General topology. Chapters 1-4. Translated from the French, Reprint of the 1966 edition.
Bridson, Martin R and Fritz J Grunewald (2004). "Grothendieck's problems concerning profinite completions and representations of groups". In: Annals of mathematics, pp. 359-373.
Cassels, John William Scott (2008). Rational quadratic forms. Courier Dover Publications.
Grothendieck, Alexander (1970). "Représentations linéaires et compactification profinite des groupes discrets". In: Manuscripta mathematica 2.4, pp. 375-396.
Humphreys, James E (2006). Arithmetic groups. Vol. 789. Springer.
Kammeyer, Holger (2014). "L2-invariants of nonuniform lattices in semisimple Lie groups". In: Algebraic $8 \mathcal{G}$ Geometric Topology 14.4, pp. 2475-2509.

- (2015). Lecture notes on L2-invariants.

Kneser, Martin (1979). "Normalteiler ganzzahliger Spingruppen." In: Journal für die reine und angewandte Mathematik 311, pp. 191-214.
Koch, Helmut (2013). Galois theory of p-extensions. Springer Science \& Business Media.
Lang, Serge (2004). "Algebra, volume 211". In: Graduate Texts in Mathematics, pp. 2930.

Lück, Wolfgang (1994). "Approximating L2-invariants by their finite-dimensional analogues". In: Geometric and Functional Analysis 4.4, pp. 455-481.

- (2013). L2-invariants: theory and applications to geometry and K-theory. Vol. 44. Springer Science \& Business Media.
Neukirch, Jürgen (1990). "Algebraische Zahlentheorie". In: Ein Jahrhundert Mathematik 1890-1990. Springer, pp. 587-628.
Nica, Bogdan (2013). "Linear groups-Malcev's theorem and Selberg's lemma". In: arXiv preprint arXiv:1306.2385.
Nikolov, Nikolay, Dan Segal, and Nikolay Nikolav (2007). "On Finitely Generated Profinite Groups, I: Strong Completeness and Uniform Bounds". In: Annals of Mathematics 165.1, pp. 171-238. ISSN: 0003486X.
Platonov, Vladimir Petrovich and Andrei Stepanovich Rapinchuk (1992). "Algebraic groups and number theory". In: Russian Mathematical Surveys 47.2, pp. 133-161.
Reid, Alan W. (2013). "Profinite properties of discrete groups". In: Proceedings of Groups St Andrews, pp. 73-104.
Ribes, Luis (2010). Profinite Groups. Ed. by Pavel Zalesskii. Berlin, Heidelberg.


## Erklärung

Ich versichere wahrheitsgemäß, die Arbeit selbstständig verfasst, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde sowie die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet zu haben.

Karlsruhe, den 23. Januar 2018

