SCHOOL OF COMPUTATION,
INFORMATION AND TECHNOLOGY —
INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Topological Groups

Niklas Krofta

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Topological Groups

Topologische Gruppen

Author:	Niklas Krofta
Examiner:	Prof. Dr. Tobias Nipkow
Supervisor:	Emin Karayel
Submission Date:	July 31st, 2024

I confirm that this bachelor's thesis is my own work and I have documented all sources and material used.

Munich, July 31st, 2024 Niklas Krofta

Acknowledgments

I would like to thank my supervisor Emin Karayel for his feedback and advice. Moreover, I thank Andriy Kryzhanovskyy for manifold interesting discussions about algebra and topology. Last but not least, my family and friends definitely deserve my gratitude for their measurable continuous support almost everywhere.

Abstract

Topological groups are blends of groups and topological spaces with the property that the multiplication and inversion operations are continuous functions. They frequently occur in mathematics and physics, e.g. in the form of Lie groups. We have developed a formalization of topological groups in the theorem prover Isabelle. It contains basic properties of topological groups as well as their uniform structures. The most notable formalized result is the Birkhoff-Kakutani theorem which gives a necessary and sufficient condition for the metrizability of a topological group. We also give examples for topological groups such as $\mathbb{R}^n$, $\mathbb{R}^\times$ and the general linear group $\mathrm{GL}_n(\mathbb{R})$ with its subgroups. In this thesis we present our formalization and describe the proof of Birkhoff-Kakutani in detail.

Contents

1 Introduction

Algebraic objects like groups or vector spaces often have a natural topological structure which is, in some sense, compatible with the algebraic structure. It can be very fruitful to analyze the interplay of algebraic and topological properties of such objects instead of focusing solely on one of these two domains. This motivates defining blends of algebraic and topological structures satisfying certain compatibility axioms. An example for such a blend is the concept of *topological groups*. [1, foreword] A topological group is a group G with a topology T endowed on G such that both the group multiplication $G \times G \to G$, $(\sigma, \tau) \mapsto \sigma\tau$ and the inverse mapping $G \to G$, $\sigma \mapsto \sigma^{-1}$ are continuous functions with respect to T. Here, the topology on $G \times G$ is the product topology. Some authors additionally require G to be a Hausdorff space. First examples of topological groups are $(\mathbb{R}^n, +)$ and $(\mathbb{R}^\times, \cdot)$ as well as the general linear groups $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$ and their subgroups. [1, Chapter 1.2] Moreover, all *Lie groups* are topological groups. Lie groups are groups which are also differentiable manifolds such that both multiplication and inversion are smooth (i.e. C^∞) functions. [2, page 31] Lie groups, in particular the *matrix Lie groups*, appear frequently in physics (especially in particle physics), where they are used to study symmetries. Matrix Lie groups are the groups $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$ and their closed subgroups. For instance, the special orthogonal group $\mathrm{SO}_n \subseteq \mathrm{GL}_n(\mathbb{R})$ is a matrix Lie group consisting of the rotations of the n-dimensional space $\mathbb{R}^n$ around the origin. It often occurs in physics problems involving rotational symmetry. [3]

An important motivation for studying topological groups are *Haar measures*, which are measures on topological groups with properties similar to the Lebesgue measure on $\mathbb{R}^n$. Haar measures enable us to integrate over topological groups in a way that is, in some sense, compatible with the group structure. Formally, a left Haar measure is a *regular left-invariant* Borel measure μ on a locally compact group G. A locally compact group is a topological group which is a locally compact Hausdorff space. Regularity of a measure is a property of compatibility with the underlying topology: For every Borel set $A \subseteq G$,

$$\mu(A) = \inf_{A \subseteq U,\ U \text{ open}} \mu(U) = \sup_{K \subseteq A,\ K \text{ compact}} \mu(K).$$

Left-invariance, on the other hand, is about compatiblity with the group structure: For every Borel set $A \subseteq G$ and group element $\sigma \in G$, we have $\mu(\sigma A) = \mu(A)$ where

$\sigma A := \{\sigma\tau \mid \tau \in A\}$. The notions of right-invariance and right Haar measure are defined analogously. It can be shown that Haar measures μ satisfy $\mu(U) > 0$ for non-empty open sets $U \subseteq G$ and $\mu(K) < \infty$ for compact sets $K \subseteq G$. The left-invariance of left Haar measures μ implies the following property of integrals with respect to μ: Let $f : G \to \mathbb{R}$ be a function and $\tau \in G$ a group element. Then f is μ-integrable if and only if $G \to \mathbb{R}$, $\sigma \mapsto f(\tau\sigma)$ is, and in this case

$$\int_G f(\tau\sigma)\, d\mu(\sigma) = \int_G f(\sigma)\, d\mu(\sigma).$$

It can be shown that left and right Haar measures exist on all locally compact groups and both measures are unique up to constant multiples. For example, the Lebesgue measure λ^n is a left and right Haar measure on $\mathbb{R}^n$. Furthermore,

$$\mu(A) := \int_A |\det(X)|^{-n}\, d\lambda^{n^2}(X)$$

for Borel sets $A \subseteq \mathrm{GL}_n(\mathbb{R})$ defines a left and right Haar measure on $\mathrm{GL}_n(\mathbb{R})$. Here, λ^{n^2} is the Lebesgue measure on the matrix space $\mathbb{R}^{n\times n}$ which can be identified with $\mathbb{R}^{n^2}$. [2, pages 3-5]

The above motivation shows that topological groups are an interesting and important topic in mathematics. We have formalized the basic theory of topological groups in the theorem prover *Isabelle* [4]. Our formalization [5] is based on the HOL-Algebra and HOL-Analysis libraries. It proves basic properties of topological groups and gives examples for such groups. It also includes the left and right uniformities of topological groups. For this purpose, we have given a definition of uniform structures which is not based on type classes, in contrast to the definition from HOL-Analysis. The most important theorem proven is the *Birkhoff-Kakutani* theorem which gives a necessary and sufficient condition for the metrizability of topological groups. In the following, we first describe our formalization and then explain the proof of Birkhoff-Kakutani in detail.

2 Description of formalization

In this chapter we give an overview of our formalization and present the most important definitions and results. The section proving the Birkhoff-Kakutanti theorem is excluded and discussed in Chapter 3 instead. Table 2.1 provides information on relevant Isabelle notation from HOL-Algebra and HOL-Analysis.

2.1 Definition and basic results

There are two implementations of groups in HOL-Algebra: a type class and a locale. Likewise, there are two notions of topologies in HOL-Analysis: a type class `topological_space` and a type `'a topology`. The weakness of the type class definitions is that one cannot define groups or topologies on proper subsets of a type's universe, resulting in the lack of fundamental concepts like (normal) subgroups. Therefore we avoid the type classes. We give the following Isabelle definition of topological groups:

locale *topological-group* = *group* +
  fixes T :: *'g topology*
  assumes *group-is-space*: *topspace* T = *carrier* G
  assumes *inv-continuous*: *continuous-map* T T $(\lambda\sigma.\ inv\ \sigma)$
  assumes *mul-continuous*: *continuous-map* (*prod-topology* T T) T $(\lambda(\sigma,\tau).\ \sigma\otimes\tau)$

A trivial consequence of the `group_is_space` assumption is that open sets are subsets of the group's carrier set. This fact will be used throughout the formalization to connect topological and algebraic arguments.

lemma *open-set-in-carrier*:
  assumes *openin* T U
  shows $U \subseteq$ *carrier* G
using *openin-subset group-is-space assms* **by** *auto*

It follows immediately from the continuity of the multiplication operation that left translations $G \to G$, $\tau \mapsto \sigma\tau$ as well as right translations $G \to G$, $\tau \mapsto \tau\sigma$ by some group element $\sigma \in G$ are continuous. In fact, translations are even homeomorphisms since their inverse functions are translations again. The inverse mapping is also a

homeomorphism because it is its own inverse function. [6, Lemma 1.4] Moreover, conjugations $G \to G$, $\tau \mapsto \sigma\tau\sigma^{-1}$ by some element $\sigma \in G$ are homeomorphisms since they are compositions of translations.

lemma *translations-continuous*:
assumes *in-group*: $\sigma \in$ *carrier G*
shows *continuous-map T T* $(\lambda\tau.\ \sigma\otimes\tau)$ **and** *continuous-map T T* $(\lambda\tau.\ \tau\otimes\sigma)$

lemma *translations-homeos*:
assumes *in-group*: $\sigma \in$ *carrier G*
shows *homeomorphic-map T T* $(\lambda\tau.\ \sigma\otimes\tau)$ **and** *homeomorphic-map T T* $(\lambda\tau.\ \tau\otimes\sigma)$

abbreviation *conjugation* :: $'g \Rightarrow 'g \Rightarrow 'g$ **where**
conjugation $\sigma\ \tau \equiv \sigma \otimes \tau \otimes$ *inv* σ

corollary *conjugation-homeo*:
assumes *in-group*: $\sigma \in$ *carrier G*
shows *homeomorphic-map T T* (*conjugation* σ)

lemma *inverse-homeo*: *homeomorphic-map T T* $(\lambda\sigma.$ *inv* $\sigma)$

Furthermore, translations being homeomorphisms implies the *translation invariance* of the topology: The image $\sigma U = \{\, \sigma\tau \mid \tau \in U \,\}$ of an open subset $U \subseteq G$ under left translation by an element $\sigma \in G$ is open again. This is still true if we exchange left with right and/or open with closed. [6, Corollary 1.5]

corollary *open-set-translations*:
assumes *open-set*: *openin T U* **and** *in-group*: $\sigma \in$ *carrier G*
shows *openin T* $(\sigma$ *<#* $U)$ **and** *openin T* $(U$ *#>* $\sigma)$

corollary *closed-set-translations*:
assumes *closed-set*: *closedin T U* **and** *in-group*: $\sigma \in$ *carrier G*
shows *closedin T* $(\sigma$ *<#* $U)$ **and** *closedin T* $(U$ *#>* $\sigma)$

Table 2.1: List of relevant operators from HOL-Algebra and HOL-Analysis

Operator	Meaning
`carrier G`	carrier set of a group
`topspace T`	carrier set of a topology
`x ⊗ y`	group multiplication operation
`inv x`	group inversion operation
`1`	neutral element of group
`N ◁ G`	normal subgroup
`x <# S`	multiplication of element with set
`S #> x`	multiplication of set with element
`S <#> T`	multiplication of set with set
`openin T U`	true if U is open set in topology T
`closedin T U`	true if U is closed set in topology T
`T closure_of S`	closure of set S in topology T
`continuous_map T1 T2 f`	true if f is a continuous map $T_1 \to T_2$
`connected_component_of_set T x`	connected component of x in topology T
`prod_topology T1 T2`	product of two topologies
`product_topology T I`	product of the topologies $T(i)$ with $i \in I$
`euclidean`	topology induced by `topological_space` type class
`'a^'n`	vector type of dimension n over `'a`
`v $ i`	i-th component of vector v
`'a^'n^'m`	type of matrices m rows, n columns and entries of type `'a`
`A $ i $ j`	entry in i-th row and j-th column of matrix A
`A ** B`	matrix product
`matrix_inv A`	inverse matrix
`mat 1`	identity matrix
`bdd-above S`	true if set S is bounded from above
`bdd-below S`	true if set S is bounded from below
`Metric-space.mtopology X d`	metric topology of metric d on X

2.2 Subspaces and quotient spaces

Keeping in mind the homeomorphisms identified above and making use of the fact that connected components are mapped to connected components under homeomorphisms, it is not hard to obtain the following result: The connected component of the neutral element $1 \in G$ is closed under multiplication, inverses and conjugation and is thus a normal subgroup of G. [1, Proposition 1.4.26] Furthermore, it is a closed subset of G since connected components are closed in general.

lemma *connected-components-homeo*:
assumes *homeo*: *homeomorphic-map* T_1 T_2 φ **and** *in-space*: $x \in$ *topspace* T_1
shows φ'(*connected-component-of-set* T_1 x) = *connected-component-of-set* T_2 (φ x)

abbreviation *connected-component-1* :: '*g set* **where**
connected-component-1 ≡ *connected-component-of-set* T **1**

lemma *connected-component-1-props*:
shows *connected-component-1* ◁ G **and** *closedin* T *connected-component-1*

Let Z_σ be the connected component of $\sigma \in G$. The coset $Z_1\sigma$ is the image of Z_1 under right translation by σ and thus a connected component by `connected-components-homeo`. Moreover, $\sigma = 1 \cdot \sigma \in Z_1\sigma$ and thus $Z_1\sigma = Z_\sigma$. Therefore the quotient group G/Z_1 consists of the connected components of G. For example, consider the topological group $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ with the usual multiplication and the subtopologoy induced by the euclidean topology on $\mathbb{R}$. The neutral element is the real number $1 \in \mathbb{R}$ and its connected component is the set of positive real numbers $\mathbb{R}^+$. The quotient group is $\mathbb{R}^\times/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$.

Next, we show that subgroups and quotient groups of topological groups are again topological groups with the respective induced topologies. For subgroups, this is straightforward [1, Chapter 1.2].

lemma *topological-subgroup*:
assumes *subgroup* H G
shows *topological-group* (G (|*carrier* := H|)) (*subtopology* T H)

For quotient groups, we first need quotient topologies. To our knowledge, only the notion of quotient map has been introduced in HOL-Analysis, but not the notion of quotient topology. Let X be a topological space and $q : X \to Y$ a surjection. According to the usual definition, a subset $U \subseteq Y$ is open in the quotient topology of X under q if and only if the preimage $q^{-1}(U)$ is open in X. Maps with this property are called quotient maps. Our Isabelle defintion looks as follows:

definition *quot-topology* :: *'a topology* ⇒ (*'a* ⇒ *'b*) ⇒ *'b topology* **where**
quot-topology T q = *topology* (λ*U*. *U* ⊆ *q'*(*topspace T*) ∧ *openin T* {*x* ∈ *topspace T*. *q x* ∈ *U*})

It remains to be shown that the defined object actually fulfills the desired properties. This mainly requires proving that the given open set predicate satisfies the axioms of a topology. Then, we obtain the following properties of quotient topologies:

lemma *quot-topology-open*:
fixes *T* :: *'a topology* **and** *q* :: *'a* ⇒ *'b*
defines *openin-quot U* ≡ *U* ⊆ *q'*(*topspace T*) ∧ *openin T* {*x* ∈ *topspace T*. *q x* ∈ *U*}
shows *openin* (*quot-topology T q*) = *openin-quot*

lemma *projection-quotient-map*: *quotient-map T* (*quot-topology T q*) *q*

corollary *topspace-quot-topology*: *topspace* (*quot-topology T q*) = *q'*(*topspace T*)

In HOL-Algebra, the quotient group of a normal subgroup $H \trianglelefteq G$ has been defined as the set of right cosets of H. It should be endowed with the quotient topology induced by the projection map $\pi : G \to G/H$, $\sigma \mapsto H\sigma$ [1, Chapter 1.5]. We define this coset topology as follows.

abbreviation *coset-topology* :: *'g set* ⇒ *'g set topology* **where**
coset-topology H ≡ *quot-topology T* (*r-coset G H*)

Now we are ready to prove that quotient groups of topological groups are again topological groups. To do this, we need the fact that projections of open sets in G and $G \times G$ are open in G/H and $G/H \times G/H$, respectively. Therefore we show that the projection $\pi : G \to G/H$ is an open map, which is not true for projections in general. This also implies the openness of $G \times G \to G/H \times G/H$, $(\sigma, \tau) \mapsto (\pi(\sigma), \pi(\tau))$, which we prove as a general lemma. [7]

lemma *projection-open-map*:
assumes *subgroup*: *subgroup H G*
shows *open-map T* (*coset-topology H*) (*r-coset G H*)

lemma *open-map-prod-top*:
assumes *open-map* T_1 T_3 *f* **and** *open-map* T_2 T_4 *g*
shows *open-map* (*prod-topology* T_1 T_2) (*prod-topology* T_3 T_4) (λ(*x*, *y*). (*f x*, *g y*))

lemma *topological-quotient-group*:
assumes *normal-subgroup*: *N* ◁ *G*
shows *topological-group* (*G Mod N*) (*coset-topology N*)

Often one is only interested in Hausdorff spaces. Next we answer the question when quotient groups of topological groups are Hausdorff. This is the case if and only if the corresponding normal subgroup is closed. The implication from right to left is non-trivial and requires an important auxiliary result: For every neighborhood $U \subseteq G$ of 1 there is a symmetric neighborhood S of 1 with $S^2 = \{\sigma\tau \mid \sigma, \tau \in S\} \subseteq U$ [6, Lemma 1.7]. In this thesis, neighborhoods in topological spaces are always considered open, so a neighborhood of $\sigma \in G$ is an open set $U \subseteq G$ with $\sigma \in U$. A subset $S \subseteq G$ is said to be symmetric if $S^{-1} = \{\sigma^{-1} \mid \sigma \in S\} \subseteq S$. This implies the other inclusion, so symmetric subsets satisfy $S^{-1} = S$.

abbreviation *neighborhood* :: *'g* ⇒ *'g set* ⇒ *bool* **where**
neighborhood σ U ≡ *openin T U* ∧ *σ* ∈ *U*

abbreviation *symmetric* :: *'g set* ⇒ *bool* **where**
symmetric S ≡ {*inv σ* | *σ*. *σ* ∈ *S*} ⊆ *S*

lemma *neighborhoods-of-1*:
assumes *neighborhood* **1** *U*
shows ∃ *V*. *neighborhood* **1** *V* ∧ *symmetric V* ∧ *V* <#> *V* ⊆ *U*

Now we can show that the coset space of a closed subgroup is Hausdorff [6, Lemma 1.11].

lemma *Hausdorff-coset-space*:
assumes *subgroup*: *subgroup H G* **and** *H-closed*: *closedin T H*
shows *Hausdorff-space* (*coset-topology H*)

The reverse implication is trivial: If G/H is Hausdorff, then $H = \pi^{-1}(\{H\})$ is closed in G since quotient maps are continuous and all points of a Hausdorff space are closed.

lemma *Hausdorff-coset-space-converse*:
assumes *subgroup*: *subgroup H G*
assumes *Hausdorff*: *Hausdorff-space* (*coset-topology H*)
shows *closedin T H*

corollary *Hausdorff-coset-space-iff*:
assumes *subgroup*: *subgroup H G*
shows *Hausdorff-space* (*coset-topology H*) ⟷ *closedin T H*

We can also deduce from this that a topological group G is Hausdorff if and only if $1 \in G$ is a closed point since G is trivially homeomorphic to $G/\{1\}$.

corollary *topological-group-hausdorff-iff-one-closed*:
shows *Hausdorff-space T* ⟷ *closedin T* {**1**}

Having motivated the importance of closed (normal) subgroups, we continue with the following result: The closure of a subgroup of a topological group G is again a subgroup [6, Lemma 1.7]. This immediately implies that the closure of a normal subgroup is again a normal subgroup. Indeed, if $N \trianglelefteq G$ is normal and $\varphi_\sigma : G \to G$ denotes conjugation by $\sigma \in G$, then $\varphi_\sigma(\overline{N}) \subseteq \overline{\varphi_\sigma(N)} \subseteq \overline{N}$ since φ_σ is continuous and $\varphi_\sigma(N) \subseteq N$.

lemma *subgroup-closure*:
assumes *H-subgroup*: *subgroup H G*
shows *subgroup* (*T closure-of H*) *G*

lemma *normal-subgroup-closure*:
assumes *normal-subgroup*: $N \lhd G$
shows (*T closure-of N*) $\lhd$ *G*

2.3 Uniform structures

2.3.1 General theory

The definitions and results in this section are based on the book *Topological and Uniform Spaces* [8, Chapters 7 and 8].

Just as topological spaces generalize metric spaces with respect to continuity, *uniform spaces* generalize metric spaces with respect to uniform continuity. In a topological space X, a neighborhood U of a point $x \in X$ is an expression of closeness: points in U are considered close to x with respect to U. Instead of open sets, a uniform space X has a set of *entourages*. An entourage $E \subseteq X \times X$ is a relation on X, and points $x' \in X$ are considered close to $x \in X$ with respect to E if xEx' holds. Consequently, the set of points close to x with respect to E (the E-neighborhood of x) is $E[x] := \{x' \in X \mid xEx'\}$. Note that entourages are not necessarily symmetric relations.

The difference between continuity and uniform continuity is a subtle change in the ordering of quantifiers. A function $f : X \to Y$ is continuous if for every $x \in X$ and every neighborhood V of $f(x) \in Y$ there is a neighborhood U of x such that $f(U) \subseteq V$, i.e. points close to x with respect to U are mapped to points close to $f(x)$ with respect to V. In contrast, f is uniformly continuous if for every entourage F in Y there is an entourage E in X such that for every point $x \in X$ we have $f(E[x]) \subseteq F[f(x)]$, i.e. points close to x with respect to E are mapped to points close to $f(x)$ with respect to F. For an entourage E, the E-neighborhoods $E[x]$ of all points x should be considered "the

same size". Then f being uniformly continuous means that for equally sized neighborhoods $F[f(x_1)], F[f(x_2)]$ there are equally sized neighborhoods $E[x_1], E[x_2]$ such that $f(E[x_1]) \subseteq F[f(x_1)]$ and $f(E[x_2]) \subseteq F[f(x_2)]$. This motivates the term "uniform continuity".

A set becomes a uniform space via a uniform structure, which is defined as follows.

Definition 1. A uniform structure consists of a set X, the uniform space, and a predicate Φ determining which relations $E \subseteq X \times X$ are entourages. The entourages defined by Φ must additionally satisfy the following axioms:

1. There is an entourage.
2. For every entourage E and $x \in X$, $(x, x) \in E$.
3. For every entourage E, $E^{-1} = \{(x_2, x_1) \mid (x_1, x_2) \in E\}$ is an entourage.
4. For every entourage E, there is an entourage F with
$$F^2 = \{(x_1, x_3) \mid (x_1, x_2), (x_2, x_3) \in F\} \subseteq E.$$
5. For every entourage E and relation $F \subseteq X \times X$ with $E \subseteq F$, F is an entourage.
6. For entourages E, F, the intersection $E \cap F$ is an entourage.

In HOL-Analysis there is a type class `uniform_space`, but for the reasons described earlier this is not suitable for our purposes. Therefore we define a new type `'a uniformity` in analogy to `'a topology` from HOL-Analysis. Our formalization includes an equivalence proof of `'a uniformity` and the `uniform_space` type class.

definition *uniformity-on* :: *'a set* ⇒ ((*'a* × *'a*) *set* ⇒ *bool*) ⇒ *bool* **where**
uniformity-on X Φ ⟷
(∃ *E*. Φ *E*) ∧
(∀ *E*. Φ *E* ⟶ *E* ⊆ *X* × *X* ∧ *Id-on X* ⊆ *E* ∧ Φ (*E*$^{-1}$) ∧ (∃ *F*. Φ *F* ∧ *F O F* ⊆ *E*) ∧ (∀ *F*. *E* ⊆ *F* ∧ *F* ⊆ *X* × *X* ⟶ Φ *F*)) ∧
(∀ *E F*. Φ *E* ⟶ Φ *F* ⟶ Φ (*E* ∩ *F*))

typedef *'a uniformity* = {(*X* :: *'a set*, Φ). *uniformity-on X* Φ}
morphisms *uniformity-rep uniformity*

definition *uspace* :: *'a uniformity* ⇒ *'a set* **where**
uspace Φ = (*let* (*X*, Φ) = *uniformity-rep* Φ *in X*)

definition *entourage-in* :: *'a uniformity* ⇒ (*'a* × *'a*) *set* ⇒ *bool* **where**
entourage-in Φ = (*let* (*X*, Φ) = *uniformity-rep* Φ *in* Φ)

lemma *uniformity-inverse'*:
assumes *uniformity-on X* Φ
shows *uspace* (*uniformity* (*X*, Φ)) = *X* ∧ *entourage-in* (*uniformity* (*X*, Φ)) = Φ

This is followed by lemmas proving that the entourages of an `'a uniformity` object fulfill the axioms listed above. We then go on to define uniform continuity. In analogy to regular continuity, uniform continuity can be formulated concisely in the following way: A function $f : X \to Y$ between uniform spaces is uniformly continuous if and only if for every entourage E of Y, $f^{-1}(E) := \{(x_1, x_2) \in X \times X \mid (f(x_1), f(x_2)) \in E\}$ is an entourage in X.

definition *ucontinuous* :: *'a uniformity* ⇒ *'b uniformity* ⇒ (*'a* ⇒ *'b*) ⇒ *bool* **where**
ucontinuous Φ Ψ *f* ⟷
f ∈ *uspace* Φ → *uspace* Ψ ∧
(∀ *E*. *entourage-in* Ψ *E* ⟶ *entourage-in* Φ {(*x*, *y*) ∈ *uspace* Φ × *uspace* Φ. (*f x*, *f y*) ∈ *E*})

The uniform structure of a uniform space X induces a topology on X: A subset $U \subseteq X$ is called open if and only if for every $x \in U$ there is an entourage E such that $E[x] \subseteq U$. This definition is reminiscent of the topology on metric spaces which uniform spaces are a generalization of. Topologies induced by uniform structures are called uniformizable and share some of the nice properties of metric topologies. We give the following Isabelle definition of the uniform topology.

definition *utopology* :: *'a uniformity* ⇒ *'a topology* **where**
utopology Φ = *topology* (λ*U*. *U* ⊆ *uspace* Φ ∧ (∀ *x*∈*U*. ∃ *E*. *entourage-in* Φ *E* ∧ *E*``{*x*} ⊆ *U*))

As with the definition of quotient topologies we need to prove that our definition satisfies the axioms of a toplogy. From this we can derive the following desired properties:

lemma *openin-utopology*:
fixes Φ :: *'a uniformity*
defines *uopen U* ≡ *U* ⊆ *uspace* Φ ∧ (∀ *x*∈*U*. ∃ *E*. *entourage-in* Φ *E* ∧ *E*``{*x*} ⊆ *U*)
shows *openin* (*utopology* Φ) = *uopen*

lemma *topspace-utopology*:
shows *topspace* (*utopology* Φ) = *uspace* Φ

It is straightforward to show that uniform continuity implies continuity in the uniform topologies.

lemma *ucontinuous-imp-continuous*:
assumes *ucontinuous* Φ Ψ *f*
shows *continuous-map* (*utopology* Φ) (*utopology* Ψ) *f*

To conclude this section, we give a first example of a uniform space: Every metric space (M, d) can be made into a uniform space by defining entourages to be the supersets of the sets $\{(x, y) \in M \times M \mid d(x, y) < \varepsilon\}$ for $\varepsilon \in \mathbb{R}^+$. Uniform continuity of functions between metric spaces with respect to the uniform structure coincides with the usual notion of uniform continuity. In the context of the `Metric_space` locale we define the following.

abbreviation *mentourage* :: *real* ⇒ (*'a* × *'a*) *set* **where**
mentourage ε ≡ {(*x*,*y*) ∈ *M* × *M*. *d x y* < ε}

definition *muniformity* :: *'a uniformity* **where**
muniformity = *uniformity* (*M*, λ*E*. *E* ⊆ *M* × *M* ∧ (∃ ε > 0. *mentourage* ε ⊆ *E*))

Once again we show the conformity of our definition with the uniformity axioms to be able to make use of the defined properties. Then it is straightforward to show that the induced uniform topology is equal to the metric topology.

lemma
uspace-muniformity: *uspace muniformity* = *M* **and**
entourage-muniformity: *entourage-in muniformity* = (λ*E*. *E* ⊆ *M* × *M* ∧ (∃ ε > 0. *mentourage* ε ⊆ *E*))

lemma *uniformity-induces-mtopology*: *utopology muniformity* = *mtopology*

2.3.2 Uniformities on topological groups

The definitions and results in this section are taken from the book *Topological Groups and Related Structures* [1, Chapter 1.8].

In a topological group G, the elements of some neighborhood U of the neutral element $1 \in G$ can be considered "close" to 1 or "small" with respect to U. It is thus intuitive to consider elements $\tau \in G$ "close" to $\sigma \in G$ with respect to U if $\sigma^{-1}\tau \in U$. This leads to the definition of a uniform structure on G where entourages are the supersets of the sets $\{(\sigma, \tau) \in G \times G \mid \sigma^{-1}\tau \in U\}$ with U a neighborhood of 1. This uniformity is called left uniformity to distinguish it from the right uniformity which regards $\tau \in G$ as "close" to $\sigma \in G$ if $\sigma\tau^{-1} \in U$.

abbreviation *left-entourage* :: *'g set* ⇒ (*'g* × *'g*) *set* **where**
left-entourage U ≡ {(σ,τ) ∈ *carrier G* × *carrier G*. *inv* σ ⊗ τ ∈ *U*}

definition *left-uniformity* :: *'g uniformity* **where** *left-uniformity* =
uniformity (*carrier G*, λ*E*. *E* ⊆ *carrier G* × *carrier G* ∧ (∃ *U*. *neighborhood* **1** *U* ∧ *left-entourage U* ⊆ *E*))

lemma
uspace-left-uniformity: *uspace left-uniformity* = *carrier G* **and**
entourage-left-uniformity: *entourage-in left-uniformity* =
(λ*E*. *E* ⊆ *carrier G* × *carrier G* ∧ (∃ *U*. *neighborhood* **1** *U* ∧ *left-entourage U* ⊆ *E*))

It is not hard to conclude that the induced uniform topology is equal to the original topology on the group. Topological groups are thus uniformizable spaces.

lemma *left-uniformity-induces-group-topology*:
shows *utopology left-uniformity* = *T*

Analogous definitions and lemmas are given for the right uniformity. We conclude this section with the remark that left translations are uniformly continuous with respect to the left uniformity, whereas right translations are uniformly continuous with respect to the the right uniformity.

lemma *translations-ucontinuous*:
assumes *in-group*: σ ∈ *carrier G*
shows *ucontinuous left-uniformity left-uniformity* (λτ. σ ⊗ τ) **and**
ucontinuous right-uniformity right-uniformity (λτ. τ ⊗ σ)

2.4 Examples

Any group becomes a topological group by endowing it with the discrete topology since any function defined on a discrete space is continuous [1, Chapter 1.2]. This is the most trivial example of topological groups.

lemma (**in** *group*) *discrete-topological-group*:
shows *topological-group G* (*discrete-topology* (*carrier G*))

A more interesting example is the additive group of the vector space $\mathbb{R}^n$. Its topology is the product topology induced by the usual topology on $\mathbb{R}$. [1, Chapter 1.2] The continuity of addition and negation, the inverse mapping, is well-known. HOL-Analysis implements cartesian vector spaces by means of a type `'a^'n`, where `'a` is an arbitrary base type and `'n` is a finite type. For example, the type `real^3` models $\mathbb{R}^3$ using the three-element-type `3`. If the type `'a` belongs to the `topological_space` type class like `real` does, then `'a^'n` also implements `topological_space` and its topology is the product topology. If a type `'a` implements `topological_space`, there is an `'a topology` object called `euclidean` connecting the type class to the set-based notion of topologies. We use this topology for our formalization. The continuity of addition and negation has been proven in HOL-Analysis.

lemma *topological-group-real-power-space*:
defines $\mathfrak{R}$ :: (*real*^'*n*) *monoid* ≡ (|*carrier* = *UNIV*, *monoid.mult* = (+), *one* = *0*|)
defines *T* :: (*real*^'*n*) *topology* ≡ *euclidean*
shows *topological-group* $\mathfrak{R}$ *T*

The unit group $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ of the reals with the usual multiplication and the subtopology induced by the standard topology on the reals also forms a topological group [1, Chapter 1.2].

definition *unit-group* :: ('*a* :: *field*) *monoid* **where**
unit-group = (|*carrier* = *UNIV* − {*0*}, *mult* = (∗), *one* = *1*|)

lemma
group-unit-group: *group unit-group* **and**
inv-unit-group: *x* ∈ *carrier unit-group* ⟹ $inv_{unit\text{-}group}\ x$ = *inverse x*

lemma *topological-group-real-unit-group*:
defines *T* :: *real topology* ≡ *subtopology euclidean* (*UNIV* − {*0*})
shows *topological-group unit-group T*

Our most important examples of topological groups are the general linear group $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \mid \det(A) \neq 0\}$ and its subgroups. One can give the matrix space $\mathbb{R}^{m\times n}$ a natural topological structure by interpreting it as the vector space $\mathbb{R}^{mn}$ (which, again, is endowed with the product topology). [1, Chapter 1.2]

2.4.1 Topologies on vector types

HOL-Analysis considers matrices as vectors of vectors. Matrices with components of type `'a` are modelled by the type `'a^'n^'m` where m is the number of rows and n is the number of columns. In order to prove the continuity of functions between vector types, we need to exploit the fact that the `euclidean` topology on `'a^'n` is a product topology of the `euclidean` topology on `'a`. However, `euclidean` on `'a^'n` is not actually defined via the `product_topology` operator, so we cannot apply any of the results proven about `product_topology`. We address this problem by defining a function `vec_topology` which takes an `'a topology` and builds an `('a^'n) topology` via the `product_topology`. The `product_topology` is an `('n => 'a) topology`, not an `('a^'n) topology`, but `'a^'n` is just a `typedef` of `'n => 'a`. We use the morphism `vec_lambda` from `'n => 'a` to `'a^'n` and our `quot_topology` operator to induce an `('a^'n) topology` from the `product_topology`.

definition *vec-topology* :: '*a topology* ⇒ ('*a*^'*n*) *topology* **where**
vec-topology T = *quot-topology* (*product-topology* (λ*i*. *T*) *UNIV*) *vec-lambda*

The morphism `vec_lambda` is a bijective quotient map from the `product_topology` to the `vec_topology` and thus a homeomorphism, along with the inverse morphsim `vec_nth`.

lemma *producttop-vectop-homeo*:
shows *homeomorphic-map* (*product-topology* (λ*i*. *T*) *UNIV*) (*vec-topology T*) *vec-lambda*

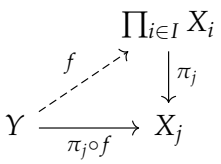
lemma *vectop-producttop-homeo*:
shows *homeomorphic-map* (*vec-topology T*) (*product-topology* (λ*i*. *T*) *UNIV*) *vec-nth*

We can now formally prove our claim that the `euclidean` topology on `'a^'n` is a product topology of the `euclidean` topology on `'a`. The proof does not contain any new ideas, it is just going back and forth between the two implementations of product topologies.

lemma *vec-topology-euclidean*:
defines *T* :: ('*a* :: *topological-space*) *topology* ≡ *euclidean*
defines T_{vec} :: ('*a*^'*n*) *topology* ≡ *euclidean*
shows *vec-topology T* = T_{vec}

The product topology on the product space $\prod_{i \in I} X_i$ has the following two essential properties.

1. All projections $\pi_j : \prod_{i \in I} X_i \to X_j$ with $j \in I$ are continuous.
2. A function $f : Y \to \prod_{i \in I} X_i$ is continuous if for all $j \in I$, $\pi_j \circ f$ is continuous (universal property of the product):



The homeomorphisms from above allow us to transfer these two properties to the `vec_topology`.

lemma *vec-projection-continuous*:
shows *continuous-map* (*vec-topology T*) *T* (λ*v*. *v*$*i*)

lemma *vec-components-continuous-imp-continuous*:
fixes *f* :: '*x* ⇒ '*a*^'*n*
assumes ∀ *i*. *continuous-map X T* (λ*x*. (*f x*) $ *i*)
shows *continuous-map X* (*vec-topology T*) *f*

We can now apply these results to the `euclidean` topology on `'a^'n` because of the lemma `vec_topology_euclidean`. For convenience we also define a `matrix_topology` on the type of matrices and give matrix versions of these lemmas. The proofs just apply the above results two times.

definition *matrix-topology* :: *'a topology* ⇒ (*'a^'n^'m*) *topology* **where**
matrix-topology T = *vec-topology* (*vec-topology T*)

lemma *matrix-topology-euclidean*:
shows *matrix-topology euclidean* = *euclidean*

lemma *matrix-projection-continuous*:
shows *continuous-map* (*matrix-topology T*) *T* (λ*A*. *A*$*i*$*j*)

lemma *matrix-components-continuous-imp-continuous*:
fixes *f* :: *'x* ⇒ *'a^'n^'m*
assumes ⋀*i j*. *continuous-map X T* (λ*x*. (*f x*) $ *i* $ *j*)
shows *continuous-map X* (*matrix-topology T*) *f*

Another advantage of the `vec_topology` operator is that it allows endowing `'a^'n` with product topologies induced by topologies on `'a` other than `euclidean`.

2.4.2 Matrix groups

HOL-Analysis proves that sums, products, etc. of continuous functions into the reals are continuous. Using this and the above lemmas, it is not hard to show that the determinant function as well as matrix transposition and multiplication are continuous.

lemma *det-continuous*:
defines *T* :: (*real^'n^'n*) *topology* ≡ *euclidean*
shows *continuous-map T euclideanreal det*

lemma *transpose-continuous*:
shows *continuous-map* (*euclidean* :: ((*'a* :: *topological-space*)^*'n*^*'m*) *topology*) *euclidean transpose*

lemma *matrix-mul-continuous*:
defines *T1* :: (*real^'n^'m*) *topology* ≡ *euclidean*
defines *T2* :: (*real^'r^'n*) *topology* ≡ *euclidean*
defines *T3* :: (*real^'r^'m*) *topology* ≡ *euclidean*
shows *continuous-map* (*prod-topology T1 T2*) *T3* (λ(*A*,*B*). *A* ** *B*)

We define the general linear group.

definition *GL* :: ((*'a* :: *field*)^*'n*^*'n*) *monoid* **where**
GL = (|*carrier* = {*A*. *invertible A*}, *monoid.mult* = (**), *one* = *mat 1*|)

definition *GL-topology* :: (*real^'n^'n*) *topology* **where**
GL-topology = *subtopology euclidean* (*carrier GL*)

lemma
GL-group: *group GL* **and**
GL-carrier [*simp*]: *carrier GL* = {*A*. *invertible A*} **and**
GL-inv [*simp*]: *A* ∈ *carrier GL* ⟹ inv_{GL} *A* = *matrix-inv A*

Showing that $\mathrm{GL}_n(\mathbb{R})$ is a topological group still requires the continuity of matrix inversion. The functions discussed above are defined explicitly via formulas, therefore we can systematically prove them to be continuous. Matrix inversion, however, is defined non-constructively via the characteristic property $AA^{-1} = A^{-1}A = 1$. Showing its continuity thus requires finding an explicit representation of the inverse matrix. This can be done with the help of Cramer's Rule, formalized in HOL-Analysis. We call the explicit inversion function `cramer_inv` and prove its correctness.

lemma *cramer-inv-is-inverse*:
assumes *invertible*: *invertible* (*A* :: ('*a* :: *field*)^'*n*^'*n*)
shows *matrix-inv A* = *cramer-inv A*

lemma *matrix-inv-continuous*:
shows *continuous-map* (*GL-topology* :: (*real^'n^'n*) *topology*) *GL-topology matrix-inv*

We can now conclude that $\mathrm{GL}_n(\mathbb{R})$ is actually a topological group. Moreover, it is open in the space of $n \times n$ matrices since it is the preimage of the open set $\mathbb{R} \setminus \{0\}$ under the continuous determinant map.

lemma
GL-topological-group: *topological-group GL GL-topology* **and**
GL-open: *openin* (*euclidean* :: (*real^'n^'n*) *topology*) (*carrier GL*)

It follows that all subgroups of $\mathrm{GL}_n(\mathbb{R})$ are topological groups, too. An example is the special linear group $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \mid \det(A) = 1\}$. It is a subgroup because the determinant $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism and $\mathrm{SL}_n(\mathbb{R}) = \ker(\det)$. Moreover, $\mathrm{SL}_n(\mathbb{R}) \subseteq \mathrm{GL}_n(\mathbb{R})$ is a closed subset because it is the preimage of the closed point $1 \in \mathbb{R}$ under the continuous determinant map. [6, Example 1.3]

lemma *det-homomorphism*: *group-hom GL unit-group det*

definition *SL* :: (('*a* :: *field*)^'*n*^'*n*) *monoid* **where**
SL = *GL* (|*carrier* := {*A*. *det A* = *1*}|)

lemma
SL-kernel-det: *carrier* (*SL* :: (('*a* :: *field*)^'*n*^'*n*) *monoid*) = *kernel GL unit-group det* **and**
SL-subgroup: *subgroup* (*carrier SL*) (*GL* :: ('*a*^'*n*^'*n*) *monoid*) **and**
SL-carrier [*simp*]: *carrier SL* = {*A*. *det A* = *1*}

lemma
SL-topological-group: *topological-group SL* (*subtopology GL-topology* (*carrier SL*)) **and**
SL-closed: *closedin GL-topology* (*carrier SL*)

Analogous results are proven for the subgroup O_n of orthogonal $n \times n$ matrices and the subgroup $\mathrm{SO}_n = \mathrm{SL}_n(\mathbb{R}) \cap \mathrm{O}_n$.

3 The Birkhoff-Kakutani theorem

The most important result in our formalization is the Birkhoff-Kakutani theorem. In this chapter, we present informal proofs of this theorem and the preliminary results it depends on. We will also compare the most interesting proof to its formalized version. The presented results (and their proofs, except for the proof of Lemma 1) have been taken and adapted from the book *Topological Groups and Related Structures* [1, pages 151-155] of Arhangel'skii and Tkachenko. (The authors of this book assume all topological groups to be Hausdorff spaces.)

Recall that a topological space X is called *metrizable* if its topology is induced by a metric on X. Furthermore, X is called *first-countable* if each point has a countable *neighborhood base*, i.e. for every $x \in X$ there is a sequence $(U_n)_{n\in\mathbb{N}}$ of neighborhoods of x such that for every neighborhood V of x there is an $n \in \mathbb{N}$ with $U_n \subseteq V$.

Definition 2. A metric $\Delta : G \times G \to G$ on a group is called *left-invariant* if $\Delta(\rho\sigma, \rho\tau) = \Delta(\sigma, \tau)$ for all $\sigma, \tau, \rho \in G$. Likewise, it is right-invariant if $\Delta(\sigma\rho, \tau\rho) = \Delta(\sigma, \tau)$.

Theorem 1 (Birkhoff-Kakutani)**.** *A topological group G is metrizable if and only if it is a first-countable Hausdorff space. In this case, the metric inducing the topology on G can be chosen to be left-invariant or right-invariant.*

Note that left-invariance and right-invariance are notions of compatibility with the group structure. Every metric space (X, Δ) is a first-countable Hausdorff space: Denote the open ball around $x \in X$ with radius $\varepsilon \in \mathbb{R}^+$ as $B_\varepsilon(x) := \{y \in X \mid \Delta(x, y) < \varepsilon\}$, then the sets $U_n := B_{1/n}(x)$ form a countable neighborhood base at x. Therefore we only have to prove that first-countable Hausdorff topological groups admit left-invariant and right-invariant metrics inducing the group topology. One can obtain a metric Δ on a normed vector space by defining $\Delta(x, y) := \|x - y\|$. The proof we present works in a similar way. Firstly, it is necessary to generalize the concept of a *norm* from vector spaces to groups.

3.1 Prenorms on groups

Definition 3. A function $N : G \to \mathbb{R}$ on a group G is called a prenorm if it satisfies the following axioms:

(i) $N(1) = 0$ for the neutral element $1 \in G$
(ii) $N(\sigma\tau) \leq N(\sigma) + N(\tau)$ for all $\sigma, \tau \in G$ (triangle inequality)
(iii) $N(\sigma^{-1}) = N(\sigma)$ for all $\sigma \in G$

It is clear that for every normed vector space $(V, \|\cdot\|)$, the norm $\|\cdot\|$ is a prenorm on the additive group $(V, +)$.

Proposition 1 (Properties of group prenorms)**.** *Let $N : G \to \mathbb{R}$ be a group prenorm. Then N satisfies the following properties:*
Non-negativity: $N(\sigma) \geq 0$ for all $\sigma \in G$
Reverse triangle inequality: $|N(\sigma) - N(\tau)| \leq N(\sigma\tau^{-1})$ for all $\sigma, \tau \in G$

Proof. We have $0 = N(1) = N(\sigma\sigma^{-1}) \leq N(\sigma) + N(\sigma^{-1}) = 2N(\sigma)$, so $N(\sigma) \geq 0$. Moreover, $N(\sigma) = N(\sigma\tau^{-1}\tau) \leq N(\sigma\tau^{-1}) + N(\tau)$, so $N(\sigma) - N(\tau) \leq N(\sigma\tau^{-1})$. Also, $N(\tau) = N(\tau^{-1}) \leq N(\sigma^{-1}) + N(\sigma\tau^{-1})$, therefore $N(\tau) - N(\sigma) \leq N(\sigma\tau^{-1})$. Thus $|N(\sigma) - N(\tau)| \leq N(\sigma\tau^{-1})$. □

This can be more or less directly translated to Isabelle.

```
definition group-prenorm :: ('g ⇒ real) ⇒ bool where
group-prenorm N ⟷
  N 1 = 0 ∧
  (∀σ τ. σ ∈ carrier G ∧ τ ∈ carrier G ⟶ N (σ ⊗ τ) ≤ N σ + N τ) ∧
  (∀σ ∈ carrier G. N (inv σ) = N σ)

lemma group-prenorm-clauses[elim]:
  assumes group-prenorm N
  shows
    N 1 = 0 and
    ⋀σ τ. σ ∈ carrier G ⟹ τ ∈ carrier G ⟹ N (σ ⊗ τ) ≤ N σ + N τ and
    ⋀σ. σ ∈ carrier G ⟹ N (inv σ) = N σ
  using assms unfolding group-prenorm-def by auto

proposition group-prenorm-nonnegative:
  assumes prenorm: group-prenorm N
  shows ∀σ ∈ carrier G. N σ ≥ 0

proposition group-prenorm-reverse-triangle-ineq:
  assumes prenorm: group-prenorm N and in-group: σ ∈ carrier G ∧ τ ∈ carrier G
  shows |N σ − N τ| ≤ N (σ ⊗ inv τ)
```

Next we need a way to construct prenorms on groups.

Lemma 1 (Induced group prenorm)**.** *Let $f : G \to \mathbb{R}$ be a bounded function on a group G. Then f induces a prenorm $N_f : G \to \mathbb{R}$, $\sigma \mapsto \sup_{\tau \in G} |f(\tau\sigma) - f(\tau)|$.*

Proof. First note that N_f is well-defined: f is bounded, so there is some $c \in \mathbb{R}$ with $|f(\tau) \leq c|$ for all $\tau \in G$. Then $|f(\tau\sigma) - f(\tau)| \leq |f(\tau\sigma)| + |f(\tau)| \leq 2c$ is bounded above, so the supremum exists. Now we need to check the prenorm axioms.
(i) $N_f(1) = \sup_{\tau \in G} |f(\tau) - f(\tau)| = 0$.
(ii) We have $|f(\rho\sigma\tau) - f(\rho)| = |f(\rho\sigma\tau) - f(\rho\sigma) + f(\rho\sigma) - f(\rho)| \leq |f(\rho\sigma\tau) - f(\rho\sigma)| + |f(\rho\sigma) - f(\rho)| \leq N_f(\tau) + N_f(\sigma)$ for all $\rho \in G$. Thus $N_f(\sigma\tau) \leq N_f(\sigma) + N_f(\tau)$ by the supremum property.
(iii) $|f(\tau\sigma^{-1}) - f(\tau)| = |f(\tau\sigma^{-1}\sigma) - f(\tau\sigma^{-1})|$ for all $\tau \in G$ and $|f(\rho\sigma) - f(\rho)| = |f(\rho\sigma\sigma^{-1}) - f(\rho\sigma)|$ for all $\rho \in G$. Therefore $N(\sigma^{-1})$ and $N(\sigma)$ are supremums over the same set, meaning $N(\sigma^{-1}) = N(\sigma)$. □

In the Isabelle formalization we add a lemma stating that the expression within the supremum is bounded. We need this fact whenever we want to use the property that the supremum is an upper bound.

definition *induced-group-prenorm* :: $('g \Rightarrow real) \Rightarrow 'g \Rightarrow real$ **where**
induced-group-prenorm f σ = (*SUP* $\tau \in$ *carrier G*. $|f\ (\tau \otimes \sigma) - f\ \tau|$)

lemma *induced-group-prenorm-welldefined*:
fixes *f* :: $'g \Rightarrow real$
assumes *f-bounded*: $\exists c. \forall \tau \in$ *carrier G*. $|f\ \tau| \leq c$ **and** *in-group*: $\sigma \in$ *carrier G*
shows *bdd-above* $((\lambda\tau.\ |f\ (\tau \otimes \sigma) - f\ \tau|)`(carrier\ G))$

lemma *bounded-function-induces-group-prenorm*:
fixes *f* :: $'g \Rightarrow real$
assumes *f-bounded*: $\exists c. \forall \sigma \in$ *carrier G*. $|f\ \sigma| \leq c$
shows *group-prenorm* (*induced-group-prenorm f*)

The translation invariance of the topology on a topological group G implies the following sufficient condition for the continuity of a prenorm $N : G \to \mathbb{R}$.

Proposition 2. *For the continuity of a prenorm $N : G \to \mathbb{R}$ on a topological group G, it is already sufficient that N is continuous at $1 \in G$, i.e. for every $\varepsilon \in \mathbb{R}^+$ there is a neighborhood U of 1 with $N(\sigma) < \varepsilon$ for all $\sigma \in U$.*

Proof. We are done if we can find a neighborhood V of σ with $N(V) \subseteq B_\varepsilon(N(\sigma))$ for every $\sigma \in G$ and every $\varepsilon \in \mathbb{R}^+$. Fix some $\sigma \in G$ and $\varepsilon \in \mathbb{R}^+$. From the assumption we obtain a neighborhood U of 1 with $N(\tau) < \varepsilon$ for all $\tau \in U$. By the translation invariance of the topology on G, σU is a neighborhood of $\sigma \cdot 1 = \sigma$. Let $\tau \in U$. We have $|N(\sigma) - N(\sigma\tau)| = |N(\sigma^{-1}) - N((\sigma\tau)^{-1})| \leq N(\sigma^{-1}\sigma\tau) = N(\tau) < \varepsilon$ using the reverse triangle inequality. Thus $N(\sigma U) \subseteq B_\varepsilon(N(\sigma))$. □

proposition *group-prenorm-continuous-if-continuous-at-1*:
assumes *prenorm*: *group-prenorm N* **and**
continuous-at-1: $\forall \varepsilon{>}0.\exists U.$ *neighborhood* $\mathbf{1}\ U \wedge (\forall \sigma{\in}U.\ N\ \sigma < \varepsilon)$
shows *continuous-map T euclideanreal N*

3.2 A prenorm respecting the group topology

As suggested earlier, we want to define a metric Δ on the topological group G by setting $\Delta(\sigma,\tau) := N(\sigma\tau^{-1})$ for some prenorm N. Δ should induce the group topology, but we can only hope for this if $\Delta(\sigma,\tau)$ being small coincides with τ being in a "small" neighborhood of σ. Therefore, $N(\rho)$ has to be small if and only if ρ is in a "small" neighborhood of 1. The following technical result constructs such prenorms N.

Lemma 2 (Construction of prenorms respecting the group topology)**.** *Let G be a topological group and $(U_n)_{n\in\mathbb{N}}$ a sequence of symmetric neighborhoods of $1 \in G$ with $U_{n+1}^2 \subseteq U_n$ for all $n \in \mathbb{N}$. Then there is a prenorm $N : G \to \mathbb{R}$ such that, for all $n \in \mathbb{N}$,*

$$\{\sigma \in G \mid N(\sigma) < 1/2^n\} \subseteq U_n \subseteq \{\sigma \in G \mid N(\sigma) \leq 2/2^n\}.$$

Proof. The first step is to associate every positive dyadic rational number $m/2^n$ where $m \in \mathbb{N}^+$, $n \in \mathbb{N}$ with a neighborhood of 1. This is done by means of a function $V(m,n)$ with the property $V(m,n) = V(m',n')$ if $m/2^n = m'/2^{n'}$. V is defined by recursion over n:

$$V(m,n) := \begin{cases} U_n & \text{if } m = 1 \\ G & \text{else if } m > 2^n \\ V(m/2, n-1) & \text{else if } m \text{ even} \\ V((m-1)/2, n-1) \cdot U_n & \text{else.} \end{cases}$$

Note: For V_1, V_2 neighborhoods of 1, $V_1V_2 = \{\sigma\tau \mid \sigma \in V_1, \tau \in V_2\} = \bigcup_{\sigma\in V_1} \sigma V_2$ is open and $1 = 1 \cdot 1 \in V_1V_2$, so V_1V_2 is a neighborhood of 1. Using this fact, it is simple to show inductively that $V(m,n) \subseteq G$ is actually a neighborhood of 1.

Claim 1: $V(m,n) \cdot U_n \subseteq V(m+1,n)$ for $m \in \mathbb{N}^+$, $n \in \mathbb{N}$. We prove this by induction on n. For $n = 0$, $V(m+1,0) = G$, so the statement is true. Now assume that the claim holds for some n. We need to show $V(m,n+1) \cdot U_{n+1} \subseteq V(m+1,n+1)$. We can assume $m+1 \leq 2^{n+1}$, otherwise $V(m+1,n+1) = G$ and the statement is trivially true. Moreover, $m > 1$ without loss of generality because

$$V(1,n+1) \cdot U_{n+1} = U_{n+1}^2 \subseteq U_n = V(1,n) = V(2,n+1).$$

We make a case distinction:
(a) m is even. Then $V(m, n+1) \cdot U_{n+1} = V(m/2, n) \cdot U_{n+1} = V(m+1, n+1)$.
(b) m is odd. Then

$$\begin{aligned} V(m, n+1) \cdot U_{n+1} &= V((m-1)/2, n) \cdot U_{n+1} \cdot U_{n+1} = V((m-1)/2, n) \cdot U_{n+1}^2 \\ &\subseteq V((m-1)/2, n) \cdot U_n \subseteq V((m-1)/2+1, n) \\ &= V((m+1)/2, n) = V(m+1, n+1) \end{aligned}$$

where $V((m-1)/2, n) \cdot U_n \subseteq V((m-1)/2+1, n)$ by the induction hypothesis.

Claim 2: For positive dyadic rationals $m_1/2^{n_1} \leq m_2/2^{n_2}$, we have $V(m_1, n_1) \subseteq V(m_2, n_2)$, i.e. V is monotone. First note that $V(m, n) = V(m, n) \cdot 1 \subseteq V(m, n) \cdot U_n \subseteq V(m+1, n)$ by Claim 1. By induction we obtain $V(m, n) \subseteq V(m+k, n)$ for $k \in \mathbb{N}$, so $V(m, n) \subseteq V(m', n)$ if $m \leq m'$. By induction it is also clear that $V(m, n) = V(m \cdot 2^k, n+k)$ for $k \in \mathbb{N}$. We make a case distinction.
(a) $n_1 \leq n_2$. Then $m_1/2^{n_1} = (m_1 \cdot 2^{n_2-n_1})/2^{n_2} \leq m_2/2^{n_2}$, thus $m_1 \cdot 2^{n_2-n_1} \leq m_2$, meaning

$$V(m_1, n_1) = V(m_1 \cdot 2^{n_2-n_1}, n_1 + n_2 - n_1) = V(m_1 \cdot 2^{n_2-n_1}, n_2) \subseteq V(m_2, n_2)$$

(b) $n_2 \leq n_1$. Proceed analogously to (a).

Now we define $f : G \to \mathbb{R}$, $\sigma \mapsto \inf\{m/2^n \mid \sigma \in V(m, n)\}$. The infimum exists since the set is bounded below by 0 and also non-empty, as $\sigma \in G = V(2, 0)$. Clearly $f(\sigma) \geq 0$ and $f(\sigma) \leq 2/2^0 = 2$. So f is bounded and thus induces a prenorm $N_f : G \to \mathbb{R}$.

Claim 3: For $\sigma \in G$ with $f(\sigma) < m/2^n$, we have $\sigma \in V(m, n)$. Indeed, by the infimum property, there must be m', n' with $m'/2^{n'} < m/2^n$ and $\sigma \in V(m', n')$. Claim 2 yields $V(m', n') \subseteq V(m, n)$, so $\sigma \in V(m, n)$.

Note that $f(1) = 0$. Otherwise $f(1) > 0$, so there is some $n \in \mathbb{N}$ with $1/2^n < f(1)$. But $1 \in U_n = V(1, n)$, so $f(1) \leq 1/2^n$ - a contradiction. Now we prove $\{\sigma \in G \mid N_f(\sigma) < 1/2^n\} \subseteq U_n$ for $n \in \mathbb{N}$. Fix $\sigma \in G$ with $N_f(\sigma) < 1/2^n$. We have $f(\sigma) = |f(1 \cdot \sigma) - f(1)| \leq N_f(\sigma) < 1/2^n$, thus $\sigma \in V(1, n) = U_n$ by Claim 3. It remains to show the second inclusion.

Let $n \in \mathbb{N}$ and $\sigma \in U_n$. Additionally, fix some $\tau \in G$. Clearly there is $k \in \mathbb{N}^+$ such that $(k-1)/2^n \leq f(\tau) < k/2^n$. Again, Claim 3 yields $\tau \in V(k, n)$. We have $\sigma^{-1} \in U_n$ because $\sigma \in U_n$ and U_n is symmetric. Therefore $\tau\sigma, \tau\sigma^{-1} \in V(k, n) \cdot U_n \subseteq V(k+1, n)$ using Claim 1, and this in turn implies $f(\tau\sigma), f(\tau\sigma^{-1}) \leq (k+1)/2^n$. Together with $(k-1)/2^n \leq f(\tau)$ from above, this shows (a) $f(\tau\sigma) - f(\tau) \leq 2/2^n$

and (b) $f(\tau\sigma^{-1}) - f(\tau) \leq 2/2^n$. Now fix some $\rho \in G$. τ represents an arbitrary element of G, so we can substitute it with ρ in (a) and $\rho\sigma$ in (b). This yields $f(\rho\sigma) - f(\rho) \leq 2/2^n$ and $f(\rho) - f(\rho\sigma) = f(\rho\sigma\sigma^{-1}) - f(\rho\sigma) \leq 2/2^n$, implying $|f(\rho\sigma) - f(\rho)| \leq 2/2^n$. It follows that $N_f(\sigma) \leq 2/2^n$ since ρ has been arbitrarily chosen. This proves the second inclusion.

□

Some intuition for this proof: Claim 2 justifies viewing $m/2^n$ as the "size" of $V(m,n)$. Then $f(\sigma)$, the infimum of the sizes of neighborhoods of 1 containing σ, can be interpreted as the "distance" of σ from 1. Thus $f(1) = 0$ is intuitively clear. Recall that $N_f(\sigma) = \sup_{\rho \in G} |f(\rho\sigma) - f(\rho)|$ should be small if and only if σ is in a small neighborhood of 1. This means that for σ in a small neighborhood of 1, i.e. $\sigma \in U_n$ for some large n, $f(\rho\sigma)$ must be close to $f(\rho)$ for any $\rho \in G$. This is achieved by the property $V(m,n) \cdot U_n \subseteq V(m+1,n)$ from Claim 1: For every $V(m,n)$ with $\rho \in V(m,n)$, this property implies that $\rho\sigma$ is in $V(m+1,n)$, and the size difference between $V(m,n)$ and $V(m+1,n)$ is $1/2^n$ which is small for large n. The property from Claim 1 is thus essential for the proof and motivates the definition of V.

In our formalization we create a new context for Lemma 2.

```
context
  fixes U :: nat ⇒ 'g set
  assumes U-neighborhood: ∀ n. neighborhood 1 (U n)
  assumes U-props: ∀ n. symmetric (U n) ∧ (U (n + 1)) <#> (U (n + 1)) ⊆ (U n)
```

We use the `fun` command to define the recursive function V. We set $V(0,n) := \emptyset$ since Isabelle functions must be total and this is the most convenient value.

```
private fun V :: nat ⇒ nat ⇒ 'g set where
V m n = (
  if m = 0 then {} else
  if m = 1 then U n else
  if m > 2^n then carrier G else
  if even m then V (m div 2) (n − 1) else
  V ((m − 1) div 2) (n − 1) <#> U n
)
```

The fact that $V(m,n)$ is a neighborhood of 1 is actually not necessary for the proof of Lemma 2, we only need the fact $V(m,n) \subseteq G$. This can be trivially shown by induction.

```
private lemma U-in-group: U k ⊆ carrier G
```

private lemma *V-in-group*:
shows $V\ m\ n \subseteq$ *carrier G*

Claim 1 and Claim 2 are proven as separate lemmas within the context.

private lemma *V-mult*:
shows $m \geq 1 \Longrightarrow V\ m\ n <\#> U\ n \subseteq V\ (m + 1)\ n$

private lemma *V-mono*:
assumes *smaller*: $(real\ m_1)/2\hat{}n_1 \leq (real\ m_2)/2\hat{}n_2$ **and** *not-zero*: $m_1 \geq 1 \wedge m_2 \geq 1$
shows $V\ m_1\ n_1 \subseteq V\ m_2\ n_2$

We also need a lemma constructing the number k in the proof of Lemma 2.

private lemma *approx-number-by-multiples*:
assumes *hx*: $x \geq 0$ **and** *hc*: $c > 0$
shows $\exists k :: nat \geq 1.\ (real\ (k-1))/c \leq x \wedge x < (real\ k)/c$
proof −
let *?k* $= \lfloor x * c \rfloor + 1$
have *?k* ≥ 1 **using** *assms* **by** *simp*
moreover from *this* **have** $real\ (nat\ ?k) =$ *?k* **by** *auto*
moreover have $(?k-1)/c \leq x \wedge x <$ *?k*$/c$
using *assms* **by** (*simp add*: *mult-imp-div-pos-le pos-less-divide-eq*)
ultimately show *?thesis*
by (*smt* (*verit*) *nat-diff-distrib nat-le-eq-zle nat-one-as-int of-nat-nat*)
qed

The formal version of the proof of Lemma 2 is structured similarly to the informal version. In Isabelle, using the lower bound property of the infimum requires the fact that the set in question is actually bounded below (fact `bdd-below` in the formal proof below); this corresponds to the well-definedness argument in the informal proof. The same is true for the supremum (fact `N_welldefined`), which is why we need the lemma `induced-group-prenorm-welldefined` from above.

lemma *construction-of-prenorm-respecting-topology*:
shows $\exists N.$ *group-prenorm* $N \wedge$
$(\forall n.\ \{\sigma \in$ *carrier G*$.\ N\ \sigma < 1/2\hat{}n\} \subseteq U\ n) \wedge$
$(\forall n.\ U\ n \subseteq \{\sigma \in$ *carrier G*$.\ N\ \sigma \leq 2/2\hat{}n\})$
proof −
define $f :: {'g} \Rightarrow real$ **where** $f\ \sigma = Inf\ \{(real\ m)/2\hat{}n \mid m\ n.\ \sigma \in V\ m\ n\}$ **for** σ
define $N :: {'g} \Rightarrow real$ **where** $N =$ *induced-group-prenorm f*

have $\sigma \in V\ 2\ 0$ **if** $\sigma \in$ *carrier G* **for** σ **using** *that* **by** *auto*

then have *contains-2*: $(real\ 2)/2\hat{}0 \in \{(real\ m)/2\hat{}n \mid m\ n.\ \sigma \in V\ m\ n\}$ **if** $\sigma \in carrier\ G$ **for** σ **using** *that* **by** *blast*
then have *nonempty*: $\{(real\ m)/2\hat{}n \mid m\ n.\ \sigma \in V\ m\ n\} \neq \{\}$ **if** $\sigma \in carrier\ G$ **for** σ **using** *that* **by** *fast*
have *positive*: $(real\ m)/2\hat{}n \geq 0$ **for** $m\ n$ **by** *simp*
then have *bdd-below*: *bdd-below* $\{(real\ m)/2\hat{}n \mid m\ n.\ \sigma \in V\ m\ n\}$ **for** σ **by** *fast*
have *f-bounds*: $0 \leq f\ \sigma \wedge f\ \sigma \leq 2$ **if** *hσ*: $\sigma \in carrier\ G$ **for** σ
proof −
from *bdd-below* **have** $f\ \sigma \leq (real\ 2)/2\hat{}0$ **unfolding** *f-def* **using** *cInf-lower contains-2*[*OF hσ*] **by** *meson*
moreover have $0 \leq f\ \sigma$ **using** *cInf-greatest contains-2*[*OF hσ*] **unfolding** *f-def* **using** *positive*
by (*smt* (*verit*, *del-insts*) *Collect-mem-eq empty-Collect-eq mem-Collect-eq*)
ultimately show *?thesis* **by** *fastforce*
qed
then have *N-welldefined*: *bdd-above* $((\lambda\tau.\ |f\ (\tau \otimes \sigma) - f\ \tau|)\ `\ carrier\ G)$ **if** $\sigma \in carrier\ G$ **for** σ
using *induced-group-prenorm-welldefined that* **by** (*metis* (*full-types*) *abs-of-nonneg*)

have *in-V-if-f-smaller*: $\sigma \in V\ m\ n$ **if** *hσ*: $\sigma \in carrier\ G$ **and** *smaller*: $f\ \sigma < (real\ m)/2\hat{}n$ **for** $\sigma\ m\ n$
proof −
from *cInf-lessD* **obtain** *q* **where** *hq*: $q \in \{(real\ m)/2\hat{}n \mid m\ n.\ \sigma \in V\ m\ n\} \wedge q < (real\ m)/2\hat{}n$
using *smaller nonempty*[*OF hσ*] **unfolding** *f-def* **by** (*metis* (*mono-tags*, *lifting*))
then obtain $m'\ n'$ **where** *hm'n'*: $\sigma \in V\ m'\ n' \wedge q = (real\ m')/2\hat{}n'$ **by** *fast*
moreover have $m' \geq 1$
proof (*rule ccontr*)
assume $\neg\ m' \geq 1$
then have $V\ m'\ n' = \{\}$ **by** *force*
then show *False* **using** *hm'n'* **by** *blast*
qed
moreover have $m \geq 1$ **using** *f-bounds smaller hσ*
by (*metis divide-eq-0-iff less-numeral-extra*(3) *less-one linorder-le-less-linear nle-le of-nat-0 order-less-imp-le*)
ultimately have $V\ m'\ n' \subseteq V\ m\ n$ **using** *V-mono hq U-props open-set-in-carrier* **by** *simp*
then show *?thesis* **using** *hm'n'* **by** *fast*
qed
have *f-1-vanishes*: $f\ \mathbf{1} = 0$
proof (*rule ccontr*)
assume $f\ \mathbf{1} \neq 0$
then have $f\ \mathbf{1} > 0$ **using** *f-bounds* **by** *fastforce*
then obtain *n* **where** *hn*: $f\ \mathbf{1} > (real\ 1)/2\hat{}n$
by (*metis divide-less-eq-1 of-nat-1 one-less-numeral-iff power-one-over real-arch-pow-inv semiring-norm*(76) *zero-less-numeral*)
have $\mathbf{1} \in V\ 1\ n$ **using** *U-neighborhood* **by** *simp*
then have $(real\ 1)/2\hat{}n \in \{(real\ m)/2\hat{}n \mid m\ n.\ \mathbf{1} \in V\ m\ n\}$ **by** *fast*
then show *False* **using** *hn cInf-lower bdd-below*[*of* $\mathbf{1}$] **unfolding** *f-def* **by** (*smt* (*verit*, *ccfv-threshold*))

```
 qed
 have in-U-if-N-small: σ ∈ U n if in-group: σ ∈ carrier G and N-small: N σ < 1/2^n for σ n
 proof −
  have f σ = |f (1 ⊗ σ) − f 1| using in-group l-one f-1-vanishes f-bounds by force
  moreover have ... ≤ N σ unfolding N-def induced-group-prenorm-def
   using cSUP-upper N-welldefined[OF in-group] by (metis (mono-tags, lifting) one-closed)
  ultimately have σ ∈ V 1 n using in-V-if-f-smaller[OF in-group] N-small by (smt (verit) of-nat-1)
  then show ?thesis by fastforce
 qed
 have N-bounds: N σ ≤ 2/2^n if hσ: σ ∈ U n for σ n
 proof −
  have diff-bounded: f (τ ⊗ σ) − f τ ≤ 2/2^n ∧ f (τ ⊗ inv σ) − f τ ≤ 2/2^n if hτ: τ ∈ carrier G
for τ
  proof −
   obtain k where hk: k ≥ 1 ∧ (real (k−1))/2^n ≤ f τ ∧ f τ < (real k)/2^n
    using approx-number-by-multiples[of f τ 2^n] f-bounds[OF hτ] by auto
   then have τ ∈ V k n using in-V-if-f-smaller[OF hτ] by blast
   moreover have σ ∈ V 1 n ∧ inv σ ∈ V 1 n using hσ U-props by auto
   moreover have V k n <#> V 1 n ⊆ V (k + 1) n
    using V-mult U-props open-set-in-carrier hk by auto
   ultimately have τ ⊗ σ ∈ V (k + 1) n ∧ τ ⊗ inv σ ∈ V (k + 1) n
    unfolding set-mult-def by fast
   then have a: (real (k + 1))/2^n ∈ {(real m)/2^n | m n. τ ⊗ σ ∈ V m n}
    ∧ (real (k + 1))/2^n ∈ {(real m)/2^n | m n. τ ⊗ inv σ ∈ V m n} by fast
   then have f (τ ⊗ σ) ≤ (real (k + 1))/2^n
    unfolding f-def using cInf-lower[of (real (k + 1))/2^n] bdd-below by presburger
   moreover from a have f (τ ⊗ inv σ) ≤ (real (k + 1))/2^n
    unfolding f-def using cInf-lower[of (real (k + 1))/2^n] bdd-below by presburger
   ultimately show ?thesis using hk
    by (smt (verit, ccfv-SIG) diff-divide-distrib of-nat-1 of-nat-add of-nat-diff)
  qed
  have |f (ϱ ⊗ σ) − f ϱ| ≤ 2/2^n if hϱ: ϱ ∈ carrier G for ϱ
  proof −
   have in-group: σ ∈ carrier G using hσ U-in-group by fast
   then have f (ϱ ⊗ σ ⊗ inv σ) − f (ϱ ⊗ σ) ≤ 2/2^n using diff-bounded[of ϱ ⊗ σ] hϱ m-closed
by fast
   moreover have ϱ ⊗ σ ⊗ inv σ = ϱ using m-assoc r-inv r-one in-group inv-closed hϱ by presburger
   ultimately have f ϱ − f (ϱ ⊗ σ) ≤ 2/2^n by force
   moreover have f (ϱ ⊗ σ) − f ϱ ≤ 2/2^n using diff-bounded[OF hϱ] by fast
   ultimately show ?thesis by force
  qed
  then show ?thesis unfolding N-def induced-group-prenorm-def using cSUP-least carrier-not-empty
by meson
 qed
```

then have *U n* $\subseteq \{\sigma \in$ *carrier G*. *N* $\sigma \leq 2/2\hat{}n\}$ **for** *n* **using** *U-in-group* **by** *blast*
moreover have *group-prenorm N* **unfolding** *N-def*
using *bounded-function-induces-group-prenorm f-bounds* **by** (*metis abs-of-nonneg*)
ultimately show *?thesis* **using** *in-U-if-N-small* **by** *blast*
qed

3.3 Proof of Birkhoff-Kakutani

We can now finally prove the Birkhoff-Kakutani theorem.

Proof of Birkhoff-Kakutani. As explained earlier, we are done if we can show that the topology of a first-countable Hausdorff topological group G is induced by left-invariant and right-invariant metrics. From the first-countability assumption we obtain a countable neighborhood base $(W_n)_{n\in\mathbb{N}}$ of $1 \in G$. Recall that for every neighborhood U of 1 there is a symmetric neighborhood V of 1 with $V^2 \subseteq U$. Note that this implies $V \subseteq U$. We construct a sequence $(U_n)_{n\in\mathbb{N}}$ of symmetric neighborhoods of 1 with $U_n \subseteq W_n$ and $U_{n+1}^2 \subseteq U_n$ for all $n \in \mathbb{N}$ by recursively choosing symmetric neighborhoods U_{n+1} of 1 with $U_{n+1}^2 \subseteq U_n \cap W_{n+1}$. Clearly, $U_n \subseteq W_n$ implies that $(U_n)_n$ is also a neighborhood base of 1. From Lemma 2 we obtain a prenorm $N : G \to \mathbb{R}$ such that

$$\{\sigma \in G \mid N(\sigma) < 1/2^n\} \subseteq U_n \subseteq \{\sigma \in G \mid N(\sigma) \leq 2/2^n\}$$

for all $n \in \mathbb{N}$. By Proposition 2, N is continuous because for any $\varepsilon \in \mathbb{R}^+$ there is some $n \in \mathbb{N}$ with $1/2^n < \varepsilon$ and thus $N(\sigma) \leq 2/2^{n+1} = 1/2^n < \varepsilon$ for every $\sigma \in U_{n+1}$. As announced earlier, we define a metric Δ on G by setting $\Delta(\sigma, \tau) := N(\sigma\tau^{-1})$. We need to check the metric axioms.
(i) Non-negativity: $\Delta(\sigma\tau) \geq 0$ since prenorms are non-negative.
(ii) Symmetry: $\Delta(\sigma, \tau) = N(\sigma\tau^{-1}) = N((\sigma\tau^{-1})^{-1}) = N(\tau\sigma^{-1}) = \Delta(\tau, \sigma)$.
(iii) Positive Definiteness: $\Delta(\sigma, \tau) = 0 \iff \sigma = \tau$. Clearly, $\Delta(\sigma, \sigma) = N(\sigma\sigma^{-1}) = N(1) = 0$. Conversely, assume $\Delta(\sigma, \tau) = 0$. Then $N(\sigma\tau^{-1}) < 1/2^n$ for all $n \in \mathbb{N}$, so $\sigma\tau^{-1} \in U_n$ for all n. By extension, $\sigma\tau^{-1}$ is contained in all neighborhoods of 1 since $(U_n)_n$ is a neighborhood base. G is a Hausdorff space, therefore

$$\sigma\tau^{-1} \in \bigcap\{V \subseteq G \mid V \text{ neighborhood of } 1\} = \{1\}$$

which implies $\sigma = \tau$. This is actually the only point where we need the Hausdorffness assumption.
(iv) Triangle inequality:

$$\Delta(\sigma, \rho) = N(\sigma\rho^{-1}) = N(\sigma\tau^{-1}\tau\rho^{-1}) \leq N(\sigma\tau^{-1}) + N(\tau\rho^{-1}) = \Delta(\sigma, \tau) + \Delta(\tau, \rho).$$

Moreover, the metric Δ is right invariant because

$$\Delta(\sigma\rho, \tau\rho) = N(\sigma\rho(\tau\rho)^{-1}) = N(\sigma\rho\rho^{-1}\tau^{-1}) = N(\sigma\tau^{-1}) = \Delta(\sigma, \tau).$$

It remains to show that the metric topology defined by Δ coincides with the original topology on G. This can be done by proving that the two topologies share a *base*. A base of a topology T is a set $\mathcal{B}$ of open sets of T such that for every open set V of T and point $x \in V$ there is some $B \in \mathcal{B}$ with $x \in B \subseteq V$. It is well-known that the open balls $B_\varepsilon(\sigma) = \{\tau \in G \mid \Delta(\sigma, \tau) < \varepsilon\}$ form a base $\mathcal{B} := \{B_\varepsilon(\sigma) \mid \sigma \in G, \varepsilon \in \mathbb{R}^+\}$ of the metric topology of Δ. Note that $B_\varepsilon(1) = \{\sigma \in G \mid N(\sigma) < \varepsilon\}$.

Claim 1: $B_\varepsilon(\sigma) = B_\varepsilon(1) \cdot \sigma$.
($\subseteq$) If $\tau \in B_\varepsilon(\sigma)$ then $\Delta(\sigma, \tau) = N(\sigma\tau^{-1}) < \varepsilon$, implying $N(\tau\sigma^{-1}) = N((\sigma\tau^{-1})^{-1}) < \varepsilon$, thus $\tau = \tau\sigma^{-1} \cdot \sigma \in B_\varepsilon(1) \cdot \sigma$.
($\supseteq$) For $\rho\sigma \in B_\varepsilon(1) \cdot \sigma$ with $\rho \in B_\varepsilon(1)$ we have $\Delta(\sigma, \rho\sigma) = N(\sigma(\rho\sigma)^{-1}) = N(\rho^{-1}) = N(\rho) < \varepsilon$, therefore $\rho\sigma \in B_\varepsilon(\sigma)$.

Claim 2: $\mathcal{B}$ is a base of the original group topology.
The sets $B_\varepsilon(\sigma) = B_\varepsilon(1) \cdot \sigma$ are open in the group topology by the translation invariance of the topology because $B_\varepsilon(1) = N^{-1}((-\infty, \varepsilon))$ is the preimage of an open set under a continuous map. Now let V be an open set of the group topology. Let $\sigma \in V$. Then $V\sigma^{-1}$ is a neighborhood of 1, so there is some $n \in \mathbb{N}$ with $B_{1/2^n}(1) \subseteq U_n \subseteq V\sigma^{-1}$. Therefore $\sigma \in B_{1/2^n}(\sigma) = B_{1/2^n}(1) \cdot \sigma \subseteq V\sigma^{-1}\sigma = V$.

We have proved that the two topologies share the base $\mathcal{B}$, thus they are equal. This means that the group topology is induced by a right-invariant metric. Note that we could have chosen Δ to be left-invariant instead of right-invariant by setting $\Delta(\sigma, \tau) := N(\sigma^{-1}\tau)$. *Mutatis mutandis*, the rest of the proof stays the same. □

In our formalization we move the construction of the sequence $(U_n)_n$ into a separate lemma. The recursive choosing is done by the lemma `dependent_nat_choice` from the HOL library.

lemma *first-countable-neighborhoods-of-1-sequence*:
assumes *first-countable T*
shows $\exists\, U :: nat \Rightarrow 'g\ set.$
$(\forall\, n.\ neighborhood\ \mathbf{1}\ (U\ n) \wedge symmetric\ (U\ n) \wedge U\ (n+1) <\#> U\ (n+1) \subseteq U\ n) \wedge$
$(\forall\, W.\ neighborhood\ \mathbf{1}\ W \longrightarrow (\exists\, n.\ U\ n \subseteq W))$

We split the theorem into two Isabelle theorems because the two propositions about left-invariant and right-invariant metrics require slightly different arguments throughout the proof. The `Metric_space` locale is used for statements about metrics. The

decisive fact that topologies sharing the same base are equal is taken from HOL-Analysis (lemma `openin_topology_base_unique`).

definition *left-invariant-metric* $\Delta \longleftrightarrow$ *Metric-space* (*carrier* G) $\Delta \wedge$
$(\forall \sigma\ \tau\ \varrho.\ \sigma \in$ *carrier* $G \wedge \tau \in$ *carrier* $G \wedge \varrho \in$ *carrier* $G \longrightarrow \Delta\ (\varrho \otimes \sigma)\ (\varrho \otimes \tau) = \Delta\ \sigma\ \tau)$

definition *right-invariant-metric* $\Delta \longleftrightarrow$ *Metric-space* (*carrier* G) $\Delta \wedge$
$(\forall \sigma\ \tau\ \varrho.\ \sigma \in$ *carrier* $G \wedge \tau \in$ *carrier* $G \wedge \varrho \in$ *carrier* $G \longrightarrow \Delta\ (\sigma \otimes \varrho)\ (\tau \otimes \varrho) = \Delta\ \sigma\ \tau)$

theorem *Birkhoff-Kakutani-left*:
assumes *Hausdorff*: *Hausdorff-space T* **and** *first-countable*: *first-countable T*
shows $\exists \Delta.$ *left-invariant-metric* $\Delta \wedge$ *Metric-space.mtopology* (*carrier* G) $\Delta = T$

theorem *Birkhoff-Kakutani-right*:
assumes *Hausdorff*: *Hausdorff-space T* **and** *first-countable*: *first-countable T*
shows $\exists \Delta.$ *right-invariant-metric* $\Delta \wedge$ *Metric-space.mtopology* (*carrier* G) $\Delta = T$

We conclude this section with the corollary that metrizability of a topological group is equivalent to first-countability together with the Hausdorff property.

corollary *Birkhoff-Kakutani-iff*:
shows *metrizable-space T* $\longleftrightarrow$ *Hausdorff-space T* $\wedge$ *first-countable T*

4 Conclusion

In this thesis we presented our formalization and had a detailed look at the proof of the Birkhoff-Kakutani theorem. What is new in our work is the formalization of topological groups which - while present in the libraries of other theorem provers - had been missing in the Isabelle Archive of Formal Proofs (AFP). Furthermore, the AFP had not yet included the matrix groups $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R})$, O_n and SO_n. Moreover, the development of a set-based formalization of uniformities in addition to the type-based notion in the `uniform_space` type class is a new contribution and complements the set-based notion of topologies in HOL-Analysis.

A necessary side effect of working with the `group` locale instead of the `group` type class is that most lemmas and propositions need additional assumptions stating that the elements in question actually belong to the group. This complicates lemma statements and prolongs proofs. It is also unpleasant that the group and its topology are represented by different Isabelle objects with - at first sight - different carrier sets.

Topological groups are a large topic in mathematics, so there is plenty of work which could be done in the future. An important task would be developing the theory of Haar measures on top of the formalization of measures in HOL-Analysis, in particular proving their existence and uniqueness. For this one first needs to introduce the notion of locally compact groups. One could also begin formalizing the theory of Lie groups. This needs the concept of differentiable manifolds which is already included in the AFP [9].

Abbreviations

AFP Archive of Formal Proofs

Bibliography

[1] Alexander Arhangel'skii and Mikhail Tkachenko. *Topological Groups and Related Structures*. Atlantis Studies in Mathematics №1. Atlantis Press, 2008. ISBN: 9789491216350.

[2] Daniel Bump. *Lie Groups*. 2nd ed. Graduate Texts in Mathematics №225. Springer, 2013. ISBN: 9781461480242.

[3] Joo Heon Yoo. *Lie groups, Lie algebras and applications in physics*. University of Chicago. Accessed on 2024-07-21. Sept. 2015. eprint: https://math.uchicago.edu/~may/REU2015/REUPapers/Yoo.pdf.

[4] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*. 1st ed. Lecture Notes in Computer Science №2283. Springer, 2002. ISBN: 9783540433767.

[5] [SW] Niklas Krofta, *Formalization of Topological Groups in Isabelle* 2024. Technical University of Munich. LIC: MIT license. SWHID: ⟨swh:1:dir:884b8e12e3026f8bf0ef2f8c1380e7bfc4717043;origin=https://github.com/nkrofta/Topological-Groups;visit=swh:1:snp:02694e94ad65ef342570f8839c888884451f235c;anchor=swh:1:rev:b09b0789878aa6045ff7de54301568401c8d6311⟩.

[6] Johannes Prem. *Topologische Gruppen und Haar'sches Maß*. Universität Regensburg. Accessed on 2024-07-22. Apr. 2013. eprint: https://homepages.uni-regensburg.de/~prj05723/talk_topogrp_and_haar_measure/TopoGruppen-und-Haarmass.pdf.

[7] Randall (https://math.stackexchange.com/users/464495/randall). *Why is the quotient group a topological group?* Mathematics Stack Exchange. Accessed on 2024-07-23. eprint: https://math.stackexchange.com/q/2424681.

[8] I.M. James. *Topological and uniform spaces*. 1st ed. Undergraduate texts in mathematics. Springer, 1987. ISBN: 9780387964669.

[9] Fabian Immler and Bohua Zhan. "Smooth Manifolds." In: *Archive of Formal Proofs* (Oct. 2018). https://isa-afp.org/entries/Smooth_Manifolds.html, Formal proof development. ISSN: 2150-914x.