

**Exercise** Let  $\{E_{i,j}\}_{i < j}$  be the set of all elementary matrices, of this form. Prove that  $E_{i,j}^{-1} = (b_{l,k})$  is  $E_{i,j} = (a_{l,k})$ , when we substitute  $a_{i,j} = 1$  with  $b_{i,j} = -1$

**Proof** We can see that directly from the fact that if we multiply  $E_{i,j}^{-1}$  by  $E_{i,j}$  from the left then  $E_{i,j}$  is operating on  $E_{i,j}^{-1}$  by adding row  $j$  to row  $i$ . So, in the product matrix,  $(c_{l,k})$ , in order to have 1 on the main diagonal, we need them to exist on the main diagonal of  $E_{i,j}^{-1}$ , to begin with. Now, in order to have  $c_{i,j} = 0$ , we need to have the addition of  $j$  to  $i$  giving  $c_{i,j} = a_{i,j} + b_{i,j} = 0 \Rightarrow b_{i,j} = -a_{i,j} = -1$

**Exercise** Prove that if  $(a_{ij}) = E_{i,j}$ ,  $i < j$  is an elementary matrix, then  $\forall m \in (N)$ ,  $E_{i,j}^m$  is  $E_{i,j}$ , but with  $a_{ij} = m$

$$E_{i,j} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

$$E_{i,j}^2 = E_{i,j} \cdot E_{i,j}$$

Since  $E_{i,j}$  is an elementary matrix, then it operates on the right matrix as an addition of row  $j$  to row  $i$

So,

$$E_{i,j}^2 = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & 2 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

We assume this is true for all  $E_{i,j}^m$ , now we prove for  $E_{i,j}^{m+1}$

$$E_{i,j}^{m+1} = E_{i,j} \cdot E_{i,j}^m = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}^m$$

(by the assumption)

$$= \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & m & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \ddots & m+1 & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

From these two exercises, we obtain an almost trivial corollary

**Exercise** Prove that if  $(a_{ij}) = E_{i,j}$ ,  $i < j$  is an elementary matrix, then  $\forall m \in (N)$ ,  $(E_{i,j}^{-1})^m = (E_{i,j}^m)^{-1} = E_{i,j}^{-m}$  is  $E_{i,j}$ , but with  $a_{ij} = -m$

**Proof** We immitate both proofs from above (we can either show how the power of  $m$  is operating on  $E_{i,j}^{-1}$ , or show how the inversion is operating on  $E_{i,j}^m$ ).

## Commutators of elementary matrices

Let  $\{E_{i,j}\}_{i < j}$  be the set of all elementary matrices of this form.

**Exercise**  $(a_{l,m}) = E_{i,j}^{-1}$  is the matrix with 1 on the main diagonal, and  $-1$  in  $a_{i,j}$

**Proof** We can see that directly from the fact that in order to have

$$(c_{l,m}) = (a_{l,m}) \cdot (b_{l,m}) = E_{i,j} \cdot E_{i,j}^{-1} = I,$$

we need to have  $c_{i,j} = 0$ , which means that adding row  $j$  to row  $i$ , in  $E_{i,j}^{-1}$  (by the left multiplication of  $E_{i,j}$ )

must give  $a_{i,j} + b_{i,j} = c_{i,j} = 0 \Rightarrow b_{i,j} = -a_{i,j} = -1$

**Exercise**  $[E_{i,j}, E_{j,k}] = E_{i,k}$

**Proof**  $E_{i,j}$  is operating from left on  $E_{j,k}$  by addition of row  $j$  to row  $i$ , so, the product matrix,  $(a_{l,m}) = E_{i,j} \cdot E_{j,k}$  has 1 on the main diagonal and in  $a_{j,k}, a_{i,j}, a_{i,k}$

$E_{i,j}^{-1}$  is operating from left on  $E_{j,k}^{-1}$  by subtraction of row  $j$  from row  $i$ , so, the product matrix,  $(b_{l,m}) = E_{i,j}^{-1} \cdot E_{j,k}^{-1}$  has 1 on the main diagonal and in  $b_{i,k}$ , and  $-1$  in  $b_{j,k}, b_{i,j}$

Multiplying  $(a_{l,m}) \cdot (b_{l,m})$  yields a product matrix,  $(c_{l,m})$  with 1 on the main diagonal, and,

since  $a_{i,i} = a_{i,j} = a_{i,k} = 1$ , with all other cells in row  $j$  being 0, and since  $b_{i,k} = b_{j,k} = 1$ , and  $b_{j,k} = -1$ , multiplying row  $(a_{l,m})_i$  by column  $(b_{l,m})_k$  yields the value  $c_{i,k} = b_{i,k} + b_{j,k} + b_{k,k} = 1 - 1 + 1 = 1$

We can see that multiplying  $(a_{l,m})_i \cdot (b_{l,m})_j$  yields  $c_{i,j} = a_{i,i} \cdot b_{i,j} + a_{i,j} \cdot b_{j,j} = 1 \cdot -1 + 1 \cdot 1 = 1 - 1 = 0$

And, we can see that multiplying  $(a_{l,m})_j \cdot (b_{l,m})_k$  yields  $c_{j,k} = a_{j,j} \cdot b_{j,k} + a_{j,k} \cdot b_{k,k} = 1 \cdot -1 + 1 \cdot 1 = 1 - 1 = 0$

### Conclusion

$$[E_{j,k}, E_{i,j}] = E_{j,k} \cdot E_{i,j} \cdot E_{j,k}^{-1} \cdot E_{i,j}^{-1} = ((E_{i,j}^{-1})^{-1} \cdot (E_{j,k}^{-1})^{-1} \cdot E_{i,j}^{-1} \cdot E_{j,k}^{-1})^{-1} = (E_{i,j} \cdot E_{j,k} \cdot E_{i,j}^{-1} \cdot E_{j,k}^{-1})^{-1} = [E_{i,j}, E_{j,k}]^{-1}$$

For example,  $n = 4$ ,

$$E_{1,2} \cdot E_{2,3} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned}
E_{1,2}^{-1} \cdot E_{2,3}^{-1} &= \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
[E_{1,2} \cdot E_{2,3}] &= E_{1,2} \cdot E_{2,3} \cdot E_{1,2}^{-1} \cdot E_{2,3}^{-1} = \\
&= \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = E_{1,3}
\end{aligned}$$

**Exercise**  $[E_{i,j}, E_{l,k}] = I$ , where  $j \neq l$

**Proof**  $E_{i,j}$  is operating from left on  $E_{l,k}$  by addition of row  $j$  to row  $i$ , so, the product matrix,  $(a_{n,m} = E_{i,j} \cdot E_{l,k})$  has 1 on the main diagonal and in  $a_{l,k}, a_{i,j}$

$E_{i,j}^{-1}$  is operating from left on  $E_{l,k}^{-1}$  by subtraction of row  $j$  from row  $i$ , so, the product matrix,  $(b_{n,m} = E_{i,j}^{-1} \cdot E_{l,k}^{-1})$  has 1 on the main diagonal, and  $-1$  in  $b_{l,k}, b_{i,j}$

We can see that multiplying  $(a_{n,m})_i \cdot (b_{n,m})_j$  yields  $c_{i,j} = a_{i,i} \cdot b_{i,j} + a_{i,j} \cdot b_{j,j} = 1 \cdot -1 + 1 \cdot 1 = 1 - 1 = 0$

And, we can see that multiplying  $(a_{n,m})_l \cdot (b_{n,m})_k$  yields  $c_{l,k} = a_{l,l} \cdot b_{l,k} + a_{l,k} \cdot b_{k,k} = 1 \cdot -1 + 1 \cdot 1 = 1 - 1 = 0$

For example,  $n = 4$ ,

$$\begin{aligned}
E_{1,2} \cdot E_{3,4} &= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
E_{1,2}^{-1} \cdot E_{3,4}^{-1} &= \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
[E_{1,2} \cdot E_{3,4}] &= E_{1,2} \cdot E_{3,4} \cdot E_{1,2}^{-1} \cdot E_{3,4}^{-1} = \\
&= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I
\end{aligned}$$

### Conclusion

$$\begin{aligned} [E_{i,j}, [E_{j,k}, E_{k,l}]] &= [E_{i,j}, E_{j,l}] = E_{i,l} \\ [E_{i,j}, [E_{j,k}, E_{m,l}]], m \neq k &= [E_{i,l}, I] = I \\ [E_{i,m}, [E_{j,k}, E_{k,l}]], m \neq j &= [E_{i,m}, E_{j,l}] = I \end{aligned}$$

$$\Rightarrow [E_{i_1, i_2}, [E_{i_3, i_4}, \dots [E_{i_{n-2}, i_{n-1}}, E_{i_{n-1}, i_n}]]] = \begin{cases} E_{i_1, i_n}, & i_{2k} = i_{2k+1}, \forall 1 \leq k \leq \frac{n}{2} - 1 \\ I, & \text{otherwise} \end{cases}$$

### Exercise

$$\#\{E_{i,j} \in M_n(\mathbb{Z})\}_{i < j} = \binom{n}{2}$$

### Proof

$(a_{i,j} = E_{i,j})$ . We need to count the options for 1 above the main diagonal.  
 $a_{l,l} = 1, \forall 1 \leq l \leq n$ , so, if  $i = l$ , we have  $n - l = n - i$  options to choose the column index  $j$ .

So, the total number of options for  $i, j$  is  $\sum_{k=1}^{n-1} = \frac{(1+n-1) \cdot (n-1)}{2} = \frac{n \cdot (n-1)}{2} = \binom{n}{2}$

This means that we have  $\binom{n}{2}^2$  commutators of the form  $[E_{i,j}, E_{l,k}]$ .

### Exercise

$$\#\{[E_{i,j}, E_{l,k}] \neq I \in M_n(\mathbb{Z})\}_{i < j} = 2 \cdot \binom{n}{3}$$

### Proof

As shown above,  $[E_{i,j}, E_{l,k}] \neq I \Leftrightarrow j = l$

Which means we're counting all the commutators of the form  $[E_{i,j}, E_{j,k}]$ .

So, the count of such commutators is based on the number of options to choose

ordered triples  $\{i, j, k\}$  out of the ordered set  $[n] = \{1, 2, \dots, n\}$ , which is  $\binom{n}{3}$   
 But, as already shown above,  $[E_{l,k}, E_{i,j}] = [E_{i,j}, E_{l,k}]^{-1}$ , so, for each triple  $\{i, j, k\}$ , we have two commutators,  $[E_{i,j}, E_{j,k}]$  and its inverse, which sum up to  $\binom{n}{3}$  pairs of commutators.

For example,  $n = 5$ ,

$$(a_{l,k}) = E_{i,j} = \begin{pmatrix} 1 & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} \\ 0 & 1 & a_{2,3} & a_{2,4} & a_{2,5} \\ 0 & 0 & 1 & a_{3,4} & a_{3,5} \\ 0 & 0 & 0 & 1 & a_{4,5} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Where  $a_{i,j} = 1$ , and all other  $a_{i,k} = 0$

The number of options for choosing  $i, j$ , in this case, are  $1 + 2 + 3 + 4 = 10 = \binom{5}{2}$ ,

so, we have  $10^2 = 100$  commutators. The number of triples we can choose from  $[5] = \{1, 2, 3, 4, 5\}$  is

$$\#\{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 3, 4\}, \{2, 3, 5\}, \{2, 4, 5\}, \{3, 4, 5\}\} = 10 = \binom{5}{3},$$

so we have 10 commutators that are not the unit matrix, and their inverse, total  $20 = 2 \cdot 10 = 2 \cdot \binom{5}{3}$ .

### Exercise

Given the set of commutators of elementary matrices of the form

$$\{[E_{i,j}, E_{j,k}] \in M_n(\mathbb{Z})\}_{i < j < k},$$

we can divide this set to subsets of the form

$$\{[E_{i_1,j_{1,1}}, E_{j_{1,1},k_1}], [E_{i_1,j_{1,2}}, E_{j_{1,2},k_1}], \dots, [E_{i_1,j_{1,l_1}}, E_{j_{1,l_1},k_1}]\}, \dots, \\ \{[E_{i_m,j_{m,1}}, E_{j_{m,1},k_1}], \dots, [E_{i_m,j_{m,l_m}}, E_{j_{m,l_m},k_1}]\}$$

These subsets are equivalence classes, trivially, since the relation is equality (i.e.  $[E_{i_l,j_{l,m_1}}, E_{j_{l,m_1},k_l}] = [E_{i_l,j_{l,m_2}}, E_{j_{l,m_2},k_l}], i_l < j_{l,m_1}, j_{l,m_2} < k_l$ ).

Fix  $i, k, 1 \leq i \leq n-1, 3 \leq k \leq n$ , then all the triples of the form  $\{i, j, k\}, i \leq i+1 \leq k-1$  are in the same equivalence class,

due to the above equality. So, the number of these equivalence classes is  $2 \cdot \binom{n-1}{2}$

### Proof

By induction on  $n$ . For  $n = 3$ , we have only one triple, namely  $\{1, 2, 3\}$ , so  $\binom{3-1}{2} = \binom{2}{2} = 1$

For  $n + 1$ , we shall observe that if we add one to the upper bound (i.e.  $n \rightarrow n' = n + 1$ ,

then we add one more equivalence class, for each one of the lower bounds of  $n' - 1 = n$  (i.e., the index  $i$ ).

But we also add a new equivalence class, whose lower bound is  $i = n + 1 - 2 = n - 1 = n' - 2$ , which was not in any equivalence class

for  $n = n' - 1$ , since we consider only the triples where  $i \leq n - 2$ . So, if we mark  $m_n$  as the number of equivalence classes

for  $n$ , then we have  $m_{n'} = m_{n+1} = m_n + (n - 2) + 1 = m_n + n - 1$ . But, by the assumption,  $m_n = \binom{n-1}{2}$ ,

$$\text{so } m_{n'} = m_{n+1} = m_n + n - 1 = \binom{n-1}{2} + n - 1 = \frac{(n-1) \cdot (n-2)}{2} + n - 1 =$$

$\frac{n^2-3n+2}{2} + n - 1 = \frac{n^2-3n+2+2n-2}{2} = \frac{n^2-n}{2} = \frac{n \cdot (n-1)}{2} = \binom{n}{2} = m_{n+1} = m_{n'}$ , and we proved the assumption

### The group $U_n(\mathbb{Z})$

We have proved several basic facts, regarding elementary matrices, of the form  $\{E_{i,j}\}_{i < j}$ .

Now, we shall propose a few more basic facts.

### Notation

We mark by  $U_n(\mathbb{Z})$  the set of all upper triangular matrices  $n \times n$  with 1 in the main diagonal, and any integer values above the main diagonal,  $a_{i,j} \in \mathbb{Z}$ .

**Exercise** Prove that the set  $U_n(\mathbb{Z})$  is a group, with the usual operation of matrix multiplication.

### Proof

$$(a_{i,j}) = A = \begin{pmatrix} 1 & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ 0 & 1 & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_{k,n-1} & a_{k,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{n-1,n} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, (b_{i,j}) = B = \begin{pmatrix} 1 & b_{1,2} & \dots & b_{1,n-1} & b_{1,n} \\ 0 & 1 & \dots & b_{2,n-1} & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & b_{k,n-1} & b_{k,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & b_{n-1,n} \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

We need to prove that  $(c_{i,j}) = A \cdot B \in U_n(\mathbb{Z})$

I.  $1 \leq l \leq n, c_{l,l} = \sum_{k=1}^n a_{l,k} \cdot b_{k,l}$ .

We observe that  $a_{l,1} = a_{l,2} = \dots = a_{l,l-1} = 0$ , and  $b_{l+l,l} = b_{l+2,l} = \dots = b_{n,l} = 0$ .

So,  $c_{l,l} = \sum_{k=1}^n a_{l,k} \cdot b_{k,l} = 0 + 0 + \dots + 0 + a_{l,l} \cdot b_{l,l} + 0 + 0 \dots 0 = 1$ .

This proves that each element on the main diagonal of  $(c_{i,j})$  is 1.

II.  $2 \leq l \leq n, 1 \leq m \leq l - 1, c_{l,m} = \sum_{k=1}^n a_{l,k} \cdot b_{k,m}$ .

We observe that  $a_{l,1} = a_{l,2} = \dots = a_{l,l-1} = 0$ , and  $b_{m+1,m} = b_{m+2,m} = \dots = b_{n,m} = 0$ .

This means, that  $a_{l,k} \cdot b_{k,m} = 0, 1 \leq k \leq l - 1$ ,

because the first  $l - 1$  elements of  $a_{l,k}$  are 0.

and the last  $n - m$  elements of  $b_{k,m}$  are also 0.

This proves that each element under the main diagonal of  $(c_{i,j})$  is 0.

III.  $2 \leq l \leq n, 1 \leq m \leq l-1, c_{m,l} = \sum_{k=1}^n a_{m,k} \cdot b_{k,l}$ .  
 $a_{m,k}, b_{k,l} \in \mathbb{Z} \Rightarrow \sum_{k=1}^n a_{l,k} \cdot b_{k,m} \in \mathbb{Z}$ .

This proves the each element above the main diagonal of  $(c_{i,j})$  is an integer.

Thus, we prove that  $U_n(\mathbb{Z})$  is closed under matrix multiplication.

Associativity is obvious, from the fact that matrix multiplication is associative.

Obviously,  $I_n$  is a matrix of this form, so the unit of  $U_n(\mathbb{Z})$  is  $I_n$ .

The fact that all matrices of this form have an inverse is obvious by looking at the rank of a matrix of this form, which, clearly, is  $n$ , since the matrix is already in a reduced form.

Conclusion:  $U_n(\mathbb{Z})$  is a group.

**Exercise** All the matrices of the form  $\{E_{i,i+1}, 1 \leq i \leq n-1\}$  generate  $U_n(\mathbb{Z})$ .

### Proof

We already proved that  $[E_{i,j}, E_{j,k}] = E_{i,k}$ , specifically,  $[E_{i,i+1}, E_{i+1,i+2}] = E_{i,i+2}$ .

Also, we proved that  $\forall m \in \mathbb{N}, (a_{i,j})^m = E_{i,j}^m = (a_{i,j})$  with  $a_{i,j} = m$ .

This mean that all the matrices of the form  $\{E_{i,i+1}\}$  yield all the matrices which have only one integer above the main diagonal.

Let

$$(a_{i,j}) = A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_{i,j} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, (b_{l,k}) = B = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & b_{l,k} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$



$|a_{i,j}|, |b_{l,k}| > 1$ , and the two pairs of indices,  $\{i, j\}, \{l, k\}$ , are pairwise disjoint. Then,  $(c_{m,p}) = A \cdot B$  is the matrix with 1 on the main diagonal, 0 below the main diagonal,

and  $c_{i,j} = a_{i,j}, c_{l,k} = b_{l,k}$ .

To prove this, we can observe that since  $|a_{i,j}|, |b_{l,k}| > 1$ , we can write (based on what we already proved)

$$(a_{i,j}) = A = E_{i,j}^{a_{i,j}}$$

### The free Lie algebra $L_n$

The group  $U_n(\mathbb{Z})$  gives rise to a Lie algebra over some field  $\mathbb{F}$ , which consists of all matrices of the form

$$(a_{l,k}) = \begin{pmatrix} 0 & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ 0 & 0 & a_{2,3} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Which means, we have 0 on the main diagonal and under it, and  $a_{i,j} \in \mathbb{F}, i < j$ ,

that is, arbitrary scalars above the main diagonal. These matrices are precisely the matrices of  $U_n(\mathbb{Z})$

minus the unit matrix, and with scalars from  $\mathbb{F}$ , rather than  $\mathbb{Z}$ .

**Exercise** This is a Lie algebra over  $\mathbb{F}$

#### Proof

Defining the multiplication (Lie brackets) on  $L_n$  by the standard matrix commutator (i.e.,  $\forall A, B \in M_n(\mathbb{F}), [A, B] := A \cdot B - B \cdot A$ , automatically gives all the Lie algebra axioms, for example,

$\forall A, B, C \in M_n(\mathbb{F}), \alpha, \beta \in \mathbb{F}$ ,

$$[\alpha \cdot A + \beta \cdot B, C] = (\alpha \cdot A + \beta \cdot B) \cdot C - C \cdot (\alpha \cdot A + \beta \cdot B) =$$

$$(\alpha \cdot A) \cdot C + (\beta \cdot B) \cdot C - (C \cdot (\alpha \cdot A) + C \cdot (\beta \cdot B)) =$$

$$\alpha \cdot (A \cdot C) + \beta \cdot (B \cdot C) - \alpha \cdot (C \cdot A) - \beta \cdot (C \cdot B) =$$

$$\alpha \cdot (A \cdot C) - \alpha \cdot (C \cdot A) + \beta \cdot (B \cdot C) - \beta \cdot (C \cdot B) =$$

$$\alpha \cdot (A \cdot C - C \cdot A) + \beta \cdot (B \cdot C - C \cdot B) = \alpha \cdot [A, C] + \beta \cdot [B, C]$$

, Thus we prove linearity in the first component. There should be no need to prove all other axioms,

since they can all be easily proved using the same matrix and scalar multiplications.

We do need to prove that  $L$  is closed under Lie brackets defined above.

Let

$$A = (a_{l,k}) = \begin{pmatrix} 0 & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ 0 & 0 & a_{2,3} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}, B = (b_{l,k}) = \begin{pmatrix} 0 & b_{1,2} & b_{1,3} & \dots & b_{1,n} \\ 0 & 0 & b_{2,3} & \dots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & b_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Then,

$$A \cdot B = \begin{pmatrix} 0 & 0 & a_{1,2} \cdot b_{2,3} & \dots & \sum_{k=2}^{n-1} a_{1,k} \cdot b_{k,n} \\ 0 & 0 & 0 & \dots & \sum_{k=3}^{n-1} a_{2,k} \cdot b_{k,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_{n-1,n} \cdot b_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} 0 & 0 & b_{1,2} \cdot a_{2,3} & \dots & \sum_{k=2}^{n-1} b_{1,k} \cdot a_{k,n} \\ 0 & 0 & 0 & \dots & \sum_{k=3}^{n-1} b_{2,k} \cdot a_{k,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & b_{n-1,n} \cdot a_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

And then,

$$[A, B] = A \cdot B - B \cdot A = \begin{pmatrix} 0 & 0 & a_{1,2} - b_{1,2} \cdot a_{2,3} & \dots & \sum_{k=2}^{n-1} a_{1,k} \cdot b_{k,n} - \sum_{k=2}^{n-1} b_{1,k} \cdot a_{k,n} \\ 0 & 0 & 0 & \dots & \sum_{k=3}^{n-1} a_{2,k} \cdot b_{k,n} - \sum_{k=3}^{n-1} b_{2,k} \cdot a_{k,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & a_{n-1,n} \cdot b_{n-1,n} - b_{n-1,n} \cdot a_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

So, the Lie brackets operation, defined above, is preserving the form of the matrices in  $L_n$ .

In addition, we observe that the second diagonal, above the main diagonal, is also 0, thus we conclude

that  $\forall A, B, C, D \in L_n, [[A, B], [C, D]]$  will have the main, the second and the third diagonal all 0.

In other words,  $L_n$  is a nilpotent Lie algebra.

After verifying that the Lie brackets operation is defined, as multiplication in  $L_n$ , we observe also that  $L_n$

is closed under addition, defined as the standard matrix addition. But this is obvious since the matrix addition is simply  $a_{i,j} + b_{i,j}, 1 \leq i, j \leq n$ ,

and so, the sums of all 0 on the main diagonal and under it, which means  $a_{i,j} + b_{i,j}, j \leq i = 0 + 0 = 0$

And the sums of all elements above the main diagonal,  $a_{i,j} + b_{i,j}, j > i$ , are sums of two scalars in  $\mathbb{F}$ ,

hence, scalars in the same field.

in the same way,  $L_n$  being closed under multiplication by a scalar is also a trivial fact.

**Exercise** The Lie algebra  $L_n$  has a base, which is all the elementary matrices of the form  $E_{i,i+1}$  minus the unit matrix, that is,  $e_{i,i+1} = E_{i,i+1} - I$ .

**Exercise** The Lie brackets operation on  $L_n$  is compatible with the operation of the  $U_n$  group commutators i.e.,  $[e_{i,j}, e_{l,k}] \neq 0 \Leftrightarrow j = l \vee i = k$ .

**Proof**

We shall distinguish between the two cases,

$j = l$

$A = (a_{i,j})$  a matrix with 1 only in  $a_{i,j}$

$B = (b_{j,k})$  a matrix with 1 only in  $b_{j,k}$

Then  $(c_{i,k}) = A \cdot B$  is a matrix with 1 only in  $c_{i,k}$

(we obtain this by multiplying row  $i$  of  $A$  with column  $k$  of  $B$ , having only  $a_{i,j} \cdot b_{j,k} = 1 \cdot 1 = 1$ ),

while  $(d_{s,t}) = B \cdot A$  is a zero matrix. since multiplying row  $j$  of  $B$  with column  $j$  of  $A$  yields  $b_{j,k} \cdot a_{k,j} + b_{j,i} \cdot a_{i,j} =$

$$1 \cdot 0 + 0 \cdot 1 = 0 + 0 = 0$$

Hence,  $A \cdot B - B \cdot A = (c_{i,k}) - 0 = (c_{i,k}) = e_{i,k} = E_{i,k} - I$

$i = k$

$A = (a_{i,j})$  a matrix with 1 only in  $a_{i,j}$

$B = (b_{k,i})$  a matrix with 1 only in  $b_{k,i}$

We can observe that this case is exactly the opposite of the first case, since multiplying  $A \cdot B$  yields a zero matrix, while multiplying

$B \cdot A$  yields a matrix  $c_{k,j}$  with 1 only in  $c_{k,j}$

Hence,  $A \cdot B - B \cdot A = 0 - (c_{k,j}) = -(c_{k,j}) = -e_{k,j} = E_{k,j} - I$

**Exercise**

The Lie algebra  $L = L_n$ , has its lower central series,

$\gamma_k(L)$  (defined recursively by  $\gamma_k(L) := [L, \gamma_{k-1}(L)]$ , where  $\gamma_1(L) := L$ ),

$\gamma_k(L) \neq 0, \forall k < n$ , and  $\gamma_n(L) = 0$

**Proof**

$$\text{As seen above, } [e_{i,j}, e_{l,k}] = \begin{cases} e_{i,k} & j = l \\ -e_{l,j} & i = k \\ 0 & \text{otherwise} \end{cases}$$

So, if the base of  $L_n$  is  $B(L) = \{e_{i,i+1} | 1 \leq i \leq n-1\}$ , we can see that

$$\gamma_2(B(L)) = [B(L), B(L)] = \{e_{i,i+2} | 1 \leq i \leq n-1\},$$

containing only elements which come from commutators of the form

$$[e_{i,i+1}, e_{i+1,i+2}] = e_{i,i+2} \text{ (or } [e_{i+1,i+2}, e_{i,i+1}] = -e_{i,i+2})$$

So,  $\gamma_3(B(L)) = [B(L), \gamma_2(B(L))] = \{e_{i,i+3} | 1 \leq i \leq n-1\}$ , since the only commutators that are not 0, are of the form  $[e_{i,i+1}, e_{i+1,(i+1)+2}] = [e_{i,i+1}, e_{i+1,i+2+1}] = [e_{i,i+1}, e_{i+1,i+3}] = e_{i,i+3}$

Obviously,  $\gamma_{n-1}(B(L))$  must contain only commutators of the form  $e_{i,i+n-1}$ , which can only be  $e_{1,1+n-1} = e_{1,n}$

That means, for  $\gamma_n(B(L))$ , we have no valid commutators, since we do not have any element with a second index  $n+1$

$$\text{So, } \gamma_n(B(L)) = 0$$

**Exercise** The Lie algebra  $L_n$ , has an automorphism,  $\eta$ , defined by,

$$1 \leq i < j \leq n, a_{i,j} \in \mathbb{F}, \eta(a_{i,j} \cdot e_{i,j}) := (-1)^{j-i+1} \cdot (a_{i,j} \cdot e_{n-j+1, n-i+1}) = a_{i,j} \cdot (-1)^{j-i+1} \cdot e_{n-j+1, n-i+1}$$

**Proof**

First, we need to show that  $\eta$  is a homomorphism.

We shall omit the scalars, as the Lie brackets operation is bilinear.

$$\begin{aligned} 1 \leq i < j < k \leq n, [\eta(e_{i,j}), \eta(e_{j,k})] &= \\ [(-1)^{j-i+1} \cdot e_{n-j+1, n-i+1}, (-1)^{k-j+1} \cdot e_{n-k+1, n-j+1}] &= \\ (-1)^{j-i+1} \cdot (-1)^{k-j+1} [e_{n-j+1, n-i+1}, e_{n-k+1, n-j+1}] &= \\ (-1)^{j-i+1+k-j+1} \cdot -e_{n-k+1, n-i+1} &= (-1)^{k-i+2} \cdot -e_{n-k+1, n-i+1} = \\ (-1)^{k-i} \cdot (-1)^2 \cdot -e_{n-k+1, n-i+1} &= (-1)^{k-i} \cdot -e_{n-k+1, n-i+1} = \\ (-1)^{k-i} \cdot (-1) \cdot e_{n-k+1, n-i+1} &= (-1)^{k-i+1} \cdot e_{n-k+1, n-i+1} = \eta(e_{i,k}) = \eta([e_{i,j}, e_{j,k}]) \end{aligned}$$

So, we proved that  $\eta$  is a homomorphism, obviously from  $L_n$  to itself.

To prove the rest, we can observe that  $\eta$  defines a bijection on the base elements of  $L_n$ ,

$$1 \leq i < n,$$

$$\eta(e_{i,i+1}) = (-1)^{i+1-i+1} \cdot e_{n-(i+1)+1, n-i+1} =$$

$$(-1)^2 \cdot e_{n-i-1+1, n-i+1} = 1 \cdot e_{n-i, n-i+1}$$

and,

$$\eta(e_{n-i, n-i+1}) = (-1)^{n-i+1-(n-i)+1} \cdot e_{n-(n-i+1)+1, n-(n-i)+1} =$$

$$(-1)^{n-n-i+1+1} \cdot e_{n-n+i-1+1, n-n+i+1} = (-1)^2 \cdot e_{i, i+1} = 1 \cdot e_{i, i+1}$$

Hence,  $e_{i,i+1} \leftrightarrow e_{n-i,n-i+1}$ , so  $\eta$  is an automorphism.  
 $\eta$  acts on the base elements as the permutation  
 $(e_{1,2} \ e_{n-1,n}) \cdot (e_{2,3} \ e_{n-2,n-1}) \cdots (e_{i,i+1} \ e_{n-i,n-i+1}) \cdots$

**Exercise** Let  $\phi \in \text{Aut}(L_n)$ , and let  $e_{l,l+1} \in L_n$ , then,

$$\phi(e_{k,k+1}) \in C_{L_n}(\phi(e_{l,l+1})) \Leftrightarrow 1 \leq i \leq n-1, a_{i+1,i+2}^{k,k+1} = a_{i,i+1}^{k,k+1} \cdot \frac{a_{i+1,i+2}^{l,l+1}}{a_{i,i+1}^{l,l+1}},$$

Where,

$$m \in \{l, k\}, \phi(e_{m,m+1}) = \sum_{i=1}^{n-1} a_{i,i+1}^{m,m+1} \cdot e_{i,i+1}$$

**Proof**

$$\begin{aligned} \phi(e_{k,k+1}) \in C_{L_n}(\phi(e_{l,l+1})) \text{ means that } [\phi(e_{l,l+1}), \phi(e_{k,k+1})] &= [\phi(e_{k,k+1}), \phi(e_{l,l+1})] = \\ [\sum_{i=1}^{n-1} a_{i,i+1}^{k,k+1} \cdot e_{i,i+1}, \sum_{j=1}^{n-1} a_{j,j+1}^{l,l+1} \cdot e_{j,j+1}] &= 0 \\ \text{Lie brackets operation is bilinear, so,} \\ [\phi(e_{k,k+1}), \phi(e_{l,l+1})] &= \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_{i,i+1}^{k,k+1} \cdot a_{j,j+1}^{l,l+1} \cdot [e_{i,i+1}, e_{j,j+1}] = 0 \end{aligned}$$

For the following exercise, we shall use the annotation,

$\phi_k(e_{i,j}) := \sum_l a_{l,l+k}^{i,j} \cdot e_{l,l+k}$ , that is, a sum of all the expressions of the form  $a_{l,m} \cdot e_{l,m}$ , where  $m - l = k$  (hence, a partial sum to  $\phi(e_{i,j})$  itself).

**Exercise**

Let  $L_n$  be a Lie algebra

$$\begin{aligned} [\phi_1(e_{1,2}), \phi_1(e_{2,3})] &= \phi_1(e_{1,3}) = [\sum_{i=1}^{n-1} a_{i,i+1}^{1,2} \cdot e_{i,i+1}, \sum_{i=1}^{n-1} a_{i,i+1}^{2,3} \cdot e_{i,i+1}] = \\ \sum_{i=1}^{n-2} (a_{i,i+1}^{1,2} \cdot a_{i+1,i+2}^{2,3} - a_{i+1,i+2}^{1,2} \cdot a_{i,i+1}^{2,3}) \cdot [e_{i,i+1}, e_{i+1,i+2}] &= 0 \\ \text{So, if } [\phi_1(e_{1,2}), \phi_1(e_{2,3})] &= 0, \text{ it means that all the expressions of the form } \\ (a_{i,i+1}^{1,2} \cdot a_{i+1,i+2}^{2,3} - a_{i+1,i+2}^{1,2} \cdot a_{i,i+1}^{2,3}) &\text{ must be 0 (because the } [e_{i,i+1}, e_{i+1,i+2}] = e_{i,i+2} \\ \text{are linearly independent).} \\ a_{i,i+1}^{1,2} \cdot a_{i+1,i+2}^{2,3} - a_{i+1,i+2}^{1,2} \cdot a_{i,i+1}^{2,3} &= 0 \Rightarrow a_{i,i+1}^{1,2} \cdot a_{i+1,i+2}^{2,3} = a_{i+1,i+2}^{1,2} \cdot a_{i,i+1}^{2,3} \Rightarrow \\ a_{i+1,i+2}^{2,3} &= a_{i,i+1}^{2,3} \cdot \frac{a_{i+1,i+2}^{1,2}}{a_{i,i+1}^{1,2}}, \text{ if } a_{i,i+1}^{1,2} \neq 0 \end{aligned}$$

If  $a_{i,i+1}^{1,2} = 0$ , we have a few cases,

1. If  $a_{i+1,i+2}^{1,2} = 0$ , then both  $a_{i,i+1}^{2,3}$  and  $a_{i+1,i+2}^{2,3}$  can be any integers.
2. If  $a_{i+1,i+2}^{1,2} \neq 0$ , then  $a_{i,i+1}^{2,3}$  must be 0

We can sum up all the above, and say that when given

$$\phi_1(e_{1,2}) = \sum_{i=1}^{n-1} a_{i,i+1}^{1,2} \cdot e_{i,i+1}, \text{ we have,}$$

If  $a_{i,i+1}^{1,2} \neq 0, 1 \leq i \leq n-1$ , then the number of free coefficients in an element of the centralizer of  $\phi_1(e_{1,2})$  is 1

**Proof**

Assume we choose  $a_{k,k+1}^{2,3}$  to be any integer, then, according to the above,

$$a_{k+1,k+2}^{2,3} = a_{k,k+1}^{2,3} \cdot \frac{a_{k+1,k+2}^{1,2}}{a_{k,k+1}^{1,2}}, \text{ since } a_{l,l+1}^{1,2} \neq 0, 1 \leq l \leq n-1, \text{ so it is easy to}$$

observe that this determines all the  $a_{k+l,k+l+1}^{2,3}, 1 \leq l \leq n-k-1$   
Precisely in the same way (but running backward),  
since  $a_{k,k+1}^{2,3} = a_{k-1,k}^{2,3} \cdot \frac{a_{k,k+1}^{1,2}}{a_{k-1,k}^{1,2}} \Rightarrow a_{k-1,k}^{2,3} = a_{k,k+1}^{2,3} \cdot \frac{a_{k-1,k}^{1,2}}{a_{k,k+1}^{1,2}}$ , it is easy to observe  
that the choice of  $a_{k,k+1}^{2,3}$  determines also  $a_{l,l+1}^{2,3}$ , for all  $1 \leq l \leq k-1$   
(or  $a_{k-l,k-l+1}^{2,3}, 1 \leq l \leq k-1$ )

Now, assume that we do not have all  $a_{l,l+1}^{1,2} \neq 0$ ,  
Take  $a_{k,k+1}^{1,2} = 0$ , then, obviously  $a_{k,k+1}^{1,2} \cdot a_{k+1,k+2}^{2,3} = 0$ ,  
so, in order for the expression  $a_{k,k+1}^{1,2} \cdot a_{k+1,k+2}^{2,3} - a_{k+1,k+2}^{1,2} \cdot a_{k,k+1}^{2,3}$  to be 0, we  
must have either  $a_{k+1,k+2}^{1,2} = 0$  or  $a_{k,k+1}^{2,3} = 0$   
Assume we have  $a_{k+1,k+2}^{1,2} = 0$ , so,  $a_{k,k+1}^{2,3}$  can be a free choice of an integer.  
So, for the chain of  $a_{k+l,k+l+1}^{1,2} = 0, 1 \leq l \leq m < n-1$ , we can have all  
 $a_{k+l,k+l+1}^{2,3}, 1 \leq l < m$  as free integers. Since  $a_{m+1,m+2}^{1,2} \neq 0$ ,  
and  $a_{m,m+1}^{1,2} = 0 \Rightarrow a_{m,m+1}^{1,2} \cdot a_{m+1,m+2}^{2,3} = 0$ , then we must have  $a_{m,m+1}^{2,3} = 0$ ,  
so, a consecutive chain of  $m$  zero coefficients of  $\phi_1(e_{1,2})$  will allow  $m-1$  free  
choices of integers for all the coefficients of  $\phi_1(e_{2,3})$ , with the same indices,  
except for the last coefficient in the chain.  
However, we observe that if  $m \leq n-1$ , that is, the chain of zeros continues  
until the last coefficient of  $\phi_1(e_{1,2})$  (meaning,  $a_{n-1,n}^{1,2}$  is also 0), then  $a_{n-1,n}^{2,3}$  is,  
obviously, also a free choice of an integer. To make a unification of the cases,  
we can think of  $\phi_1(e_{1,2})$  as  $\sum_{i=1}^n a_{i,i+1}^{1,2} \cdot e_{i,i+1}$ , where  $a_{n,n+1} = 0$ , but this is  
only semantics.  
So, in this case, where the chains of  $m$  zeros continues to the end, we have  
 $m$  free choices of integers, for the coefficients  $a_{l,l+1}^{2,3}, k \leq l \leq m = n-1$ ,  
of  $\phi_1(e_{2,3})$