3.4 The exponential map

The exponential map of a Lie group is a powerful computational tool that links a Lie group to its Lie algebra. It is obtained from the simple observation that a left invariant vector field generates a one parameter group of diffeomorphisms of a special type.

We will start by discussing the special case of $GL(n,\mathbb{R})$ which requires less background from differential geometry. In this case, the Lie group exponential turns out to be the matrix exponential.
↪ We will prove this statement later!

Choose any norm $\| \ \|$ on $\mathbb{R}^n$ and endow $M_{n\times n}(\mathbb{R})$ with the so called operator norm

$$\|A\| := \sup_{\|v\| \leq 1} \|Av\|.$$

The operator norm satisfies $\|AB\| \leq \|A\| \, \|B\|$.

Proposition 3.44

1) The series $\sum_{n=0}^{\infty} \frac{A^n}{n!}$ converges uniformly on balls with finite radius in $M_{n,n}(\mathbb{R})$ to a smooth map called Exp. In fact Exp is real analytic.

2). For all A, B with $[A,B] = 0$

$$\mathrm{Exp}(A+B) = \mathrm{Exp}(A)\cdot\mathrm{Exp}(B).$$

In particular Exp takes values in $GL(n,\mathbb{R})$.

3) For all $A \in M_{n,n}(\mathbb{R})$ the map

$$\phi : \mathbb{R} \longrightarrow GL(n,\mathbb{R})$$
$$t \longmapsto \mathrm{Exp}(tA)$$

is a smooth homomorphism with $\phi'(0) = A$.

4) Any smooth homomorphism

$$\psi : \mathbb{R} \longrightarrow GL(n,\mathbb{R})$$

is of the form $\psi(t) = \mathrm{Exp}(t\,\dot\psi(0))$

Proof

1) For all A with $\|A\| \le R$ and $N \geq 1$,

we have $\left\| \frac{A^N}{N!} \right\| \leq \frac{R^N}{N!}$

The uniform convergence of the series on compact sets follows since $\sum \frac{R^N}{N!} < \infty$.

In order to show the uniform convergence of the derivatives we note that:

$$\frac{\partial}{\partial x_{ij}} X^n = \sum_{k_1+k_2=n-1} X^{k_1} E_{ij} X^{k_2} \qquad (*)$$

Hence $\left\| \frac{\partial}{\partial x_{ij}} X^n \right\| \leq n \cdot \| X^{n-1} \|$.

Applying $(*)$ iteratively it is possible to get analogous estimates for higher order partial derivatives, and show that for all $K \in \mathbb{N}$ and all partial derivatives $\frac{\partial^I}{\partial x_I}$ of order K.

$$\sum_{n=0}^{\infty} \frac{\partial^I}{\partial x_I} \frac{X^n}{n!}$$

converges uniformly on compact sets. Hence Exp is smooth. A similar argument proves real analyticity. $\square$

2) If $AB = BA$ then:

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k}.$$

Can use this to prove (commutativity) not true in general!

In particular:

$$I = \operatorname{Exp}(0) = \operatorname{Exp}(A) \cdot \operatorname{Exp}(-A),$$

which shows that Exp takes values in $GL(n,\mathbb{R})$.

3) Follows immediately from 1) and 2).

uses derivative of the power series. End of lecture

4) Let $\varphi : \mathbb{R} \longrightarrow GL(n,\mathbb{R})$ be a smooth homomorphism. Then:

$$\varphi'(t) = \frac{d}{ds}\Big|_{s=0} \varphi(t+s)$$

$$= \frac{d}{ds}\Big|_{s=0} \varphi(t)\,\varphi(s)$$

$$= \varphi(t)\,\dot{\varphi}(0)$$

ODE on $M_{n\times n}(\mathbb{R})$.

Note that $\frac{d}{dt}\Big|_{t=0} \operatorname{Exp}(t\,\dot\psi(0)) = \dot\psi(0)$ by 3).

Hence the statement follows by uniqueness of solutions of ODEs. $\square$

Now we turn to the construction of the exponential map for a general Lie group.

We need to recall an existence result about integral curves of smooth vector fields.

$\boxed{\text{Definition 3.45}}$ [Integral curve]

An integral curve of a smooth vector field X on M is a smooth map $\gamma : I \longrightarrow M$ with
$$\dot\gamma(t) = X_{\gamma(t)} \qquad \forall\, t \in I.$$

Here $I \subset \mathbb{R}$ is an open interval and
$$\dot\gamma(t) := (D_t\gamma)(1) \qquad 1 \in T_t\mathbb{R}.$$

The fundamental existence and uniqueness theorem for first order ordinary differential equations in $\mathbb{R}^n$ implies (see for instance [Boothby "An introduction to Differentiable Manifolds and Riemannian Geometry", Chapter IV.4]:

Theorem 3.46

Let $X \in Vect^{\infty}(M)$. For every $m \in M$, there exist $a(m), b(m) \in \mathbb{R} \cup \{\pm\infty\}$ and a smooth curve

$$\gamma_m : (a(m), b(m)) \longrightarrow M.$$

such that:

1). $0 \in (a(m), b(m))$ and $\gamma(0) = m$.
2) γ_m is an integral curve of X
3) If $\mu : (c,d) \longrightarrow M$. is a smooth curve satisfying 1) and 2) then: $(c,d) \subset (a(m), b(m))$ and

$$\gamma|_{(c,d)} = \mu .$$

Definition 3.47

The vector field $X \in Vect^{\infty}(M)$ is complete if $\forall\, m \in M$. $(a(m), b(m)) = \mathbb{R}$.

that is, the integral curves given by Theorem 3.46 are defined on $\mathbb{R}$.

$$\boxed{\text{Proposition 3.48}}$$

Let $X \in \mathrm{Vect}^{\infty}(M)$ be complete. Then the map

$$\Phi^X : \mathbb{R} \times M \longrightarrow M$$
$$(t, m) \longmapsto \gamma_m(t)$$

is a smooth map satisfying

$$(*) \qquad \Phi^X(t_1 + t_2, m) = \Phi^X(t_1, \Phi^X(t_2, m)) \qquad \forall t_1, t_2 \in \mathbb{R}, \; \forall m \in M.$$

One calls $t \longmapsto \Phi^X(t, \cdot)$ a 1-parameter family of diffeomorphisms.

Check that they are diffeomorphisms!

Proof

We prove the "semigroup law" $(*)$.

The map $t \longmapsto \gamma_m(t_2 + t)$ is an integral curve of X such that $0 \longmapsto \gamma_m(t_2)$. By the uniqueness part of Theorem 3.46. we get:

$$\gamma_m(t_2+t) = \gamma_{\gamma_m(t_2)}(t)$$

Reformulating this in terms of Φ^X gives (*). $\blacksquare$

The proof of the smoothness of the flow map Φ^X follows from the smooth dependence from the initial conditions of solutions of ODEs in $\mathbb{R}^n$, see again [Boothby, Chapter IV.4] for the details $\square$

We can use flows of vector fields to compute derivatives of other vector fields.

Given a (smooth) vector field X on M and a smooth function $f: M \to \mathbb{R}$, we already defined the derivative of f in the direction of X by $X_p(f)$

This generalizes from $\mathbb{R}^n$ to an arbitrary manifold the notion of directional derivative of a function.

If we wish to determine the rate of change of a vector field Y at $p \in M$ in the direction of X_p we get into troubles as soon as we leave $\mathbb{R}^n$ as there is no clear way to compare the values of Y at different points as we would like to do in order to compute its rate of change.

A key observation is the following. Assume for the sake of simplicity that X is complete. Consider its flow Φ^X. Set $\Phi^X_t := \Phi^X(t, \cdot)$.

For each $p \in M$ and each $t \in \mathbb{R}$ there is an induced isomorphism

$$D_p \Phi^X_t : T_p M \longrightarrow T_{\Phi^X_t(p)} M .$$

We can use these isomorphisms to compare values of Y at different points. This leads to the following

Definition 3.49

Let $X, Y \in \mathrm{Vect}^{\infty}(M)$ and assume that they are complete for simplicity. Then the Lie derivative of Y with respect to X at p is:

$$(L_X Y)_p := \lim_{t \to 0} \frac{1}{t}\left[\left(D_{\Phi^X_t(p)} \Phi^X_{-t}\right)\left(Y_{\Phi^X_t(p)}\right) - Y_p\right]$$

Then we have the following:

Theorem 3.50

Under the same assumptions above. it holds

$$L_X Y = [X, Y]$$

We address the reader to [Boothby, Thm 7.8 Chapter IV] for a proof.

This new perspective on the Lie bracket is very helpful for proving the following

Proposition 3.51

Let $X, Y \in \mathrm{Vect}^\infty(M)$ be complete. Then $\Phi^X_t \circ \Phi^Y_s = \Phi^Y_s \circ \Phi^X_t$ $\forall t, s \in \mathbb{R}$ if and only if $[X, Y] = 0$.

———— o ————

We come back to Lie groups and invariant vector fields.

Proposition 3.52

Let G be a Lie group.

1) Left invariant vector fields are complete.

2) For every $v \in T_eG$ let $v^L \in \mathrm{Vect}^\infty(G)^G$ be the corresponding left invariant vector field and $\varphi_v : \mathbb{R} \longrightarrow G$ be the integral curve of v^L through e. Then φ_v is a smooth homomorphism.

3) The one parameter group of

diffeomorphisms

$$\Phi^{v^L} : \mathbb{R} \times G \longrightarrow G.$$

is given by $\Phi^{v^L}(t,g) = g\,\varphi_v(t)$.

Proof

Let $\gamma_e : (a(e), b(e)) \longrightarrow G$ be the integral curve of v^L through e given by Theorem 3.46. We claim that

(*) $\gamma_g(t) := g\,\gamma_e(t)$, $t \in (a(e), b(e))$

is an integral curve of v^L through g.

Indeed:

$$\dot{\gamma}_g(t) = D_{\gamma_e(t)} L_g (\dot{\gamma}_e(t)) = D_{\gamma_e(t)} L_g (v^L_{\gamma_e(t)})$$

γ_e is an integral curve.

$$= v^L_{g\gamma_e(t)}$$

v^L is left-invariant by definition

Let now $\delta > 0$ be such that $(-\delta, \delta) \subset (a(e), b(e))$ and define.

$$\gamma(t) := \begin{cases} \gamma_e(t) & t \in (a(e), b(e)) \\ \gamma_e(\delta) \cdot \gamma_e(t-\delta) & t \in (a(e)+\delta, b(e)+\delta) \end{cases}$$

This curve γ is well-defined since by $(*)$
$t \mapsto \gamma_e(t)$ and $t \mapsto \gamma_e(\delta) \cdot \gamma_e(t-\delta)$
are both integral curves of v^L through
$\gamma_e(\delta)$, hence they coincide on any
common interval of definition by
the uniqueness part of Theorem 3.46.

It follows that γ is an integral curve of v^L
through e defined on $(a(e), b(e)+\delta)$,
which by Theorem 3.46 again implies
that $b(e) = +\infty$.
A similar argument gives $a(e) = -\infty$.

Thus by $(*)$, v^L is complete. In particular
Φ^{v^L} is defined on $\mathbb{R} \times G$ and it follows
from $(*)$ again that:

$$\Phi^{v^L}(t,g) = g \cdot \Phi^{v^L}(t,e).$$

This completes the proofs of 1) and 3).

Concerning 2) since Φ^{v^L} is a 1-

parameter group of diffeomorphisms

$$\Phi(t_1+t_2,g) = \Phi(t_1,\Phi(t_2,g))$$

$$3) \rightarrow = \Phi(t_2,g)\,\Phi(t_1,e)$$

Since obviously $t_1+t_2 = t_2+t_1$ we obtain.

$$\Phi(t_1+t_2,e) = \Phi(t_1,e)\,\Phi(t_2,e)$$

which completes the proof of 2) since.

$$\rho_v(t) = \Phi^{v^L}(t,e) \qquad \square$$

In this context it seems natural to introduce the following.

Definition 3.53

A one parameter group in G is a smooth homomorphism $\mathbb{R} \longrightarrow G$.

We have seen thanks to Proposition 3.52, that a tangent vector $v \in T_eG$ leads via the corresponding left-invariant vector field. to a one parameter group

$\varphi_v : \mathbb{R} \longrightarrow G$

Also the converse is true. Namely:

Corollary 3.54.

If $\varphi : \mathbb{R} \longrightarrow G$ is a one parameter group then $\varphi = \varphi_v$ where $v = \dot{\varphi}(0)$.

<u>Proof</u>

Let $v := \dot{\varphi}(0) \in T_e G$ and v^L be the corresponding left-invariant vector field.

We have.

$$\dot{\varphi}(t) = \frac{d}{ds}\Big|_{s=0} \varphi(t+s)$$

φ is homomorphism

$$= \frac{d}{ds}\Big|_{s=0} \varphi(t)\varphi(s)$$

Definition of v^L.

$$= D_e L_{\varphi(t)} (\underbrace{\dot{\varphi}(0)}_{v}) = v^L_{\varphi(t)}$$

Hence φ is an integral curve through e of v^L and therefore $\varphi = \varphi_v$ $\square$

Exercise. 3.55.

understand one parameter groups in $(\mathbb{R}^n, +)$ and in T^2.

We are now ready to define the exponential on general Lie groups.

Definition 3.56

Let G be a Lie group with Lie algebra $\mathfrak{g}$. The exponential map

$$\exp_G : \mathfrak{g} \longrightarrow G$$

is defined by $\exp_G(v) := \varphi_v(1)$ where φ_v is the integral curve of v^L through e.

Corollary 3.57

The following properties hold:

1) $\exp_G(tv) = \varphi_v(t) \quad \forall t \in \mathbb{R}$
$\forall v \in \mathfrak{g}$

2). If $v, w \in \mathfrak{g}$ satisfy $[v, w] = 0$ then $\exp_G(v+w) = \exp_G(v)\exp_G(w)$.

For the proof of 2) we will require

Lemma 3.58

Let $m : G \times G \longrightarrow G$ be the product map. Then under the identification of $T_{(e,e)}(G\times G)$ with $T_eG \times T_eG$ we have:

$$D_{(e,e)} m (v,w) = v+w .$$

Proof

Since $D_{(e,e)} m : T_eG \times T_eG \longrightarrow T_eG$ is a linear map. we have.

$$D_{(e,e)} m(v,w) = D_{(e,e)} m(v,0) + D_{(e,e)} m(0,w).$$

Consider now
$$\begin{array}{ccccc} G & \xrightarrow{i_1} & G\times G & \xrightarrow{m} & G \\ g & \longmapsto & (g,e) & \longmapsto & g\cdot e. \end{array}$$

Then $m \circ i_1 = id_G$ and hence

$$D_{(e,e)} m \underbrace{D_e i_1 (v)}_{(v,0).} = v \quad \forall v \in T_eG$$

$\square$

Proof of Corollary 3.57

1) By definition

$$\exp_G(t\cdot v) = \varphi_{(t\cdot v)}(1).$$

Consider now $\psi(s) := \varphi_v(ts)$.
Then ψ is a one parameter group with
$\dot\psi(0) = t\,\dot\varphi_v(0) = tv$ and hence by
Corollary 3.54 $\psi = \varphi_{tv}$ which
implies $\varphi_v(ts) = \varphi_{(tv)}(s)$ $\forall s$
and hence $\varphi_{tv}(1) = \varphi_v(t)$, that is
$\exp_G(tv) = \varphi_v(t)$.

2). If $[v,w] = 0$ then by Proposition 3.51

$$\Phi_t^{v^L} \circ \Phi_s^{w^L} = \Phi_s^{w^L} \circ \Phi_t^{v^L} \quad \forall\, t,s.$$

and hence by Proposition 3.52 3).

$$\varphi_w(t)\,\varphi_v(s) = \varphi_v(s)\,\varphi_w(t) \quad \forall t,s$$

This implies that
$$\psi(t) := \varphi_v(t)\,\varphi_w(t) \qquad t \in \mathbb{R}.$$
is a one parameter group in G with
$\dot\psi(0) = D_{(e,e)}m(\dot\varphi_v(0), \dot\varphi_w(0))$

$$= D_{(e,e)} m (v, w)$$
$$= v + w \qquad \leftarrow \text{Lemma 3.58}$$

Hence $\psi(t) = \rho_{v+w}(t)$ which implies $\exp_G(v+w) = \exp_G(v) \exp_G(w)$. $\square$

The characterization of one parameter groups in terms of the exponential leads to the following

Proposition 3.59

Let $\rho : G \longrightarrow H$ be a smooth homomorphism. Then the diagram

$$\begin{tikzcd} G \arrow[r, "\rho"] & H \\ T_eG \arrow[u, "\exp_G"] \arrow[r, "D_e\rho"] & T_eH \arrow[u, "\exp_H"'] \\ \mathfrak{g} \arrow[u, phantom, "\shortparallel"] & \mathfrak{h} \arrow[u, phantom, "\shortparallel"] \end{tikzcd}$$

commutes.

Proof

The map $\psi : \mathbb{R} \longrightarrow H$.
$$t \longmapsto \rho(\exp_G(tv))$$

is a 1-parameter group in H with
$$\dot{\psi}(0) = D_e \phi(v).$$
Hence by Corollary 3.57 1) and Corollary 3.54 we have
$$\psi(t) = \exp_H(t D_e \phi(v))$$
which proves the statement. $\square$

Exercise 3.60

Prove that $\exp_{GL(n,\mathbb{R})}(tA) = \mathrm{Exp}(tA)$

$\forall t \in \mathbb{R},\ A \in gl(n,\mathbb{R}) = M_{n\times n}(\mathbb{R})$

Hint: use Proposition 3.44 3).

— o —

The exponential map gives a preferred chart at e. Namely we have:

Corollary 3.61

Let G be a Lie group with Lie algebra $\mathfrak{g}$. Then the following hold:

1) $D_0 \exp_G = \mathrm{Id}_{\mathfrak{g}}$

2). There is $0 \in U \subset \mathfrak{g}$ open such that $\exp_G(U) \subset G$ is open and

$$\exp_G : U \longrightarrow \exp_G(U)$$

is a diffeomorphism.

Proof

For every $X \in \mathfrak{g}$ $\frac{d}{dt}\Big|_{t=0} \exp_G(tX) = X$

which shows 1). Then 2) follows from the inverse function Theorem $\square$

$\boxed{\text{Theorem 3.62.}}$ [Cartan]

If K is a compact and connected Lie group then $\exp_K : K \longrightarrow K$ is surjective.

It is an Exercise. to show that:

$$\mathrm{Exp} : u(n) \longrightarrow U(n)$$

is surjective.

Hint: combine the fact that every $A \in U(n)$ is diagonalizable with the formula $g\,\mathrm{Exp}(X)\,g^{-1} = \mathrm{Exp}(gXg^{-1})$

valid for all $X \in M_{nn}(\mathbb{C})$, $g \in GL(n,\mathbb{C})$.

A similar argument using Jordan's normal form implies that

$$\mathrm{Exp} : \mathfrak{gl}(n,\mathbb{C}) \longrightarrow GL(n,\mathbb{C})$$

is surjective.

Example 3.63

Let

$$N_1 = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} : * \in \mathbb{R} \right\} \text{ with}$$

Lie algebra

$$\mathfrak{n}_1 = \left\{ \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} : * \in \mathbb{R} \right\}.$$

Since $X^n = 0 \quad \forall X \in \mathfrak{n}_1$ we have

$$\mathrm{Exp}\, X = Id + X + \frac{X^2}{2!} + \cdots + \frac{X^{n-1}}{(n-1)!}.$$

Moreover if $Y \in N_1$ then we can write $Y = Id + Y'$ with Y' such that $(Y')^n = 0$.

Then if we define $\log : N_1 \longrightarrow \mathfrak{n}_1$ by

$$\log(Y) = \log(\mathbb{1} + Y') = \sum_{j=0}^{n-1} (-1)^{j-1} \frac{(Y')^j}{j}$$

it is possible to verify that $\text{Exp}: n_1 \longrightarrow N_1$ and $\log: N_1 \longrightarrow n_1$ are (smooth and) inverse to each other. Hence Exp here is a smooth diffeomorphism, in particular it is surjective.

Example 3.64

We claim that $\text{Exp}: \mathfrak{sl}(n,\mathbb{R}) \longrightarrow SL(n,\mathbb{R})$ is not surjective. Indeed, since

$$\left(\text{Exp}\left(\frac{X}{2}\right)\right)^2 = \text{Exp}(X).$$

every matrix in the image of Exp is a square. On the other hand

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ is not a square.}$$

——— ○ ———

We can use the properties of the exponential map to study the structure of connected abelian Lie groups.

Definition 3.65

A Lie algebra $\mathfrak{g}$ is abelian if $[\,,\,] \equiv 0$.

We have then:

Proposition 3.66

1) Let G be a connected Lie group with Lie algebra $\mathfrak{g}$. Then G is abelian iff $\mathfrak{g}$ is abelian.

2) Let G be a connected abelian Lie group. Then $\exp_G : \mathfrak{g} \longrightarrow G$ is a smooth surjective homomorphism.
Its kernel $\Gamma := \ker \exp_G$ is a discrete subgroup of $\mathfrak{g}$ and $\exp_G$ induces an isomorphism of Lie groups

$$\mathfrak{g}/\Gamma \simeq G.$$

Proof

We are going to prove 1) and 2) at

the same time.

Assume that G is connected and abelian. By Proposition 3.52, for all $v, w \in \mathfrak{g}$ it holds:
$$\Phi_t^{v^L} \circ \Phi_s^{w^L} = \Phi_s^{w^L} \circ \Phi_t^{v^L} \quad \forall t, s$$

Hence Proposition 3.51 implies that
$$[v^L, w^L] = 0$$
that is $[v, w] = 0 \quad \forall v, w \in \mathfrak{g}$.

Assume now that $\mathfrak{g}$ is abelian and G is connected. Corollary 3.57 2) implies that $\exp_G : \mathfrak{g} \to G$ is a smooth homomorphism. By Corollary 3.61 2) $\exp_G(G)$ is an open subgroup of G hence closed. Since G is connected we obtain $\exp_G(G) = G$ and G is abelian.

open in G

Let $U \ni 0$ be open in $\mathfrak{g}$ such that $\exp_G : U \to \exp_G(U)$ is a diffeo given by Corollary 3.61 2) above. Then

$\Gamma \cap U = \{0\}$ and Γ is a discrete group.

Then (Exercise), the induced group isomorphism

$$\mathfrak{g}/\Gamma \longrightarrow G$$

is a diffeomorphism. $\square$

$\boxed{\text{Exercise } 3.67}$

Let V be a finite dimensional vector space and $\Gamma < V$ a discrete subgroup. Show that there are $\gamma_1, \dots, \gamma_r \in \Gamma$ linearly independent in V such that

$$\Gamma = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_r.$$

$\boxed{\text{Exercise } 3.68}$

Show that every connected abelian Lie group G is isomorphic as a Lie group to

$$T^a \times \mathbb{R}^{n-a}$$

where $n = \dim G$ on $T = \mathbb{R}/\mathbb{Z}$.

We end this section about the exponential map with an application related to Hilbert's fifth problem, that was discussed during the first lecture.

In the works of Gleason, Montgomery–Zippin, and Yamabe, when the problem was solved, and even earlier with the work of Von Neumann, it was understood that a key notion for understanding the distinction between topological and Lie groups was that of a small subgroup.

Definition 3.69 [Small subgroup]

A topological group G is said to have small subgroups if every neighborhood of the identity contains a non-trivial subgroup.

Theorem 3.70

A connected locally compact topological group admits a Lie group structure if and only if it has no small subgroups.

Proof

We will only prove the implication
Lie group $\Longrightarrow$ No small subgroups.

The proof of the converse implication goes beyond the scope of the course.

Let $0 \in U \subset \mathfrak{g}$ be an open neighborhood in the Lie algebra of the Lie group G such that $\exp_G : U \longrightarrow \exp_G(U)$ is a diffeomorphism with its image, which is open in G, see Corollary 3.6.1 2). Let $W := \exp \frac{1}{2} U$. Note that W is an open neigh of $e \in G$. We claim that W contains no non-trivial subgroups. $H < G$.

Suppose that $\{e\} \neq H < G$, $H \subset W$. Let $e \neq h \in H$ and $X \in \frac{1}{2} U$ such that $\exp_G X = h$.

Note that we could assume U to be bounded in the very first place.

We will show that there are powers of h not in H, this will contradict the fact that H is a subgroup.

Let $n \in \mathbb{N}$ be such that $2^n X \in \frac{1}{2}U$ and $2^{n+1} X \notin \frac{1}{2}U$. Note that since $2^n X \in \frac{1}{2}U$ clearly $2^{n+1} X \in U$.

Then

$$h^{2^{n+1}} = \exp(2^{n+1}X) \in \exp(U \setminus \tfrac{1}{2}U)$$

However $\exp(U \setminus \frac{1}{2}U) \subseteq \exp_G(U) \setminus W$

Hence $h^{2^{n+1}} \notin W$, a contradiction since we assumed that $H \subset W$ $\square$