Notes 4: The exponential map.

Version 0.00 — with misprints,

Recap of vector fields.

Recall that a smooth vector field, or just a vector field for short, on G is a section of the tangent bundle; in other words, it is a smooth map $v: G \to TG$ such that $v\pi = \mathrm{id}_G$. The map v picks out a tangent vector $v(x) \in T_xG$ for each $x \in G$, and it does this in smooth way.

There are two ways of thinking about vector fields, depending on your tendencies. Geometers would may be think about G as being a submanifold of some euclidian space \mathbb{R}^N (of really huge dimension) and the tangent vectors would then be real, old fashioned vectors being tangent to G. If you are more analytically in your thoughts (or more bourbakistic perhaps) you would think about a vector field as a global derivation: A map $D: C^{\infty}(G) \to C^{\infty}G$, satisfying D(fg) = fD(g) + gD(f). This last point of view is more in conformity with the now universal way of defining the tangent vector to a manifold, as a point derivation.

The correspondence between the two views is of course the formula

$$D_v(f) = \nabla f \cdot v.$$

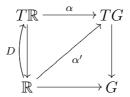
for the directional derivative $D_v(f)$.

Locally, in a chart U with coordinates x_1, \ldots, x_n a vector field is represented as a linear combination $\sum a_i \partial/\partial x_i$ where the a_i -s are smooth functions on U. So for example on the real numbers \mathbb{R} , we have the global vector field $D_t = d/dt$, that is, D_t is a global generator for the tangent bundle $T_{\mathbb{R}}$. Any other field may be written as $f(t)D_t$ where $f \in C^{\infty}(\mathbb{R})$. To simplify the notation, we will some times dismiss the variable t, and only write D.

If $\alpha : \mathbb{R} \to G$ is a smooth map, we denote by α' the vector field $d\alpha(D)$ and $\alpha'(t)$ will be shorthand for $d_t\alpha(D)(\alpha(t))^{-1}$. Strictly speaking, this is not a vector field on G, it is only defined for points in the image $\alpha(\mathbb{R})$. In terms of commutative diagrams

¹The shorthand notation is really indicated here. It is a good training for your ability to dechiffer formalities to convince yourself that the formula $d_t\alpha(D)(\alpha(t))$ means what it is supposed to mean.

it fits into the following one:



For those not accustomed to the compact notaion of global differential geometry, let us use a few words to see what the expression $d_t\alpha(D)(\alpha(t))$ means in local coordinates, so let U be a chart in G with coordinates x_1, \ldots, x_n as above.

Recall that if f is a function defined in U, then $d_t\alpha(D)$ is the derivation sending f to $D(f \circ \alpha) = df(\alpha(t))/dt$. If $\alpha_i = x_i \circ \alpha$ denote the components of α , the chain rule tells us that $df(\alpha(t))/dt = \sum_i \partial f/\partial x_i \alpha_i'(t)$. This means that the field $d_t\alpha(D)$ is expressed as $\sum_i \alpha_i'(t)\partial/\partial x_i$ in the local basis $\partial/\partial x_1, \ldots, \partial/\partial x_n$ for the tangent bundle. If the tangent spaces are identified with \mathbb{R}^n via that basis, we retrieve the good old derivative $\alpha'(t) = (a_1'(t), \ldots, a_n'(t))$.

Integral curves

Let now v be a vector field on G. We say that a smooth map $\alpha \colon I \to G$, where $I \subseteq \mathbb{R}$ is an open interval, is an *integral curve* for v if $\alpha'(t) = v(\alpha(t))$ for all $t \in I$. If $x\mathbb{G}$ is a point, we may ask that the integral curve pass through x, and that this occure as the parameter takes a given value $t_0 \in I$. These conditions constitute the initial value problem

$$\alpha'(t) = v(\alpha(t)) \text{ and } \alpha(t_0) = x,$$
 (\diamondsuit)

which should be satisfied for $t \in I$.

From analysis we know that given any smooth vector field v on a manifold X and a point $x \in X$, then v has a unique maximal, integral curve to x passing through x. Having an integral curve meaning that there is an interval I containing 0 and a function $\alpha \colon I \to X$ satisfying $\alpha'(t) = v(a(t))$ and $\alpha(0) = x$, and the curve being maxial means that if $I \subseteq J$ is a strictly larger interval than I, then no such curve exists.

It also holds true, that in the case the field v depends smoothly on some parameters, the integral curves α likewise depend smoothly on those parameters. If U is the parameter space, there is a smooth map $I \times U \to X$ say $\alpha(t, u)$, such that $\alpha'(t, u) = V(\alpha(t), u)$.

Left invariant vector fields

A vector field v on the Lie group G is called *left invariant* if it for all x and y in g satisfies the following:

$$v(xy) = d_v \lambda_x v(y) \tag{*}$$

that is, if you move along G following a translation, the vector field is also translated. One easily verifies that a linear combination of two left invariant vector fields is left invariant, so that the left invariant vector fields constitute a real vector space.

EXAMPLE — $Gl(n, \mathbb{R})$. Putting y = e in the formula \star , we see that

$$v(x) = d_e \lambda_x v(e) \tag{*}$$

so v is uniquely determined by its value at e. On the other hand, if $v \in T_eG$ is given, * with v(e) = v defines a vector field on G, which is both left invariant and smooth. To verify the left invariance, use that $\lambda_{xy} = \lambda_x \lambda_y$ and the chain rule:

$$v(xy) = d_e \lambda_{xy} v(e) = d_e \lambda_x \circ d_e \lambda_y v(e) = d_e \lambda_x v(y)$$

Smoothness follows from the diagram below where all maps are smooth,

$$G \times T_{e}G \xrightarrow{\operatorname{id}_{G} \times \eta} G \times TG \xrightarrow{\iota} TG \times TG \xrightarrow{d\mu} TG$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow$$

$$G \times \{e\} \xrightarrow{G} G \times G \xrightarrow{\mu} G$$

and where η is the inclusion of T_eG in TG, and $\iota(g,v)=(0,v)$. The map $(g,v)\mapsto d_e\lambda_g v$ is just the composition of the maps in the upper row, and as all maps in that row are smooth, it is smooth, both as a function of g and v.

We have proven the following:

Proposition 1 The definition

$$D_v(x) = d_e \lambda_x v$$

sets up a one to one correspondenc between left invariant vector fields D_v on G and tangent vectors v in T_eG , and it depends on v in a smooth way.

EXAMPLE — $Gl(n, \mathbb{R})$. In this case the derivative $d_x \lambda_a$ is just multiplication by the matrix a. So the invariant field D_v is no more mystrious than $D_v(a) = av$.

One parameter groups

We let G be a Lie group and nose-dive directly into the definition:

Defenition 1 A one-parameter group in G is a Lie group homomorphism $\alpha \colon \mathbb{R} \to G$; that is a smooth map with $\alpha(s+t) = \alpha(s)\alpha(t)$ and $\alpha(0) = 1$.

The set of one parameter groups in G will be denoted by $\operatorname{Hom}(\mathbb{R}, G)$. It is functorial in G; if $\alpha \in \operatorname{Hom}(\mathbb{R}, G)$ and $\phi \colon G \to H$ is a Lie group homomorphism, then clearly $f \circ \alpha \in \operatorname{Hom}(\mathbb{R}, H)$. Thus there is a functor

$$\operatorname{Hom}(\mathbb{R},*)$$
: Liegrps \to Sets.

EXAMPLE — \mathbb{S}^1 . A one parameter group in \mathbb{S}^1 is a Lie group homorphism $\alpha \colon \mathbb{R} \to \mathbb{S}^1$. It lifts uniquely to a homorphism $\widetilde{\alpha} \colon \mathbb{R} \to \mathbb{R}$, *i.e.*, $\alpha(t) = e^{2\pi i \widetilde{\alpha}(t)}$. Any Lie group homorphism $\mathbb{R} \to \mathbb{R}$ is given by its value at 1, hence if $\widetilde{\alpha}(1) = a$, then $\alpha(t) = e^{2\pi i at}$. Sending a to α gives a surjective map from \mathbb{R} to $\operatorname{Hom}(\mathbb{R},\mathbb{S}^1)$, and the condition that a and a' give the same one parameter group is that their difference be an integer. We have seen:

$$\operatorname{Hom}(\mathbb{R}, \mathbb{S}^1) \simeq \mathbb{S}^1$$
.

The aim of this pharagraph is to prove that the one parameter groups in G are precisely the integral curves passing through e of left invariant vector fields.

Lemma 1 If v is a left invariant vectorfield on G and $\alpha(t)$ is a integral curve for v, then a(t+s) = a(s)a(t) whenever $\alpha(s)$, $\alpha(t)$ and $\alpha(s+t)$ all three are defined.

PROOF: We let β be the curve $\beta(t) = a(t+s)$ and $\gamma(t)$ the curve $\gamma(t) = \alpha(s)\alpha(t)$, where s is fixed and t is the running parameter. We are going to show that both these curves are integral curves for the vector field v, *i.e.*, they satisfy the differential equation

$$\eta'(t) = v(\eta(t)),$$

and, as obviously $\beta(0) = \gamma(0) = \alpha(s)$, it follows by the uniqueness of the integral curve through a point, that $\alpha(t+s) = \alpha(s)\alpha(t)$.

If for a moment λ_s is translation by s in \mathbb{R} , them $\beta = \alpha \circ \lambda_s$, and since $d_t \lambda_s = 1$ everywhere ((t+s)'=1), it follows from the cahin rule that $\beta'(t) = \alpha'(t+s) = v(\alpha(t+s))$.

On the other hand, computing the derivative $\gamma'(t)$ we get

$$\gamma'(t) = d_0(\lambda_{\alpha(s)}\alpha(t)) = d_{\alpha(t)}\lambda_{\alpha(s)}\alpha'(t) = d_{\alpha(t)}\lambda_{\alpha(s)}v(\alpha(t)) = v(\alpha(s)\alpha(t)) = v(\gamma(t)).$$

Lemma 2 If v is a left invariant vector field on G, then the integral curve $\alpha(t)$ passing through e, is defined for all $t \in \mathbb{R}$

PROOF: Let $I \subseteq \mathbb{R}$ be a maximal interval over which α is defined. Let $t \in I$. Then on t+I we may define $\alpha(t+s) = \alpha(t)\alpha(s)$, and by lemma 1 this agrees with the original definition of α on the intersection $I \cap t + I$, Hence $t+I \subseteq I$ for all $t \in I$ such that $I \cap t + I \neq \emptyset$. This clearly implies that $I = \mathbb{R}$.

The two lemmas put together prove:

Theorem 1 There is a one-to-one correspondence between one-parameter groups $\mathbb{R} \to G$ and left invariant vector fields on G given by associating to α the left invariant vector field $D_{\alpha'(0)}$ with value $\alpha'(0)$ in T_eG .

Let $\phi \colon G \to H$ be a map of Lie groups and $\alpha \colon \mathbb{R} \to G$ a one parameter group. If $\beta = f \circ \alpha$ is the induced one parameter group in H, the chain rule gives

$$\beta'(0) = d_0\beta(D_t) = d_0(f \circ \alpha)(D_t) = d_ef(d_0D_t) = d_ef(a'(0)).$$

Theorem 2 The correspondence $\operatorname{Hom}(\mathbb{R}, G) \simeq T_e G$ above, given as $\alpha \mapsto \alpha'(0)$, is functorial. That is if $\phi \colon G \to H$ is a Lie group map and $\beta(t) = \phi(\alpha(t))$, then $\beta'(0) = d_e \phi(\alpha'(0))$.

The exponential map

Let G be a Lie group. If $v \in T_eG$, then we have seen that there is a one parameter group α_v corresponding to the left invariant vector field D_v , that is the one with $D_v(g) = d_e \lambda_g v$. We now perform a change of notation, and from now on we denote the one parameter group associated to the left invariant vector field D_v by $\exp tv$. This notation is clearly inspired by the traditional exponential function, but the connection is of course much deeper than pure notational.

EXAMPLE— $\operatorname{Gl}(n,\mathbb{R})$. In the case of $\operatorname{Gl}(n,\mathbb{R})$, the derivative of the translation map λ_a is just multiplication by the matrix a, and this is the key to understanding several of the statements about the exponential map in a setting of a general Lie group and how they are related to the cooresponding statements in the setting of matrix groups.

Pick an $a \in T_I \operatorname{Gl}(n, \mathbb{R}) = \operatorname{M}_n(\mathbb{R})$. The initial value problem \diamond defining $\exp ta$ becomes:

$$\alpha'(t) = d_I \lambda_{\alpha(t)} a = \alpha(t) \cdot a \text{ and } \alpha(0) = I_n,$$

and this initial value problem is solved by the good old power series

$$\exp at = \sum_{n=0}^{\infty} \frac{a^n t^n}{n!}.$$

The series is absolute and uniformely convergent, and in fact, has a meaning in any Banach algebra 2 . One can compute the derivative term by term, which gives

$$(\exp at)' = \sum_{n=1}^{\infty} \frac{a^n t^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} \frac{a^n t^n}{n!} a = (\exp at)a,$$

and naturally $\exp 0 = I$.

EXAMPLE— $\operatorname{Sl}(n, \mathbb{R})$. Consider the map $\exp M_n(\mathbb{R}) \to \operatorname{Gl}(n, \mathbb{R})$ sending a matrix a to $\exp a$. Clearly

$$\exp(\epsilon x) = I_n + \epsilon x + O(\epsilon^2)$$

hence the derivative of exp at zero is the identity $T_0 \,\mathrm{M_n}(\mathbb{R}) = \mathrm{M_n}(\mathbb{R}) \to T_e \,\mathrm{Gl}(n,\,\mathbb{R}) = \mathrm{M_n}(\mathbb{R})$. We have seen that the derivative of the determinant is the trace; hence the derivative of the map $a \mapsto \det \exp a$ is equal to $\operatorname{tr} a$, and it follows that $\det \exp a = e^{\operatorname{tr} a}$, hence the exponential carries $\operatorname{so}(n,\,\mathbb{R})$ into $\operatorname{Sl}(n,\,\mathbb{R})$.

EXAMPLE— $a^2 = I$. It might be instructive to compute one explicit example. Assume that a is an $n \times n$ -matrix with $a^2 = I_n$. Then

$$\exp ta = \sum_{m=0}^{\infty} \frac{t^{2m} a^{2m}}{(2m)!} + a \sum_{m=1}^{\infty} \frac{t^{2m+1} a^{2m}}{(2m+1)!} = (\cosh t)I_n + (\sinh t)a,$$

so for example if

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

then

$$\exp a = \begin{pmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{pmatrix}.$$

² You need a multiplicative norm that is a norm that in addition to the triangle inequality satisfies $||x|| y \le ||x|| ||y||$, and you need completeness to be sure an absolutely convergent series is convergent.

*

The exponential map is a smooth one parameter group, that is a map

$$\exp tv \colon \mathbb{R} \to G$$

depending smoothly on t. But it depends also smoothly on v. This follows from the observation in proposition 1 that the left invariant vector field $d_e \lambda_g v$ depends smoothly on v, and the result from analysis about initial value problems with parameters saying that the solution depends smoothly on the parameters (if all input data do).

Hence we may recollect the functions $\exp tv$ for different v's into one, smooth function

$$E(t, v) = \exp \colon \mathbb{R} \times T_e G \to G.$$

Defenition 2 Let G be a Lie group. The exponential map is the map exp: $T_eG \to G$ defined by exp v = E(1, v).

Proposition 2 The derivative of exp: $T_eG \to G$ at the origin in T_eG is the identity. Hence exp is a local diffeomorphism near the origin.

PROOF: We are to examine expressions like $E(1, \epsilon v) - E(1, 0) = \exp(\epsilon v) - e$ for ϵ small in a coordinate neighbourhood of e (where they have a meaning). By definition of the derivative, we have

$$\exp(\epsilon v) = e + \epsilon d_t \exp(\epsilon v) = e + \epsilon d_e \lambda_{\exp(\epsilon v)} v$$

hence $\exp(\epsilon v) - e/\epsilon = d_e \lambda_{\exp(\epsilon v)} v$ and letting ϵ tend to zero, we find $d_e \lambda_e v = v$.

As $\exp tv$ by definition is a one parameter group, it satisfying

Proposition 3

$$\exp(s+t)v = \exp sv \cdot \exp tv \text{ for all } s,t \in \mathbb{R} \text{ and }$$

and

$$d_0 \exp tv = v$$
.

These two propertie characterise $\exp tv$.

Furthermore, the map $\exp tv$ is functorial in the following sense

Proposition 4 If $\phi: G \to H$ is a Lie group map, then

$$\exp(td_e\phi(v)) = \phi(\exp tv).$$

PROOF: This follows immediatly from the corresponding property of one parameter groups, theorem 2.

Putting t = 1, we get

Proposition 5 The exponential map is functorial, that is, if $\phi: G \to H$ is a Lie group map, then

$$\exp(d\phi_e v) = \phi \exp(v),$$

For diagrammatics the statement about the functoriality may be expressed by the following commutative diagram:

$$T_e G \xrightarrow{\exp} G$$

$$\downarrow^{d_e \phi} \qquad \downarrow^{\phi}$$

$$T_e H \xrightarrow{\exp} H.$$

When applied to different homomorphisms, this functoriality gives several important formula. We shall give to examples. In the first one, the homorphism is the the adjoint representation $Ad_*: G \to \operatorname{Aut}(T_eG)$, whose derivative is $ad_*: \operatorname{Hom}(T_eG, T_eG) \to \operatorname{Aut}(T_eG)$. The functoriality of exp then gives the commutative diagram

$$\begin{array}{c|c} T_eG & \xrightarrow{\exp} & G \\ & \downarrow^{ad_*} & & \downarrow^{Ad_*} \\ & & \downarrow^{Ad_*} & & \\ \operatorname{Hom}(T_eG, T_eG) & \xrightarrow{\exp} & \operatorname{Aut}(T_eG). \end{array}$$

where we use that $T_{id} \operatorname{Aut}(T_e G) = \operatorname{Hom}(T_e G, T_e G)$. Or formulated as a formula:

Proposition 6 For any Lie group, it holds true that

$$Ad_* \circ \exp = \exp \circ ad_*$$
.

This formula deserves a few remarks. First of all, the bottom map is the classical exponential function, as described in the example above, applied to the endomorphisms ad_x of T_eG , which we recall is given as $ad_v \cdot w = [v, w]$, so

$$\exp(ad_v) = \sum_{n=1}^{\infty} \frac{a_v^n}{n!}$$

where ad_v^n is the *n*-fold composition $ad_v^n = ad_v \circ ad_v \circ \cdots \circ ad_v$, or if you want, $ad_v^n w = [v, [v, [v, \dots, [v, w], \dots]]]$ where there are *n* nested brackets. So for example, if [v, w] = 0, then $ad_v^n \cdot w = 0$ for n > 0, and hence $\exp(ad_v \cdot w) = w$.

The homorphism in our second example, the homorphism is the conjugation map $c_x \colon G \to G$, whose derivative at unity is the adjoint representation Ad_x evaluated at x. Hence the commutative diagram

$$T_eG \xrightarrow{\exp} G$$
 $Ad_v \downarrow \qquad \qquad \downarrow c_x$
 $T_eG \xrightarrow{\exp} G.$

Or as a formula

Proposition 7 For any Lie group G and any elements $x \in G$ and $v \in T_eG$

$$x \exp v = \exp A d_x v$$
.

As an application of these two formulas we show the following:

Proposition 8 Let G be a Lie group and let v and w be two tangent vectors at unity. If [v, w] = 0, then $\exp v$ and $\exp w$ commute. Furthermore $\exp(v + w) = \exp(v) \exp(w)$.

PROOF: By proposition 7 we have

$$x \cdot \exp w \cdot x^{-1} = \exp Ad_x \cdot w,$$

where $x = \exp v$. Now by proposition 6

$$Ad_{\exp v} \cdot w = \exp ad_v \cdot w = w$$

where the last equality holds because [v, w] = 0 as explained in the remark after proposition 6, hence combining the two equations, we see that

$$\exp v \cdot \exp w \cdot \exp v^{-1} = \exp w,$$

so $\exp v$ and $\exp w$ commute. To prove the last part of the statement, regard the function $\alpha(t) = \exp tv \cdot \exp tw$. This is a one parameter group, since

$$\alpha(s+t) = \exp(s+t)v \cdot \exp(s+t)w$$

$$= \exp sv \cdot \exp tv \cdot \exp sw \cdot \exp tw$$

$$= \exp sv \cdot \exp sw \cdot \exp tv \cdot \exp tw = \alpha(s)\alpha(t)$$

where we have used that $\exp tv$ and $\exp sw$ commute since [tv, sw] = 0. Now, what is the derivative in 0 of this one parameter subgroup? To answere that, we use a version of the product rule, as in lemma 3 below:

$$d_0 \exp tv \cdot \exp tw = d_0 \exp tv + d_0 \exp tw = v + w,$$

Hence $\alpha(t)$ is the one parameter group whose derivative at 0 equals v+w, that is $\exp t(v+w)$, and we are done.

An obvious corollary is

Corollary 1 Let G be an abelian Lie group. Then the exponential map is a group homomorphism.

PROOF: By corollary 1 Lie G is abelian, and the statement follows from proposition 8.

Lemma 3 Let α and β be smooth maps from \mathbb{R} to G with $\alpha(0) = \beta(0) = e$. If $\gamma(t) = \alpha(t) \cdot \beta(t)$ then

$$d_0 \gamma = d_0 \alpha + d_0 \beta$$
.

PROOF: This follows directly by the chain rule and the fact that $d_{(e,e)}\mu(v,w) = v + w$, where μ is the multiplication map. Indeed, $\gamma(t) = \mu(\alpha(t), \beta(t))$, and thus $\gamma = \mu \circ \eta$ if we let $\eta(t) = (\alpha(t), \beta(t))$.

Then $d_0\gamma$ is the composition

$$T_0 \mathbb{R} \xrightarrow{d_0 \eta} T_e G \oplus T_e G \xrightarrow{d_{(e,e)} \mu} T_e G.$$

$$-10 -$$

Hence $d_0\eta = d_0\alpha + d_0\beta$.

EXAMPLE— THE EXPONENTIAL MAP FOR $Sl(2, \mathbb{R})$ is not surjective. The point of this example is to show that the exponential map is not necessarily a surjective map. This is e.g., the case for the group $Sl(2, \mathbb{R})$, as we shall see here; in fact, the elements in $Sl(2, \mathbb{R})$ with two negative egienvalues are not in the image.

The matrices $x \in sl(2, \mathbb{R})$ satisfy by definition $\operatorname{tr} x = 0$, and therefore by Cayley-Hamilton theorem we have $x^2 = -\det xI$. We shall discuss all the three possibilities for $\det x$; it can be positive, negative or zero:

i) If det x = 0, it follows that $x^2 = 0$. Hence x is conjugate to a matrix on the form

$$\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix},$$

and $\exp x$ is conjugate to

$$\begin{pmatrix} 1 & e^t \\ 0 & 1 \end{pmatrix}.$$

Thus $\exp x$ is unipotent with 1 as the only eigenvalue.

- ii) Assume det x < 0. Then x has two distinct eigenvalues λ and $-\lambda$ with $-\lambda^2 < 0$, That is, the eigenvalue λ is a positive, real number. The exponential $\exp x$ therefore has the eigenvalues $e^{-\lambda}$ and e_{λ} , which both are positive and real.
- iii) Assume finally that $\det x > 0$. Then the eigenvalues λ and $-\lambda$ satisfy $-\lambda^2 > 0$, which means that λ is purely imaginary, *i.e.*, $\lambda = it$ for some $t \in \mathbb{R}$. Hence the eigenvalues of $\exp x$ are e^{it} and e^{-it} .

Not in any of these cases the elements from $Sl(2, \mathbb{R})$ with negative, real eigenvalues appear as $\exp x$, so they are not in the image of the exponential map.

Classification of commutative Lie groups

As the title says the aim of this section id to give the complete list of connected, abelian Lie groups. We know some examples, like the one dimensional ones \mathbb{R} and \mathbb{S}^1 , and of course we can take direct product of copies of those, and in fact, that is all there is:

Theorem 3 If G is a connected, abelian Lie group, then there are uniquely defined non-negative integers n and m, such that

$$G \simeq \mathbb{R}^m \times \mathbb{S}^n$$
.

PROOF: The proof leans on a two salient facts. The first, and also the most fundamental part, is that the exponential map is a Lie group homorphism when G is abelian. Therefore there is an exact sequence of Lie groups

$$1 \longrightarrow \Gamma \longrightarrow T_e G \xrightarrow{\exp} G \longrightarrow 1$$
,

where exp is surjective — which might have been mentioned as the third salient fact — since it is a subgroup containing the open neigbourhood of e where exp is a diffeomorphism, and that neigbourhood generates the whole of G.

We know that the kernel Γ is a discrete subgroup. The second fact we lean on, is that the structure of discrete subgroups of a real vector space T is completely known (and sufficiently simple). There are, as we shall prove in lemma 4 below, elements $\gamma_1, \ldots, \gamma_p$ which are linearly independent as vectors, that generate Γ . Letting T' be the subspace of T generated by the γ_i 's — for which then $\gamma_1, \ldots, \gamma_p$ is a basis — and letting T'' be a complementary subspace, we see that

$$G \simeq T'/\Gamma \times T'' \simeq \mathbb{R}\gamma_1/\mathbb{Z}\gamma_1 \times \mathbb{R}\gamma_2/\mathbb{Z}\gamma_2 \times \ldots \times \mathbb{R}\gamma_p/\mathbb{Z}\gamma_p \times T''$$

and each of the quotients $\mathbb{R}\gamma_i/\mathbb{Z}\gamma_i$ is a circle \mathbb{S}^1 .

Lemma 4 Let T be a finite diemsional real vector space, and let $\Gamma \subseteq T$ be a discrete subgroup of T. Then there are elements $\gamma_1, \ldots, \gamma_p$ in γ , linearly independent as vectors, that generate Γ .

PROOF: Recall that Γ is discrete of T if any point γ possesses an open neigbourhood U_{γ} in T with $\Gamma \cap U_{\gamma} = \{\gamma\}$. By a translation argument, this is equivalent to this being the case for one point, say 0. Another usefull characterisation is that if $\{\eta_i\}$ is a sequence of elements in Γ that converges, then it is eventually constant, *i.e.*, $\eta_i = \eta_{i+1}$ for i >> 0.

The proof will be by induction on the dimension. We first treat the case that V is one dimensional, that is $V = \mathbb{R}$. We let $\gamma \in \Gamma$ be the smallest positive element, which exists since any descending sequence of positive element from Γ must converge, and therefore is eventually constant. Let $b \in \Gamma$ be another positive element. Then $b/\gamma > 1$ and the integer value $[b/\gamma]$ satisfies $[b/\gamma] \ge 1$, hence $0 \le b - n\gamma < \gamma$, and γ being the smallest positive element in γ , it follows that $b = n\gamma$.

Assume dim T > 1 and pick $\gamma \in \Gamma$. By the dimension one case, $\Gamma \cap \mathbb{R}\gamma$ has a generator, which we after a change of names, can assume is γ . Let T' be the quotient

 $T/\mathbb{R}\gamma$ and let π be the projection. We claim that $\pi\Gamma$ is a discrete subgroup of $T/\mathbb{R}\gamma$. Assume there is sequence $\pi(\eta_i)$ in $\Gamma/\mathbb{Z}\gamma$ that converges to zero.

If we could choose $\{\eta_i\}$ to be a bounded sequence, we would be in safety, since then $\{\eta_i\}$ has convergent subsequence which is eventually constant, Γ being discret, and therefore $\pi(\eta_i)$ is eventually constant.

The problem is that η_i might escape to infinity, but, luckily, we are allowed to change each η_i by a multiple $n\gamma$ without $\pi\eta_i$ changing, and thus are able to replace the sequence $\{\eta_i\}$ by one which is bounded.

To this end, write each η_i as $\eta_i = x_i + y_i$ where $x_i \in \mathbb{R}\gamma$ and y_i is orthogonal to $\mathbb{R}\gamma$. We may find integers n_i such that $||x_i - n_i\gamma|| < ||\gamma||$, then by replacing $\{\eta_i\}$ with $\{\eta_i - n_i\gamma\}$, we may assume that $||x_i|| < ||\gamma||$ for all i.

Now if U is any open, bounded set with $U \cap \mathbb{R}\gamma$ containing the "intervall" $\{t\gamma \mid t \in [-1,1]\}$, then πU is open and hence contains all but finitely many members from the sequence $\{\pi(\eta_i)\}$. Consequently the bounded set U contains all but finitely many of the η_i , and we are through.

So by induction $\Gamma/\mathbb{Z}\gamma\subseteq T/\mathbb{R}\gamma$ has a generator set $\gamma_1,\ldots,\gamma_{p-1}$ of linearly independent vectors, and any lifting of these will together with γ form a linearly independent generator set for Γ .

Recall that a Lie group isomorphic to a product $\mathbb{S}^n = \mathbb{S}^1 \times \mathbb{S}^1 \times \ldots \times \mathbb{S}^1$ of circles is called a *torus*. Tori play a fundamental role in the representation theory of compact groups. One reason is the following:

Corollary 2 Any compact, connected group G is a torus.

Proposition 9 Any compact, abelian lie group is isomorphic to a product $T \times A$ where T is a torus and A is a finite group.

PROOF: Let $A = \pi_0 G$. Then there is an exact sequence

$$0 \longrightarrow G_0 \longrightarrow G \longrightarrow A \longrightarrow 0.$$

The identity component G_0 is abelian, compact and connected, hence isomorphic to a torus after the theorem. The quotient $A = G/G_0$ is discrete and compact, hence finite. We claim that the sequence splits, that is, there is a subgroup $A' \subseteq G$ projecting isomorphically onto A. As G is abelian, the action of A' on G_0 by conjugation is trivial, and G is the direct product $G_0 \times A'$.

To get hold of A', the main feature is the following: Let $a \in A$ be a generator for one of the cyclic components of A of order e say. Lift a to some x in G. Then

 $x^e \in G_0$, and since G_0 is divisible, $x^e = y^e$ with $y \in G_0$, but then $(xy^{-1})^e = 1$ (G being abelien) and xy^{-1} maps to a.

Now write $A = \bigoplus_{i=1}^p \mathbb{Z}/e_i\mathbb{Z}$, and repeat the procedure we just described, for the generators of each of the factors $\mathbb{Z}/e_i\mathbb{Z}$. Their lifts generate the group A'.