



Course 424  
Group Representations III

Dr Timothy Murphy

EELT 3      Tuesday, 11 May 1999      14:00–16:00

*Answer as many questions as you can; all carry the same number of marks.*

*In this exam, ‘Lie algebra’ means Lie algebra over  $\mathbb{R}$ , and ‘representation’ means finite-dimensional representation over  $\mathbb{C}$ .*

1. Define the *exponential*  $e^X$  of a square matrix  $X$ .

Determine  $e^X$  in each of the following cases:

$$\begin{aligned} X &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, & X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & X &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ X &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & X &= \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, & X &= \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

Which of these 6 matrices  $X$  are themselves expressible in the form  $X = e^Y$ , where  $Y$  is a real matrix? (Justify your answers in all cases.)

**Answer:** *The exponential of a square matrix  $X$  is defined by*

$$e^X = I + X + \frac{1}{2!}X^2 + \frac{1}{3!}X^3 + \dots .$$

*This series converges for all  $X \in \mathbf{Mat}(n, k)$  by comparison with the series for  $e^{\|X\|}$ , since  $\|X^n\| \leq \|X\|^n$ .*

(a) If

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

then

$$X^2 = 0$$

and so

$$e^X = I + X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(b) If

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

then

$$X^2 = I,$$

and so

$$e^X = \begin{pmatrix} \cosh 1 & \sinh 1 \\ \sinh 1 & \cosh 1 \end{pmatrix}$$

(c) If

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

then

$$X^2 = -I,$$

and so

$$e^X = \begin{pmatrix} \cos 1 & -\sin 1 \\ \sin 1 & \cos 1 \end{pmatrix}.$$

(d) If

$$X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

then

$$e^X = \begin{pmatrix} e & 0 \\ 0 & e^{-1} \end{pmatrix}.$$

(e) If

$$X = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = I + Y,$$

where

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

then, since  $I, Y$  commute,

$$e^X = e^I e^Y = \begin{pmatrix} e \cos 1 & -e \sin 1 \\ e \sin 1 & e \cos 1 \end{pmatrix}.$$

(f) If

$$X = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = -I + Z,$$

where

$$Z = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

then, since  $-I, Z$  commute,

$$e^X = e^{-I} e^Z = \begin{pmatrix} e^{-1} & -e^{-1} \\ 0 & e^{-1} \end{pmatrix}.$$

- (a)  $e^Y$  is non-singular for all  $Y$ , since  $e^Y e^{-Y} = I$ . Since  $X$  is singular in this case,  $X \neq e^Y$ .
- (b)  $X$  has eigenvalues  $\pm 1$ . Suppose  $X = e^Y$ ; and suppose  $Y$  has eigenvalues  $\lambda, \mu$ . Then  $X$  has eigenvalues  $e^\lambda, e^\mu$ . There are two possibilities. Either  $\lambda, \mu$  are complex conjugates, in which case the same is true of  $e^\lambda, e^\mu$ ; or else  $\lambda, \mu$  are both real, in which case  $e^\lambda, e^\mu > 0$ . In neither case can we get  $\pm 1$ . Hence  $X \neq e^Y$ .
- (c) By the isomorphism between the complex numbers  $z = x + iy$  and the matrices

$$\mathbb{C}(z) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

we see that

$$X = \mathbb{C}(i).$$

Since

$$i = e^{\pi i/2},$$

while

$$\mathbb{C}(e^z) = e^{\mathbb{C}(z)},$$

it follows that  $X = e^Y$  with

$$Y = \begin{pmatrix} 0 & -\pi/2 \\ \pi/2 & 0 \end{pmatrix}.$$

- (d)  $X$  has eigenvalues  $\pm 1$ . Thus by the argument in case (b) above,  $X \neq e^Y$ .

(e) We have

$$X = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \mathbb{C}(1 + i).$$

But

$$1 + i = \sqrt{2}e^{\pi i/4} = e^{\log 2/2 + \pi i/4}.$$

Thus  $X = e^Y$  with

$$Y = X = \begin{pmatrix} \log 2/2 & -\pi/4 \\ \pi/4 & \log 2/2 \end{pmatrix}.$$

(f)  $X$  has eigenvalues  $-1, -1$ . Thus if  $X = e^Y$  (with  $Y$  real) then  $Y$  must have eigenvalues  $\pm(2n + 1)\pi i$  for some integer  $n$ . In particular,  $Y$  has distinct eigenvalues, and so is semisimple (diagonalisable over  $\mathbb{C}$ ).

But in that case  $X = e^Y$  would also be semisimple. That is impossible, since a diagonalisable matrix with eigenvalues  $-1, -1$  is necessarily  $-I$ . Hence  $X \neq e^Y$ .

2. Define a linear group, and a Lie algebra; and define the Lie algebra  $\mathcal{L}G$  of a linear group  $G$ , showing that it is indeed a Lie algebra.

Define the dimension of a linear group; and determine the dimensions of each of the following groups:

$\mathbf{O}(n), \mathbf{SO}(n), \mathbf{U}(n), \mathbf{SU}(n), \mathbf{GL}(n, \mathbb{R}), \mathbf{SL}(n, \mathbb{R}), \mathbf{GL}(n, \mathbb{C}), \mathbf{SL}(n, \mathbb{C})$ ?

**Answer:** A linear group is a closed subgroup  $G \subset \mathbf{GL}(n, \mathbb{R})$  for some  $n$ .

A Lie algebra is defined by giving

- (a) a vector space  $L$ ;
- (b) a binary operation on  $L$ , ie a map

$$L \times L \rightarrow L : (X, Y) \mapsto [X, Y]$$

satisfying the conditions

- (a) The product  $[X, Y]$  is bilinear in  $X, Y$ ;
- (b) The product is skew-symmetric:

$$[Y, X] = -[X, Y];$$

(c) Jacobi's identity is satisfied:

$$[[X, Y], Z] + [[Y, Z], X] + [[Z, X], Y] = 0$$

for all  $X, Y, Z \in L$ .

Suppose  $G \subset \mathbf{GL}(n, \mathbb{R})$  is a linear group. Then its Lie algebra  $L = \mathcal{L}G$  is defined to be

$$L = \{X \in \mathbf{Mat}(n, \mathbb{R}) : e^{tX} \in G \forall t \in \mathbb{R}\}.$$

It follows at once from this definition that

$$X \in L, \lambda \in \mathbb{R} \implies \lambda X \in L.$$

Thus to see that  $L$  is a vector subspace of  $\mathbf{Mat}(n, \mathbb{R})$  we must show that

$$X, Y \in L \implies X + Y \in L.$$

Now

$$(e^{X/n} e^{Y/n})^n \mapsto e^{X+Y}$$

as  $n \mapsto \infty$ . (This can be seen by taking the logarithms of each side.) It follows that

$$X, Y \in L \implies e^{X+Y} \in G.$$

On replacing  $X, Y$  by  $tX, tY$  we see that

$$\begin{aligned} X, Y \in L &\implies e^{t(X+Y)} \in G \\ &\implies X + Y \in L. \end{aligned}$$

Similarly

$$(e^{X/n} e^{Y/n} e^{-X/n} e^{-Y/n})^{n^2} \mapsto e^{[X, Y]},$$

as may be seen again on taking logarithms. It follows that

$$X, Y \in L \implies e^{[X, Y]} \in G.$$

Taking  $tX$  in place of  $X$ , this implies that

$$\begin{aligned} X, Y \in L &\implies e^{t[X, Y]} \in G \\ &\implies [X, Y] \in L. \end{aligned}$$

Thus  $L$  is a Lie algebra.

The dimension of a linear group  $G$  is the dimension of the real vector space  $\mathcal{L}G$ :

$$\dim G = \dim_{\mathbb{R}} \mathcal{L}G.$$

(a) We have

$$\mathfrak{o}(n) = \{X \in \mathbf{Mat}(n, \mathbb{R}) : X' + X = 0\}$$

A skew symmetric matrix  $X$  is determined by giving the entries above the diagonal. This determines the entries below the diagonal; while those on the diagonal are 0. Thus

$$\dim O(n) = \dim \mathfrak{o}(n) = \frac{n(n-1)}{2}.$$

(b) We have

$$\mathfrak{so}(n) = \{X \in \mathbf{Mat}(n, \mathbb{R}) : X' + X = 0, \operatorname{tr} X = 0\} = \mathfrak{o}(n),$$

since  $X' + X = 0 \implies \operatorname{tr} X = 0$ . Thus

$$\dim SO(n) = \dim O(n) = \frac{n(n-1)}{2}.$$

(c) We have

$$\mathfrak{u}(n) = \{X \in \mathbf{Mat}(n, \mathbb{C}) : X^* + X = 0\}$$

Again, the elements above the diagonal determine those below the diagonal; while those on the diagonal are purely imaginary. Thus

$$\begin{aligned} \dim \mathbf{U}(n) &= 2 \frac{n(n-1)}{2} + n \\ &= n^2. \end{aligned}$$

(d) We have

$$\mathfrak{su}(n) = \{X \in \mathbf{Mat}(n, \mathbb{C}) : X^* + X = 0, \operatorname{tr} X = 0\}$$

This gives one linear condition on the (purely imaginary) diagonal elements. Thus

$$\dim \mathbf{SU}(n) = \dim \mathbf{U}(n) - 1 = n^2 - 1.$$

(e) We have

$$\mathfrak{gl}(n, \mathbb{R}) = \mathbf{Mat}(n, \mathbb{R}).$$

Thus

$$\dim \mathbf{GL}(n, \mathbb{R}) = n^2.$$

(f) We have

$$\mathfrak{sl}(n, \mathbb{R}) = \{X \in \mathbf{Mat}(n, \mathbb{R}) : \operatorname{tr} X = 0\}.$$

This imposes one linear condition on  $X$ . Thus

$$\dim \mathbf{SL}(n, \mathbb{R}) = \dim \mathbf{GL}(n, \mathbb{R}) - 1 = n^2 - 1.$$

(g) We have

$$\mathfrak{gl}(n, \mathbb{C}) = \mathbf{Mat}(n, \mathbb{C}).$$

Each of the  $n^2$  complex entries takes 2 real values. Thus

$$\dim \mathbf{GL}(n, \mathbb{C}) = 2n^2.$$

(h) We have

$$\mathfrak{sl}(n, \mathbb{C}) = \{X \in \mathbf{Mat}(n, \mathbb{C}) : \operatorname{tr} X = 0\}.$$

This imposes one complex linear condition on  $X$ , or 2 real linear conditions. Thus

$$\dim \mathbf{SL}(n, \mathbb{C}) = \dim \mathbf{GL}(n, \mathbb{C}) - 2 = 2n^2 - 2.$$

3. Determine the Lie algebras of  $\mathbf{SU}(2)$  and  $\mathbf{SO}(3)$ , and show that they are isomorphic.

Show that the 2 groups themselves are *not* isomorphic.

**Answer:** We have

$$\begin{aligned} \mathfrak{u}(2) &= \{X \in \mathbf{Mat}(2, \mathbb{C}) : e^{tX} \in \mathbf{U}(2) \forall t \in \mathbb{R}\} \\ &= \{X : (e^{tX})^* e^{tX} = I \forall t\} \\ &= \{X : e^{tX^*} = e^{-tX} = I \forall t\} \\ &= \{X : X^* = -X\} \\ &= \{X : X^* + X = 0\}. \end{aligned}$$

Also

$$\begin{aligned} \mathfrak{sl}(2, \mathbb{C}) &= \{X \in \mathbf{Mat}(2, \mathbb{C}) : e^{tX} \in \mathbf{SL}(2, \mathbb{C}) \forall t \in \mathbb{R}\} \\ &= \{X : \det e^{tX} = 1 \forall t\} \\ &= \{X : e^{t \operatorname{tr} X} = 1 \forall t\} \\ &= \{X : \operatorname{tr} X = 0\}. \end{aligned}$$

Since

$$\mathbf{SU}(2) = \mathbf{U}(2) \cap \mathbf{SL}(2, \mathbb{C})$$

it follows that

$$\begin{aligned}\mathbf{su}(2) &= \mathbf{u}(2) \cap \mathbf{sl}(2, \mathbb{C}) \\ &= \{X : X^* + X = 0, \operatorname{tr} X = 0\}.\end{aligned}$$

The 3 matrices

$$e = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, f = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, g = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

form a basis for the vector space  $\mathbf{su}(2)$ .

We have

$$\begin{aligned}[e, f] &= ef - fe = -2g, \\ [e, g] &= eg - ge = 2f, \\ [f, g] &= fg - gf = -2e\end{aligned}$$

Thus

$$\mathbf{su}(2) = \langle e, f, g : [e, f] = -2g, [e, g] = 2f, [f, g] = -2e \rangle.$$

We have

$$\begin{aligned}\mathfrak{o}(3) &= \{X \in \mathbf{Mat}(3, \mathbb{R}) : e^{tX} \in \mathbf{O}(3) \forall t \in \mathbb{R}\} \\ &= \{X : (e^{tX})' e^{tX} = I \forall t\} \\ &= \{X : e^{tX'} = e^{-tX} = I \forall t\} \\ &= \{X : X' = -X\} \\ &= \{X : X' + X = 0\}.\end{aligned}$$

Also

$$\begin{aligned}\mathbf{sl}(3, \mathbb{R}) &= \{X \in \mathbf{Mat}(3, \mathbb{R}) : e^{tX} \in \mathbf{SL}(3, \mathbb{R}) \forall t \in \mathbb{R}\} \\ &= \{X : \det e^{tX} = 1 \forall t\} \\ &= \{X : e^{t \operatorname{tr} X} = 1 \forall t\} \\ &= \{X : \operatorname{tr} X = 0\}.\end{aligned}$$

Since

$$\mathbf{SO}(3) = \mathbf{O}(3) \cap \mathbf{SL}(3, \mathbb{R})$$

it follows that

$$\begin{aligned}\mathfrak{so}(3) &= \mathfrak{o}(3) \cap \mathfrak{sl}(3, \mathbb{R}) \\ &= \{X : X' + X = 0, \operatorname{tr} X = 0\} \\ &= \{X : X' + X = 0\}\end{aligned}$$

since a skew-symmetric matrix necessarily has trace 0.

The 3 matrices

$$U = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

form a basis for the vector space  $\mathfrak{so}(3)$ .

We have

$$[V, W] = U;$$

and so by cyclic permutation of indices (or coordinates)

$$[W, U] = V, \quad [U, V] = W.$$

Thus

$$\mathfrak{so}(3) = \langle U, V, W : [U, V] = W, [U, W] = -V, [V, W] = U \rangle.$$

Finally,  $\mathfrak{su}(2)$  and  $\mathfrak{so}(3)$  are isomorphic under the correspondence

$$e \leftrightarrow -2U, \quad f \leftrightarrow -2V, \quad g \leftrightarrow -2W.$$

However, the groups  $\mathbf{SU}(2)$ ,  $\mathbf{SO}(3)$  are not isomorphic, since

$$\mathbf{ZSU}(2) = \{\pm I\} \text{ while } \mathbf{ZSO}(3) = \{I\}.$$

4. Define a *representation* of a Lie algebra; and show how each representation  $\alpha$  of a linear group  $G$  gives rise to a representation  $\mathcal{L}\alpha$  of  $\mathcal{L}G$ .

Determine the Lie algebra of  $\mathbf{SL}(2, \mathbb{R})$ ; and show that this Lie algebra  $\mathfrak{sl}(2, \mathbb{R})$  has just 1 simple representation of each dimension  $1, 2, 3, \dots$

**Answer:** Suppose  $L$  is a real Lie algebra. A representation of  $L$  in the complex vector space  $V$  is defined by giving a map

$$L \times V \rightarrow V : (X, v) \mapsto Xv$$

which is bilinear over  $\mathbb{R}$  and which satisfies the condition

$$[X, Y]v = X(Yv) - Y(Xv)$$

for all  $X, Y \in L, v \in V$ .

A representation of  $L$  in  $V$  is thus the same as a representation of the complexification  $L_{\mathbb{C}}$  of  $L$  in  $V$ .

Suppose  $\alpha$  is a representation of the linear group  $G$ , ie a homomorphism

$$\alpha : G \rightarrow \mathbf{GL}(n, \mathbb{C}).$$

Under the Lie correspondence this gives rise to a Lie algebra homomorphism

$$A = \mathcal{L}\alpha : L = \mathcal{L}G \rightarrow \mathfrak{gl}(n, \mathbb{C}).$$

But now  $L$  acts on  $V = \mathbb{C}^n$  by

$$Xv = A(X)v.$$

This defines a representation of  $L$  in  $V$  since

$$\begin{aligned} [X, Y]v &= A([X, Y])v \\ &= [AX, AY]v \\ &= ((AX)(AY) - (AY)(AX))v \\ &= X(Yv) - Y(Xv). \end{aligned}$$

We have

$$\begin{aligned} \mathfrak{sl}(2, \mathbb{R}) &= \{X \in \mathbf{Mat}(2, \mathbb{R}) : e^{tX} \in \mathbf{SL}(2, \mathbb{R}) \forall t \in \mathbb{R}\} \\ &= \{X : \det e^{tX} = 1 \forall t\} \\ &= \{X : e^{t \operatorname{tr} X} = 1 \forall t\} \\ &= \{X : \operatorname{tr} X = 0\}. \end{aligned}$$

The 3 matrices

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

form a basis for the vector space  $\mathfrak{sl}(2, \mathbb{R})$ .

We have

$$[H, E] = 2E, \quad [H, F] = -2F, \quad [E, F] = H.$$

Thus

$$\mathfrak{sl}(2, \mathbb{R}) = \langle H, E, F : [H, E] = 2E, [H, F] = -2F, [E, F] = H \rangle.$$

Now suppose we have a simple representation of  $\mathfrak{sl}(2, \mathbb{R})$  on  $V$ . Suppose  $v$  is an eigenvector of  $H$  with eigenvalue  $\lambda$ :

$$Hv = \lambda v.$$

Now

$$[H, E]v = 2Ev,$$

that is,

$$HEv - EHv = 2Ev.$$

In other words, since  $Hv = \lambda v$ ,

$$H(Ev) = (\lambda + 2)Ev,$$

ie  $Ev$  is an eigenvector of  $H$  with eigenvalue  $\lambda + 2$ .

By the same argument  $E^2v, E^3v, \dots$  are all eigenvectors of  $H$  with eigenvalues  $\lambda + 4, \lambda + 6, \dots$ , at least until they vanish.

This must happen at some point, since  $V$  is finite-dimensional; say

$$E^{r+1}v = 0, E^r v \neq 0.$$

Similarly we find that

$$Fv, F^2v, \dots$$

are also eigenvectors of  $H$  (until they vanish) with eigenvalues  $\lambda - 2, \lambda - 4, \dots$ . Again we must have

$$F^{s+1}v = 0, F^s v \neq 0$$

for some  $s$ .

Now let us write  $e_0$  for  $F^s v$ , so that

$$Fe_0 = 0;$$

and let us set

$$e^i = E^i e_0.$$

Then the  $e_i$  are all eigenvectors of  $H$ . Let us set  $e_i = 0$  for  $i$  outside the range  $[0, n - 1]$ . Suppose  $e_0$  is a  $\mu$ -eigenvector. Then  $e_i$  is a  $(\mu + 2i)$ -eigenvector. Let us suppose that there are  $n$  eigenvectors in the sequence, ie

$$e_{n-1} \neq 0, \quad Ee_{n-1} = 0.$$

Now we show by induction that

$$Fe_i = \rho_i e_{i-1}$$

for each  $i$ . The result holds for  $i = 0$  with  $\rho_0 = 0$ . Suppose it holds for  $i = 1, 2, \dots, m$ . Then

$$\begin{aligned} Fe_{m+1} &= F E e_m \\ &= (EF - [E, F])e_m \\ &= \rho_m E e_{m-1} - H e_m \\ &= (\rho_m - \mu - 2m)e_m. \end{aligned}$$

This proves the result, and also shows that

$$\rho_{i+1} = \rho_i - \mu - 2i$$

for each  $i$ . It follows that

$$\rho_i = -i\mu - i(i - 1).$$

We must have  $\rho_n = 0$ . Hence

$$\mu = n - 1.$$

We conclude that the subspace

$$\langle e_0, \dots, e_{n-1} \rangle$$

is stable under  $\mathfrak{sl}(2, \mathbb{R})$ , and so must be the whole of  $V$ .

Thus we have shown that there is at most 1 simple representation of each dimension  $n$ , and we have determined this explicitly, if it exists. In fact it is a straightforward matter to verify that the above actions of  $H, E, F$  on  $\langle e_0, \dots, e_{n-1} \rangle$  do indeed define a representation of  $\mathfrak{sl}(2, \mathbb{R})$ ; so that this Lie algebra has exactly 1 simple representation of each dimension.

5. Show that a compact connected abelian linear group of dimension  $n$  is necessarily isomorphic to the torus  $\mathbb{T}^n$ .

**Answer:** If  $G$  is a abelian linear group then  $\mathcal{L}G$  is trivial, ie  $[X, Y] = 0$  for all  $X, Y \in \mathcal{L}G$ . For  $e^{tX}, e^{tY} \in G$  commute for all  $t$ . If  $t$  is sufficiently small we can take logs, and deduce that  $tX = \log(e^{tX}), tY = \log(e^{tY})$  commute. Hence  $X, Y$  commute.

The map

$$\Theta : \mathcal{L}G \rightarrow G$$

under which

$$X \mapsto e^X$$

is a homomorphism, since

$$X + Y \mapsto e^{X+Y} = e^X e^Y.$$

For any linear group  $G$ , there exist open subsets  $U \ni 0$  in  $\mathcal{L}G$ ,  $V \ni I$  in  $G$  such that  $X \mapsto e^X$  defines a homeomorphism  $U \rightarrow V$ .

It follows that  $\text{im } \Theta \subset \mathcal{L}G$  is an open subgroup of  $G$ . Since  $G$  is connected,  $\text{im } \Theta = G$ . Thus

$$G \cong \mathcal{L}G / \ker \Theta.$$

Moreover,  $\ker \Theta$  is discrete, since  $U \cap \ker \Theta = \{0\}$ . Thus

$$G \cong \mathbb{R}^n / K,$$

where  $K$  is a discrete subgroup, and  $n = \dim G$ .

Lemma: A discrete subgroup  $K \subset \mathbb{R}^n$  is necessarily  $\cong \mathbb{Z}^d$  for some  $d \leq n$ , ie we can find a  $\mathbb{Z}$ -basis  $k_1, \dots, k_d$  for  $K$  such that

$$K = \{n_1 k_1 + \dots + n_d k_d : n_1, \dots, n_d \in \mathbb{Z}\}.$$

Proof: Let  $k_1$  be one of the closest points to 0 in  $K \setminus \{0\}$ . Then let  $k_2$  be one of the closest points to the subspace  $\langle k_1 \rangle$  in  $K \setminus \langle k_1 \rangle$ , let  $k_3$  be one of the closest points to the subspace  $\langle k_1, k_2 \rangle$  in  $K \setminus \langle k_1, k_2 \rangle$ , and so on.

Then  $k_1, k_2, \dots$  are linearly independent. So the process must end after  $d \leq n$  steps:

$$K = \langle k_1, \dots, k_d \rangle.$$

Now suppose  $k \in K$ , say

$$k = \lambda_1 k_1 + \cdots + \lambda_d k_d.$$

We show that  $\lambda_1, \dots, \lambda_d \in \mathbb{Z}$ . Let

$$\lambda_d = r + \epsilon,$$

where  $r \in \mathbb{Z}$  and  $|\epsilon| \leq 1/2$ . Then

$$k - r k_d = \lambda_1 k_1 + \cdots + \lambda_{d-1} k_{d-1} + \epsilon k_d$$

is closer to  $\langle k_1, \dots, k_{d-1} \rangle$  than is  $k_d$ . Hence  $\epsilon = 0$ , ie  $\lambda_d \in \mathbb{Z}$ .

Applying the same argument to

$$k - \lambda_d k_d = \lambda_1 k_1 + \cdots + \lambda_{d-1} k_{d-1},$$

we deduce that  $\lambda_{d-1} \in \mathbb{Z}$ ; and so successively  $\lambda_{d-2}, \dots, \lambda_1 \in \mathbb{Z}$

Thus  $k_1, \dots, k_d$  is a  $\mathbb{Z}$ -basis for  $K$ . Extend  $k_1, \dots, k_d$  to a basis  $k_1, \dots, k_d, e_1, \dots, e_{n-d}$  of  $\mathbb{R}^n$ . Then

$$\begin{aligned} G &\cong \mathbb{R}^n / K \cong \mathbb{R}/\mathbb{Z} \oplus \cdots \oplus \mathbb{R}/\mathbb{Z} \\ &\cong \mathbb{T}^d \oplus \mathbb{R}^{n-d}. \end{aligned}$$

Since  $G$  is compact,  $n - d = 0$ , ie

$$G \cong \mathbb{T}^n.$$