Solution Exercise Sheet 5

Exercise 1.(Discrete Subgroups of $\mathbb{R}^n$):

Let $D < \mathbb{R}^n$ be a discrete subgroup. Show that there are $x_1, \dots, x_k \in D$ such that

- $x_1, \dots, x_k$ are linearly independent over $\mathbb{R}$, and
- $D = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_k$, i.e. $x_1, \dots, x_k$ generate D as a $\mathbb{Z}$-submodule of $\mathbb{R}^n$.

Solution: We will prove this by induction on the dimension n.

Let $n = 1$ and let $D < \mathbb{R}$ be a discrete subgroup. Without loss of generality we may assume that $D \neq \{0\}$. Since D is discrete there is $x_1 \in D \setminus \{0\}$ such that $|x_1| = \min\{|x| : x \in D \setminus \{0\}\}$. We claim that $D = \mathbb{Z}x_1$. Suppose there is $y \in D \setminus \mathbb{Z}x_1$. Then there is $k \in \mathbb{Z}$ such that

$$k \cdot x_1 < y < (k+1) \cdot x_1.$$

It follows that $y - k \cdot x_1 \in D$ and $|y - k \cdot x_1| < |x_1|$ which contradicts the minimality of x_1. This shows that $D = \mathbb{Z}x_1$ and finishes the proof of the base case $n = 1$.

Let $n \in \mathbb{N}$ and assume the statement holds for all discrete subgroups of $\mathbb{R}^{n-1}$. Let $D < \mathbb{R}^n$ be a discrete subgroup. Without loss of generality we may assume that $D \neq \{0\}$. There is $x_1 \in D \setminus \{0\}$ such that $\|x_1\| = \min\{\|x\| : x \in D \setminus \{0\}\}$. Consider the quotient $\mathbb{R}^n/\mathbb{R}x_1 \cong \mathbb{R}^{n-1}$ and the projection

$$\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/\mathbb{R} \cdot x_1 \cong \mathbb{R}^{n-1}$$

onto it.

We claim that $D' = \pi(D) < \mathbb{R}^{n-1}$ is a discrete subgroup. We will see this by showing that $V' := \pi(B_r(0))$ is an open neighborhood of $0 \in D'$ such that $V' \cap D' = \{0\}$ where $r := \inf\{\|t \cdot x_1 - y\| : t \in \mathbb{R}, y \in D \setminus \mathbb{Z}x_1\}$.

First of all, we need to see that r is in fact positive. In order to prove this let us verify that

$$r = \inf\{\|t \cdot x_1 - y\| : t \in \mathbb{R}, y \in D \setminus \mathbb{Z}x_1\} = \inf\{\|t \cdot x_1 - y\| : t \in [0,1], y \in D \setminus \mathbb{Z}x_1\}.$$

Clearly, the left-hand-side is less than or equal to the right-hand-side. On the other hand, if $R \geq 0$ such that there are $t \in \mathbb{R}$ and $y \in D \setminus \mathbb{Z}x_1$ satisfying $R \geq \|t \cdot x_1 - y\|$ then also

$$R \geq \|t \cdot x_1 - y\| = \|(t - \lfloor t \rfloor)x_1 - (y - \lfloor t \rfloor x_1)\|;$$

whence there are $s := t - \lfloor t \rfloor \in [0,1]$ and $w := (y - \lfloor t \rfloor x_1) \in D \setminus \mathbb{Z}x_1$ such that $R \geq$

$\|s\cdot x_1 - w\|$. Therefore, the right-hand-side is also less than or equal to the left-hand-side such that they must be equal. Because $\{t\cdot x_1 : t \in [0,1]\} \subset \mathbb{R}^n$ is compact and $D \setminus \mathbb{Z}x_1$ is discrete the infimum on the right-hand-side is in fact a minimum. It is attained at some $t_0 \cdot x_1$ and $y_0 \in D \setminus \mathbb{Z}x_1$. If $r = \|t_0 \cdot x_1 - y_0\| = 0$ then $y_0 = t_0 x_1$ and $t_0 \in (0,1)$ because $y_0 \notin \mathbb{Z}x_1$. But then $\|y_0\| = t_0\|x_1\| < \|x_1\|$ which contradicts the minimality of $\|x_1\|$; whence $r > 0$.

Clearly, $\pi : \mathbb{R}^n \to \mathbb{R}^{n-1}$ is an open map such that $V' = \pi(B_r(0))$ is an open neighborhood of $0 \in \mathbb{R}^{n-1}$. Now, let $x' \in D' \cap V'$, i.e. $x' = \pi(u) = \pi(y)$ for some $u \in B_r(0)$, $y \in D$. Then $y - u \in \mathbb{R}x_1$, i.e. $y - u = t\cdot x_1$ for some $t \in \mathbb{R}$. This implies that

$$\|y - t\cdot x_1\| = \|u\| < r = \inf\{\|y - t\cdot x_1\| : t \in \mathbb{R}, y \in D \setminus \mathbb{Z}x_1\}.$$

We deduce that $y \in \mathbb{Z}x_1 \subset \mathbb{R}x_1$; whence $x' = \pi(y) = 0$ and $V' \cap D' = \{0\}$. Therefore, 0 is an isolated point in D' such that D' is a discrete subgroup of $\mathbb{R}^{n-1}$ as claimed.

By the induction hypothesis there are $x_2', \dots, x_k' \in D' < \mathbb{R}^{n-1}$ which are linearly independent over $\mathbb{R}$ and generate D' as a $\mathbb{Z}$-submodule, i.e. $D' = \mathbb{Z}x_2' \oplus \cdots \oplus \mathbb{Z}x_k'$. We choose for every x_i' a preimage $x_i \in \pi^{-1}(x_i') \cap D$. These $x_1, x_2, \dots, x_k \in D$ are linearly independent over $\mathbb{R}$ and satisfy $D = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_k$. Indeed, let $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ such that

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k = 0. \tag{1}$$

Then

$$\begin{aligned} 0 &= \pi(\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k) \\ &= \underbrace{\lambda_1 \pi(x_1)}_{=0} + \lambda_2 \pi(x_2) + \cdots + \lambda_k \pi(x_k) \\ &= \lambda_2 x_2' + \cdots + \lambda_k x_k'. \end{aligned}$$

Because $x_2', \dots, x_k'$ are linearly independent, $\lambda_2' = \ldots = \lambda_k' = 0$. By (1), $\lambda_1 x_1 = 0$. Finally, since $x_1 \neq 0$ also $\lambda_1 = 0$.

In order to see that $x_1, \dots, x_k$ generate D as a $\mathbb{Z}$-module, let $y \in D$. Then

$$\pi(y) = a_2 x_2' + \cdots + a_k x_k' = a_2 \pi(x_2) + \cdots + a_k \pi(x_k)$$

for some $a_2, \dots, a_k \in \mathbb{Z}$ since $x_2', \dots, x_k'$ generate D' as a $\mathbb{Z}$-module. Considering $y' = a_2 x_2 + \cdots + a_k x_k \in D$ we obtain

$$\pi(y') = \pi(a_2 x_2 + \cdots + a_k x_k) = a_2 \pi(x_2) + \cdots + a_k \pi(x_k) = \pi(y)$$

by linearity such that $y - y' \in D \cap \ker\pi = D \cap \mathbb{R}x_1$.

We claim that $D \cap \ker\pi = \mathbb{Z}x_1$. It is immediate that $\mathbb{Z}x_1 \subseteq D \cap \ker\pi$. To see the other inclusion suppose that there is $t\cdot x_1 \in D$ for some $t \in \mathbb{R} \setminus \mathbb{Z}$. Then $w =$

$(t - \lfloor t \rfloor) \cdot x_1 \in D \setminus \{0\}$ and

$$\|w\| = (t - \lfloor t \rfloor) \cdot \|x_1\| < \|x_1\|$$

in contradiction to the minimality of x_1.

Therefore, $y - y' \in \mathbb{Z}x_1$ and there exists $a_1 \in \mathbb{Z}$ such that

$$y = a_1 x_1 + y' = a_1 x_1 + a_2 x_2 + \cdots + a_k x_k.$$

Hence, $D = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_k$. $\square$

Exercise 2.(Covering maps of Lie Groups):

Let G be a Lie group, let H be a simply connected topological space and let $p : H \to G$ be a covering map.

a) Show that there is a unique Lie group structure on H such that p is a smooth group homomorphism and that the kernel of p is a discrete subgroup of G.

Solution:

Uniqueness:

We will first show uniqueness. To this end suppose that H is equipped with a Lie group structure such that $p : H \to G$ is a smooth homomorphism. Because p is a covering map p is in fact a local diffeomorphism. Therefore every chart (ψ, V) in a smooth atlas of H has to come from a chart (φ, U) of G in the sense that $\psi = \varphi \circ p$ and $V = p^{-1}(U)$ where V is an open subset of H such that $p|_V$ is a diffeomorphism. This shows that the smooth structure on H is unique. Hence we are left to prove that the group structure is unique. Let H' be the topological space H equipped with another Lie group structure such that $p = p' : H' \to G$ is a smooth covering homomorphism. Because both H and H' are simply connected they are both universal coverings of G. Therefore there is a diffeomorphism $\varphi : H \to H'$ sending the neutral element e of H to the neutral element e' of H' such that the following diagram commutes.

$$\begin{tikzcd} H \arrow[rr, "\varphi", "\sim"'] \arrow[dr, "p"] & & H' \arrow[dl, "p'"] \\ & G & \end{tikzcd}$$

We will now show that $\varphi : H \to H'$ is indeed a homomorphism such that H and H' are isomorphic Lie groups. To this end consider the set

$$A = \{(h, g) \in H \times H : \varphi(hg^{-1}) = \varphi(h)\varphi(g)^{-1}\}.$$

Clearly, $(e, e) \in A$ whence $A \neq \emptyset$. Further A is closed since multiplication, inversion and φ are all continuous maps. If we can prove that A is open then $A = H \times H$ because $H \times H$ is connected, i.e. φ is a homomorphism.

Let $(h_0, g_0) \in A$. Further, let $U' \subseteq H'$ be an open neighborhood about $\varphi(h_0 g_0^{-1}) = \varphi(h_0)\varphi(g_0)^{-1}$ such that $p'|_{U'}$ is a diffeomorphism. Let $U \subseteq H \times H$ be an open neighborhood about (h_0, g_0) such that $\varphi(hg^{-1}) \in U'$ and $\varphi(h)\varphi(g)^{-1} \in U'$ for all $(h, g) \in U$; this is possible because all maps are again continuous. Then

$$\begin{aligned} p'(\varphi(hg^{-1})) = p(hg^{-1}) = p(h)p(g)^{-1} &= p'(\varphi(h))p'(\varphi(g))^{-1} \\ &= p'(\varphi(h)\varphi(g)^{-1}) \end{aligned}$$

for all $h, g \in U$ where we have used that p and p' are homomorphisms. By construction $\varphi(hg^{-1}), \varphi(h)\varphi(g)^{-1} \in U'$ and since $p'|_{U'}$ is bijective we get $\varphi(hg^{-1}) = \varphi(h)\varphi(g)^{-1}$ for all $h, g \in U$. Hence, $(h_0, g_0) \in U \subseteq A$ and A is open because $(h_0, g_0) \in A$ were arbitrary.

It follows that $\varphi : H \to H'$ is a Lie group isomorphism.

<u>Existence:</u>

First, we may equip H with a smooth structure as described above such that p becomes a smooth covering map. It is not hard to verify that with $p : H \to G$ also $p \times p : H \times H \to G \times G$ is a smooth covering map. In particular, since H is simply connected also $H \times H$ is simply connected such that $p \times p : H \times H \to G \times G$ is a universal covering. We will now lift the multiplication and inversion maps to H and show that they define a group structure on H.

Let $m : G \times G \to G$ and $i : G \to G$ denote the multiplication and inversion maps of G, respectively, and let $\tilde{e}$ be an arbitrary element of the fiber $p^{-1}(e) \subseteq H$. Since $p \times p : H \times H \to G \times G$ is a universal covering the map $m \circ (p \times p) : H \times H \to G$ has a unique lift $\tilde{m} : H \times H \to H$ satisfying $\tilde{m}(\tilde{e}, \tilde{e}) = \tilde{e}$ and $p \circ \tilde{m} = m \circ (p \times p)$:

$$\begin{tikzcd} H \times H \arrow[r, "\tilde{m}"] \arrow[d, "p \times p"] & H \arrow[d, "p"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

Because p is a local diffeomorphism and $p \circ \tilde{m} = m \circ (p \times p)$ is smooth also $\tilde{m}$ is smooth. By the same reasoning, $i \circ p : H \to G$ has a smooth lift $\tilde{i} : H \to G$ satisfying $\tilde{i}(\tilde{e}) = \tilde{e}$ and $p \circ \tilde{i} = i \circ p$:

$$\begin{tikzcd} H \arrow[r, "\tilde{i}"] \arrow[d, "p"] & H \arrow[d, "p"] \\ G \arrow[r, "i"] & G \end{tikzcd}$$

We define multiplication and inversion in H by $xy = \tilde{m}(x, y)$ and $x^{-1} = \tilde{i}(x)$.

By the above commutative diagrams we obtain

$$p(xy) = p(x)p(y), \qquad p(x^{-1}) = p(x)^{-1}.$$

It remains to show that H is a group with these operations, for then it is a Lie group because $\tilde{m}$ and $\tilde{i}$ are smooth and the above relations imply that p is a homomorphism.

First we show that $\tilde{e}$ is an identity for multiplication in H. Consider the map $f : H \to H$ definbed by $f(x) = \tilde{e}x$. Then

$$p(f(x)) = p(\tilde{e})p(x) = ep(x) = p(x),$$

so f is a lift of $p : H \to G$. The identity map Id_H is another lift of p, and it agrees with f at a point because $f(\tilde{e}) = \tilde{m}(\tilde{e}, \tilde{e}) = \tilde{e}$, so the unique lifting property of covering maps implies that $f = \mathrm{Id}_H$, or equivalently, $\tilde{e}x = x$ for all $x \in H$. The same argument shows that $x\tilde{e} = x$.

Next, to show that multiplication in H is associative, consider the two maps $\alpha_L, \alpha_R : H \times H \times H \to H$ defined by

$$\alpha_L(x,y,z) = (xy)z, \quad \alpha_R(x,y,z) = x(yz).$$

Then

$$p(\alpha_L(x,y,z)) = (p(x)p(y))p(z) = p(x)(p(y)p(z)) = p(\alpha_R(x,y,z)),$$

so α_L and α_R are both lifts of the same map $\alpha(x,y,z) = p(x)p(y)p(z)$. Because α_L and α_R agree at $(\tilde{e}, \tilde{e}, \tilde{e})$, they are equal. A similar argument shows that $x^{-1}x = xx^{-1} = \tilde{e}$, so $\tilde{G}$ is a group.

Finally, we need to see that $\ker p$ is a discrete subgroup. To this end choose an open neighborhood $U \subseteq G$ of $e \in G$ such that $p^{-1}(U)$ is the disjoint union of open subsets $\{V_i\}_{i \in I}$ and $p|_{V_i} : V_i \to U$ is a diffeomorphism. In particular, $\ker p = p^{-1}(e) \subseteq \bigsqcup_{i \in I} V_i$ and every $x \in \ker p$ is contained in only one of the V_i. Hence, $\tilde{e} \in V_{i_0}$ for some $i_0 \in I$ and $(\ker p \setminus \{\tilde{e}\}) \cap V_{i_0} = \emptyset$ such that $\tilde{e}$ is an isolated point in $\ker p$. This implies that $\ker p$ is a discrete subgroup of H. □

b) Show that p is a local isomorphism of Lie groups and that dp is an isomorphism of Lie algebras when H is equipped with the Lie group structure from part a).

Solution: Note that dp is a Lie algebra homomorphism since p is a smooth homomorphism. Because p is additionally a smooth covering map there are open neighborhoods $U \subseteq G$ of e and $V \subseteq H$ of $\tilde{e}$ such that $p|_V : V \to U$ is a diffeomorphism. In particular, $dp : T_{\tilde{e}}H \cong \mathfrak{h} \to T_eG \cong \mathfrak{g}$ is bijective such that dp is a Lie algebra isomorphism. By a lemma from the lecture every local homomorphism with bijective $dp : \mathfrak{h} \to \mathfrak{g}$ is a local isomorphism. $\square$

c) Let H, G be arbitrary Lie groups and let G be connected. Further, let $\varphi : H \to G$ be a Lie group homomorphism. Show that φ is a covering map if and only if $d\varphi : \mathfrak{h} \to \mathfrak{g}$ is an isomorphism.

Solution: First suppose that φ is a covering map. The same proof as for part b) applies here such that $d\varphi$ is indeed an isomorphism.

Now, assume that $\varphi : H \to G$ is a smooth homomorphism such that $d\varphi : \mathfrak{h} \to \mathfrak{g}$ is an isomorphism. This means that $d_{\tilde{e}}\varphi : T_{\tilde{e}}H \to T_eG$ is invertible such that by the inverse function theorem there are open neighborhoodes $U \subseteq G$ about $e \in G$ and $V \subseteq H$ about $\tilde{e} \in H$ such that $\varphi|_V : V \to U$ is a diffeomorphism. Because G is connected the open neighborhood U about $e \in G$ generates G and it follows easily that $\varphi : H \to G$ is surjective.

Now, choose a symmetric open neighborhood $W \subseteq V$ about $\tilde{e} \in H$ such that $W^2 \subseteq V$. Consider the open subset $U' := \varphi(W) \subseteq U$. We claim that $\varphi^{-1}(U') = \bigsqcup_{h\in\ker\varphi} Wh$ and $\varphi|_{Wh} : Wh \to U'$ is a diffeomorphism for all $h \in \ker\varphi$. Because $h \in \ker\varphi$ we have that $\varphi \circ R_h = \varphi$. Further $\varphi : W \to U'$ is a diffeomorphism such that also $\varphi : Wh \to U'$ is a diffeomorphism. Also,

$$\begin{aligned} x \in \varphi^{-1}(U') = \varphi^{-1}(\varphi(W)) &\iff \varphi(x) \in \varphi(W) \\ \iff \exists w \in W : \varphi(x) = \varphi(w) &\iff \exists w \in W : \varphi(w^{-1}x) = e \\ \iff \exists w \in W : w^{-1}x \in \ker\varphi &\iff x \in \bigcup_{h\in\ker\varphi} Wh, \end{aligned}$$

such that $\varphi^{-1}(U') = \bigcup_{h\in\ker\varphi} Wh$. Finally, if $Wh \cap Wh' \neq \emptyset$ for some $h, h' \in \ker\varphi$ then there are $w, w' \in W$ such that $wh = w'h'$, i.e. $h^{-1}h' \in W^2 \subseteq V$. Because $\varphi|_V : V \to U$ is injective and also $\varphi(h^{-1}h') = \varphi(h^{-1})\varphi(h') = e$ it follows that $h^{-1}h' = \tilde{e}$, or equivalently $h = h'$. Thus, $\bigcup_{h\in\ker\varphi} Wh$ is a disjoint union as claimed.

Using this together with the fact that φ is a homomorphism proves that φ is a covering map. $\square$

Remark: Part a) and b) also work if H is not simply connected.

Exercise 3.(Abstract Subgroups as Lie Subgroups):

Let H be an abstract subgroup of a Lie group G and let $\mathfrak{h}$ be a subspace of the Lie algebra $\mathfrak{g}$ of G. Further let $U \subseteq \mathfrak{g}$ be an open neighborhood of $0 \in \mathfrak{g}$ and let $V \subseteq G$ be an open neighborhood of $e \in G$ such that the exponential map $\exp : U \to V$ is a diffeomorphism satisfying $\exp(U \cap \mathfrak{h}) = V \cap H$. Show that the following statements hold:

a) H is a Lie subgroup of G with the induced relative topology;

b) $\mathfrak{h}$ is a Lie subalgebra of $\mathfrak{g}$;

c) $\mathfrak{h}$ is the Lie algebra of H.

Solution: We will first show that H is an embedded submanifold of G. For that it is enough to check that there are slice charts about every point $h \in H$. For $h = e$ choose any linear isomorphism $E : \mathfrak{g} \to \mathbb{R}^m$ that sends $\mathfrak{h}$ to $\mathbb{R}^k$ where $\dim G = \dim \mathfrak{g} = m$ and $\dim \mathfrak{h} = k$. The composite map

$$\varphi = E \circ \exp^{-1} : \exp U = V \longrightarrow \mathbb{R}^m$$

is then a smooth chart for G, and

$$\varphi((\exp(U) \cap H) = E(U \cap \mathfrak{h})$$

is the slice obtained by setting the last $m-k$ coordinates equal to zero. Moreover, if $h \in H$ is arbitrary, the left translation map L_h is a diffeomorphism from $\exp(U)$ to a neighborhood of h. Since H is a subgroup, $L_h(H) = H$, and so

$$L_h((\exp U) \cap H) = L_h(\exp U) \cap H,$$

and $\varphi \circ L_h^{-1}$ is easily seen to be a slice chart for H in a neighborhood of h. Thus H is an embedded submanifold of G.

We will now make use of the following Lemma:

Lemma: Let G be a Lie group, and suppose $H \subseteq G$ is a subgroup that is also an embedded submanifold. Then H is a Lie subgroup.

Proof: We need only check that multiplication $m : H \times H \to H$ and inversion $i : H \to H$ are smooth maps. Because multiplication is a smooth map from $G \times G$ to G its restriction is clearly smooth from $H \times H$ to G. Because H is a subgroup, multiplication takes $H \times H$ to H. Using local slice charts for H in G it follows easily that $m : H \times H \to H$ is smooth. The same argument works for inversion. □

This proves a). We will prove b) and c) in one go:

Denote by $\iota : H \to G$ the embedding from H into G and let $\mathfrak{b} \subseteq \mathfrak{g}$ be a complementary subspace of $\mathfrak{h}$ such that $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{b}$. This yields the following commutative diagram:

$$\begin{array}{ccc}
\mathrm{Lie}(H) & \xrightarrow{d_e\iota} & \mathfrak{g} = \mathfrak{h} \oplus \mathfrak{b} \\
\downarrow{\scriptstyle \exp} & & \downarrow{\scriptstyle \exp} \\
H & \xrightarrow{\iota} & G
\end{array}$$

By construction of the slice charts of H it is immediate that $d_e\iota$ is an isomorphism of vector spaces from $\mathrm{Lie}(H)$ to $\mathfrak{h}$. Furthermore, ι is a Lie group homomorphism whence its differential $d_e\iota$ induces a Lie algebra homomorphism. Therefore $d_e\iota$ is a Lie algebra isomorphism from $\mathrm{Lie}(H)$ to $\mathfrak{h}$. Under the identification $H \cong \iota(H) \leq G$ we get $\mathrm{Lie}(H) \cong \mathfrak{h}$. This proves b) and c). □

Exercise 4.(Lie Group homomorphisms and their differentials):

Let G be a connected Lie group, let H be a Lie group and let $\varphi, \psi \colon G \to H$ be Lie group homomorphisms.

Show that $\varphi = \psi$ if and only if $d\varphi = d\psi$.

Solution: If $\varphi = \psi$ then clearly $d\varphi = d\psi$. Thus it suffices to prove the converse direction.

Assume that $d\varphi = d\psi$. We consider the set

$$A := \{g \in G \,|\, \varphi(g) = \psi(g)\},$$

and we need to show that $A = G$. Note that A is closed and contains the identity element $e \in A$. Because G is connected we are left to show that A is open.

Let $g_0 \in A$. Recall that there is an open neighborhood $0 \in V \subseteq T_eG \cong \mathfrak{g}$ and an open neighborhood $e \in U \subseteq G$ such that $\exp\colon U \to V$ is a diffeomorphism. Let $g = g_0 v \in g_0 V$ with $v = \exp(X)$ for some $X \in U$. Then

$$\begin{aligned}
\varphi(g) &= \varphi(g_0)\varphi(\exp(X)) \\
&= \varphi(g_0)\exp(d\varphi(X)) \\
&= \psi(g_0)\exp(d\psi(X)) \\
&= \psi(g_0)\psi(\exp(X)) = \psi(g),
\end{aligned}$$

whence $g_0 V \subseteq A$.

Because g_0 was arbitrary, A is open. □

Exercise 5.(Surjectivity of the Matrix Exponential):

Let $\mathrm{Exp} : \mathfrak{gl}(n,\mathbb{R}) \cong \mathbb{R}^{n\times n} \to \mathrm{GL}(n,\mathbb{R})$ be the matrix exponential map given by the power series

$$\mathrm{Exp}(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Consider the Lie subgroup of upper triangular matrices $N(n) < \mathrm{GL}(n,\mathbb{R})$ with its Lie algebra $\mathfrak{n}(n) < \mathfrak{gl}(n,\mathbb{R})$ of strictly upper triangular matrices; cf. exercise sheet 4 problem 3.

Show that $\mathrm{Exp}|_{\mathfrak{n}(n)} : \mathfrak{n}(n) \to N(n)$ is surjective.

Hint: Consider the partially defined matrix logarithm $\mathrm{Log} : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ given by

$$\operatorname{Log}(I+A) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{A^n}{n}.$$

Try to give answers to the following questions and then conclude:

What is its radius of convergence r about I? Why is it a right-inverse of Exp on the ball $B_r(I)$ of radius r about I? Why is there no problem for matrices that are in $N(n)$ but not in $B_r(I)$?

In order to answer the last question prove that $A^n = 0$ for all $A \in \mathfrak{n}(n)$.

Solution: Note that

$$r = \lim_{n\to\infty} \left| \frac{(-1)^{n-1}}{n} \cdot \frac{n+1}{(-1)^n} \right| = 1$$

such that the power series $\operatorname{Log}(I+A)$ converges absolutely for every $A \in \mathbb{R}^{n\times n}$ with $\|A\| < 1$ as in the complex case.

For all complex numbers $z \in \mathbb{C}$ with $|z| < 1$ we have

$$e^{\log(1+z)} = 1 + z. \tag{2}$$

Recall that

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!} \qquad \forall z \in \mathbb{C}$$

and

$$\log(1+z) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{z^n}{n} \qquad \forall z \in B_1(0) \subset \mathbb{C}.$$

Writing the composition $e^{\log(1+z)}$ as a power series we obtain

$$e^{\log(1+z)} = \sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{n=1}^{\infty} (-1)^{n-1} \frac{z^n}{n} \right)^k = \sum_{k=0}^{\infty} d_k z^k$$

for all $z \in B_1(0) \subset \mathbb{C}$ for some $d_k \in \mathbb{R}$, where one uses succesively the Cauchy product rule for power series to compute the power series representation of $\left(\sum_{n=1}^{\infty} (-1)^{n-1} \frac{z^n}{n}\right)^k$ and then uses the fact that the series converges absolutely for $|z| < 1$ to reorder it and to obtain the coefficients for each z^k.

Comparing coefficients in (2) then yields that $d_0 = d_1 = 1$ and $d_k = 0$ for all $k > 1$.

Let us now write $\operatorname{Exp}(\operatorname{Log}(I+A))$ as well as a power series

$$\operatorname{Exp}(\operatorname{Log}(I+A)) = \sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{n=1}^{\infty} (-1)^{n-1} \frac{A^n}{n} \right)^k = \sum_{k=0}^{\infty} d_k A^k$$

for all $z \in B_1(0) \subset \mathbb{C}$, where one uses succesively the Cauchy product rule for power series to compute the power series representation of $\left(\sum_{n=1}^{\infty} (-1)^{n-1} \frac{z^n}{n}\right)^k$ and then uses the fact that the series converges absolutely for $|z| < 1$ to reorder it and to obtain the coefficients for each z^k as above.

Observe that the coefficients $d_k \in \mathbb{R}$ are the same as in the complex case! This is due to the fact that they arise from the same computation with power series (Cauchy product rule and reordering accordingly). Hence, $d_0 = d_1 = 1$ and $d_k = 0$ for all $k > 1$ such that

$$\operatorname{Exp}(\operatorname{Log}(I + A)) = I + A$$

for every $A \in \mathbb{R}^{n\times n}$ with $\|A\| < 1$. [1]

Finally, observe that every $X \in N(n)$ can be written as $X = I + A$ where $A \in \mathfrak{n}(n)$. Furthermore, since A is strictly upper triangular it maps

$$A|_{V_i} : V_i \to V_{i-1}$$

where $V_i = \operatorname{span}\{e_1, \dots, e_i\}$, $V_0 = \{0\}$ for every $i = 1, \dots, n$. In particular,

$$A^n : \mathbb{R}^n = V_n \to V_{n-1} \to \cdots \to V_0 = \{0\}$$

such that $A^n = 0$.

That means that for every $A \in \mathfrak{n}(n)$ the power series $\operatorname{Log}(I + A)$ is actually a polynomial in A taking values in $\mathfrak{n}(n)$:

$$\operatorname{Log}(I + A) = \sum_{k=1}^{n-1} (-1)^{k-1} \frac{A^k}{k} \in \mathfrak{n}(n).$$

Because $\operatorname{Log}(I + A)$ is again in $\mathfrak{n}(n)$ also $\operatorname{Exp}(\operatorname{Log}(I + A))$ becomes a polynomial p in A:

$$\operatorname{Exp}(\operatorname{Log}(I + A)) = \sum_{k=0}^{\infty} \underbrace{\frac{1}{k!} \left(\sum_{l=1}^{n-1} (-1)^{l-1} \frac{A^l}{l} \right)^k}_{=0,\ \text{if } k \geq n} = \sum_{k=0}^{n-1} \frac{1}{k!} \left(\sum_{l=1}^{n-1} (-1)^{l-1} \frac{A^l}{l} \right)^k =: p(A)$$

Now observe that $\|tA\| < 1$ for all $t \in I_A := (-\|A\|^{-1}, \|A\|^{-1}) \subset \mathbb{R}$. Hence,

$$p(tA) = \operatorname{Exp}(\operatorname{Log}(I + tA)) = I + tA$$

for all $t \in I_A$. The left-hand-side and the right-hand-side are both polynomials in t which coincide on an open subset of $\mathbb{R}$. Thus they have to coincide everywhere; in particular

$$\operatorname{Exp}(\operatorname{Log}(I + A)) = I + A$$

[1] The reasoning applied here can be generalized. In fact, there are theorems that relate identities of complex power series to identities of power series in Banach algebras; see e.g. Königsberger: „Analysis 2", ch. 1.6 and Königsberger: „Analysis 2", Exercise 18, p. 44

for $t = 1$. This shows that $\mathrm{Log}|_{N(n)}$ is a well-defined right-inverse of $\mathrm{Exp}|_{\mathfrak{n}(n)}$. $\square$

Exercise 6.(Multiplication and exp):

Let G be a Lie group with Lie algebra $\mathfrak{g}$. Show that for all $X, Y \in \mathfrak{g}$ and small enough $t \in \mathbb{R}$

$$\exp(tX)\exp(tY) = \exp(t(X+Y) + O(t^2))$$

where $O(t^2)$ is a differentiable $\mathfrak{g}$-valued function such that $\frac{O(t^2)}{t^2}$ is bounded as $t \to 0$.

Solution: Let $X, Y \in \mathfrak{g}$. Let $U \subseteq \mathfrak{g}$ be an open neighborhood about 0 and $V \subseteq G$ be an open neighborhood about $e \in G$ such that $\exp : U \to V$ is a diffeomorphism. Choose $\varepsilon > 0$ such that $\exp(tX)\exp(tY) \in V$ for all $t \in (-\varepsilon, \varepsilon)$.

Because $\exp(tX)\exp(tY) \in V$, for all $|t| < \varepsilon$, and $\exp : U \to V$ is a diffeomorphism, we find a smooth $\mathfrak{g}$-valued function $Z : (-\varepsilon, \varepsilon) \to \mathfrak{g}$ such that

$$\exp(tX)\exp(tY) = \exp(Z(t))$$

for all $|t| < \varepsilon$.

By Taylor's theorem we may write

$$Z(t) = Z(0) + tZ'(0) + O(t^2)$$

where $O(t^2)$ is a smooth $\mathfrak{g}$-valued function such that $\frac{O(t^2)}{t^2}$ is bounded as $t \to 0$. Setting $t = 0$ yields

$$\exp(0) = e = \exp(0 \cdot X)\exp(0 \cdot Y) = \exp(Z(0))$$

and because $\exp : U \to V$ is bijective we have $Z(0) = 0$.

Let $f \in C^\infty(G)$. Then by the chain rule

$$\begin{aligned}
\frac{d}{dt}\Big|_{t=0} f(\exp(tX)\exp(tY)) &= \frac{d}{dt}\Big|_{t=0} f(\exp(tX)\exp(0 \cdot Y)) + \frac{d}{dt}\Big|_{t=0} f(\exp(0 \cdot X)\exp(tY)) \\
&= \frac{d}{dt}\Big|_{t=0} f(\exp(tX)) + \frac{d}{dt}\Big|_{t=0} f(\exp(tY)) \\
&= Xf + Yf,
\end{aligned}$$

and

$$\begin{aligned}
\frac{d}{dt}\Big|_{t=0} f(\exp(tX)\exp(tY)) &= \frac{d}{dt}\Big|_{t=0} f(\exp(Z(t)) \\
&= Z'(0)f
\end{aligned}$$

identifying $\mathfrak{g} \cong T_0\mathfrak{g}$. Therefore $Z'(0) = X + Y \in \mathfrak{g}$ and

$$\exp(tX)\exp(tY) = \exp(Z(t)) = \exp(tZ'(0) + O(t^2)) = \exp(t(X+Y) + O(t^2))$$

for all $|t| < \varepsilon$. $\square$