Problema 3. Considerem

$$\begin{array}{lll} \mathrm{GL}(n,\mathbb{Z}) & := \{M \in \mathrm{M}_{n\times n}(\mathbb{Z}) : \det(M) \in \mathbb{Z}^*\}, & \text{grup lineal,} \\ \mathrm{SL}(n,\mathbb{Z}) & := \{M \in \mathrm{GL}(n,\mathbb{Z}) : \det(M) = 1\}, & \text{grup especial lineal,} \\ \mathrm{O}(n,\mathbb{Z}) & := \{M \in \mathrm{GL}(n,\mathbb{Z}) : M^t M = Id\}, & \text{grup ortogonal,} \\ \mathrm{SO}(n,\mathbb{Z}) & := \{M \in \mathrm{O}(n,\mathbb{Z}) : \det(M) = 1\}, & \text{grup especial ortogonal.} \end{array}$$

(a) Demostreu que $\mathrm{GL}(n,\mathbb{Z})$ és un grup amb la multiplicació de matrius.

(b) Demostreu que $\mathrm{SL}(n,\mathbb{Z})$ i $\mathrm{O}(n,\mathbb{Z})$ són subgrups del grup $\mathrm{GL}(n,\mathbb{Z})$.

(c) Demostreu que $\mathrm{SO}(n,\mathbb{Z})$ és un subgrup de $\mathrm{O}(n,\mathbb{Z})$.

Solució. (a) Per demostrar que $\mathrm{GL}(n,\mathbb{Z})$ és un grup amb la multiplicació de matrius, hem de veure que:

1. La multiplicació de matrius està **ben definida** i és **interna**:

   (a) El producte de matrius quadrades $n \times n$ té sentit fer-lo per a tots els elements del conjunt; per tant, està ben definit.

   (b) Si agafem dues matrius $A, B \in \mathrm{GL}(n,\mathbb{Z})$, per a realitzar el producte AB només cal utilitzar sumes i productes, i si $det(A), det(B) \in \{-1, 1\}$ tindrem que $det(AB) = det(A)det(B) \in \{-1, 1\}$. Per tant, $AB \in \mathrm{GL}(n,\mathbb{Z})$.

2. És clar que es compleix la **propietat associativa**, ja que el producte de matrius és associatiu.

3. Existeix **element neutre**. Veiem clarament que la matriu identitat és l'element neutre del producte de matrius, ja que els seus components són enters i $det(Id_n) = 1 \in \mathbb{Z}^*$; per tant, $Id_n \in \mathrm{GL}(n,\mathbb{Z})$.

4. Tot element del grup té **invers**. Sabem clarament que per a tota matriu del conjunt, existeix la seva matriu inversa. Si $A \in \mathrm{GL}(n,\mathbb{Z}) \Rightarrow \det(A) \neq 0$ volem veure que existirà $B \in \mathrm{GL}(n,\mathbb{Z}) \Rightarrow \det(B) \neq 0$ tal que $AB = Id_n$ i $BA = Id_n$. Tenim que el $\det(A)\det(\mathrm{B}) = \det(Id_n) \Rightarrow \det(B) = \frac{det(Id_n)}{det(A)}$, com $\det(A) \neq 0$, aleshores existira el determinan de B que també serà diferent de 0, ja que $dey(Id_n) \neq 0$, per tan $B \in \mathrm{GL}(n,\mathbb{Z})$.

(b) Perquè $\mathrm{SL}(n,\mathbb{Z})$ sigui subgrup de $\mathrm{GL}(n,\mathbb{Z})$, per definició $\mathrm{SL}(n,\mathbb{Z}) \subset \mathrm{GL}(n,\mathbb{Z})$ i $\mathrm{SL}(n,\mathbb{Z}) \neq \emptyset$. També cal comprovar que $\mathrm{SL}(n,\mathbb{Z})$ és tancat per l'operació de $\mathrm{GL}(n,\mathbb{Z})$, així $\mathrm{SL}(n,\mathbb{Z})$ amb l'operació restringida de $\mathrm{GL}(n,\mathbb{Z})$ és un grup.

$\forall A, B \in \mathrm{SL}(n,\mathbb{Z})$, $AB \in \mathrm{SL}(n,\mathbb{Z})$; per l'apartat anterior, és té que $A, B \in \mathrm{GL}(n,\mathbb{Z})$, $AB \in \mathrm{GL}(n,\mathbb{Z})$ i, per les propietats dels determinants, $det(AB) = det(A)det(B) = 1 \cdot 1 = 1$.

Per demostrar que $\mathrm{O}(n,\mathbb{Z})$ és subgrup de $\mathrm{GL}(n,\mathbb{Z})$, s'actua de manera similar. Per definició $\mathrm{O}(n,\mathbb{Z}) \subset \mathrm{GL}(n,\mathbb{Z})$, i $\mathrm{O}(n,\mathbb{Z}) \neq \emptyset$. Ara cal comprovar que $\forall A, B \in \mathrm{O}(n,\mathbb{Z})$, $AB^{-1} \in \mathrm{O}(n,\mathbb{Z})$:

Hem de veure si $(AB^{-1})^t AB^{-1} = Id$, $(AB^{-1})^t AB^{-1} = (B^{-1})^t A^t AB^{-1} = (B^{-1})^t IdB^{-1} = (B^{-1})^t B^{-1} = Id$.

(c) Veiem clarament que $\mathrm{SO}(n,\mathbb{Z}) \subset \mathrm{O}(n,\mathbb{Z})$ i $\mathrm{SO}(n,\mathbb{Z}) \neq \emptyset$. $\forall A, B \in \mathrm{SO}(n,\mathbb{Z})$, aleshores hem de veure si $AB^{-1} \in \mathrm{SO}(n,\mathbb{Z})$:

$\det(AB^{-1})=\det(A)\det(B^{-1})=\det(A)\det(B)^{-1}=\det(A)\frac{1}{det(B)} = 1$, ja que $\det(A)=\det(B)=1$. Per tan $AB^{-1} \in \mathrm{SO}(n,\mathbb{Z})$.

Si $A, B \in \mathrm{SO}(n,\mathbb{Z}) \Rightarrow A, B \in \mathrm{O}(n,\mathbb{Z}) \Rightarrow AB^{-1} \in \mathrm{O}(n,\mathbb{Z}) \Rightarrow AB^{-1}$ és ortogonal i $(AB^{-1})^t AB^{-1} = Id_n$. $\mathrm{SO}(n,\mathbb{Z})$ és un subgrup de $\mathrm{O}(n,\mathbb{Z})$.