Moshe Mason Rubin

MATH 330 Homework #3

19 September 2016

**Exercise 3.8.** Give an example of two elements $A$ and $B$ in $GL_2(\mathbb{R})$ with $AB \neq BA$.

*Solution.* Let $A = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right]$. Then $A, B \in GL_2(\mathbb{R})$ as $A^{-1}$ and $B^{-1}$ are given by $A^{-1} = \left[\begin{smallmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{smallmatrix}\right]$ and $B^{-1} = \left[\begin{smallmatrix} -4 & 3 \\ \frac{7}{2} & -\frac{5}{2} \end{smallmatrix}\right]$. However,

$$AB = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix} \neq \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix} = BA$$

So $BA \neq AB$ for $A = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right]$. □

**Exercise 3.12.** Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)\,.$$

Prove that $\mathbb{Z}_2^n$ is a group under this operation.

*Proof:*

**Associative** Let $a, b, c \in \mathbb{Z}_2^n$ such that $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n)$, and $c = (c_1, c_2, \ldots, c_n)$. Then

$$\begin{aligned}
(a+b)+c &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) + c \quad \text{by definition of } a+b \\
&= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2, \ldots, (a_n + b_n) + c_n) \quad \text{by definition of a+b} \\
&= (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), \ldots, a_n + (b_n + c_n)) \quad \text{by associativity of real addition} \\
&= a + (b_1 + c_1, b_2 + c_2, \ldots, b_n + c_n) \quad \text{by definition of } a+b \\
&= a + (b + c) \quad \text{by definition of } a+b
\end{aligned}$$

So $+$ is associative in $\mathbb{Z}_2^n$.

**Identity** For $a \in \mathbb{Z}_2^n$ let $b$ be given by $b = (0, 0, \ldots, 0)$. Then $b \in \mathbb{Z}_2^n$ as $0 \in \mathbb{Z}_2$. Then

$$\begin{aligned}
a + b &= (a_1 + 0, a_2 + 0, \ldots, a_n + 0) \quad \text{by definition of } a+b \\
&= (a_1, a_2, \ldots, a_n) \quad \text{as 0 is the additive identity in } \mathbb{Z}_2^n \\
&= a \quad \text{by definition of } a \qquad (1) \\
&= (0 + a_1, 0 + a_2, \ldots, 0 + a_n) \quad \text{as 0 is the additive identity in } \mathbb{Z}_2^n \\
&= b + a \quad \text{by definition of } a+b \qquad (2)
\end{aligned}$$

So (1) and (2) imply that $a + b = a = b + a$ for $b \in \mathbb{Z}_2^n$ given by $b = (0, 0, \ldots, 0)$. So there exists an identity in $\mathbb{Z}_2^n$ under $+$.

**Inverse** For $a \in \mathbb{Z}_2^n$ let $b = a$. Then

$$\begin{aligned}
a + b &= ([a_1 + b_1]_2, [a_2 + b_2]_2, \ldots, [a_n + b_n]_2) \quad \text{by definition of } a+b \\
&= ([2a_1]_2, [2a_2]_2, \ldots, [2a_n]_2) \quad \text{as } a_i = b_i \text{ for } i \in (\mathbb{Z} \cap [1, n]) \\
&= (0, 0, \ldots, 0) \quad \text{as } [2k]_2 = 0 \text{ for all } k \in \mathbb{Z}. \text{ Notice } (0, 0, \ldots, 0) \text{ is the additive inverse from above.} \qquad (3) \\
&= ([2a_1]_2, [2a_2]_2, \ldots, [2a_n]_2) = ([b_1 + a_1]_2, [b_2 + a_2]_2, \ldots [b_n + a_n]_2) \quad \text{as } a_i = b_i \text{ for } i \in (\mathbb{Z} \cap [1, n]) \\
&= b + a \quad \text{by definition of } a+b \qquad (4)
\end{aligned}$$

So (3) and (4) imply that for all $a \in \mathbb{Z}_2^n$, $a$ is its own inverse element under $+$.

So $(\mathbb{Z}_2^n, +)$ is a group. □

**Exercise 3.15.** Prove or disprove that every group containing six elements is abelian.

*Counterexample.* Consider the group $D_3 = \{id, \rho, \rho^2, \tau_A, \tau_B, \tau_C\}$ which contains exactly 6 elements with $id = \left(\begin{smallmatrix} a & b & c \\ a & b & c \end{smallmatrix}\right)$, $\rho = \left(\begin{smallmatrix} a & b & c \\ b & c & a \end{smallmatrix}\right)$, $\rho^2 = \left(\begin{smallmatrix} a & b & c \\ c & a & b \end{smallmatrix}\right)$, $\tau_A = \left(\begin{smallmatrix} a & b & c \\ a & c & b \end{smallmatrix}\right)$, $\tau_B = \left(\begin{smallmatrix} a & b & c \\ c & b & a \end{smallmatrix}\right)$, and $\tau_C = \left(\begin{smallmatrix} a & b & c \\ b & a & c \end{smallmatrix}\right)$. $D_3$ is *not* abelian. For example,

$$\begin{aligned}\tau_A\tau_B &= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \rho\end{aligned}$$

but

$$\begin{aligned}\tau_B\tau_A &= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \rho^2\end{aligned}$$

So $D_3$ is an example of a group containing 6 elements that is not abelian. □

**Exercise 3.26.** Prove that the inverse of $g_1g_2\cdots g_n$ is $g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}$.

*Proof.* **Base case $\mathbf{n = 2}$** If $n = 2$ then $g_2^{-1}g_1^{-1}$ is the inverse of $g_1g_2$ as

$$\begin{aligned}(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) &= g_1\left(g_2g_2^{-1}\right)g_1^{-1} \quad \text{by associativity} \\ &= g_1(e)g_1^{-1} \quad \text{by definition of } g_2^{-1} \\ &= g_1g_1^{-1} \quad \text{by definition of } e \\ &= e \quad \text{by definition of } g_1^{-1} \qquad (5) \\ &= g_2^{-1}g_2 \quad \text{by definition of } g_2^{-1} \\ &= g_2^{-1}(e)g_2 \quad \text{by definition of } e \\ &= g_2^{-1}\left(g_1^{-1}g_1\right)g_2 \quad \text{by definition of } g_1^{-1} \\ &= \left(g_2^{-1}g_1^{-1}\right)(g_1g_2) \qquad (6)\end{aligned}$$

So (5) and (6) imply that $\left(g_2^{-1}g_1^{-1}\right)$ is unique inverse element such that $(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) = e = \left(g_2^{-1}g_1^{-1}\right)(g_1g_2)$.

**Assume $(\mathbf{g_1g_2\cdots g_n})^{-1} = \mathbf{g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}}$ for some $\mathbf{n} \in \mathbb{N}$ and show that $(\mathbf{g_1g_2\cdots g_ng_{n+1}})^{-1} = \mathbf{g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}}$:**

Consider

$$\begin{aligned}(g_1g_2\cdots g_{n-1}g_ng_{n+1})\left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) &= (g_1g_2\cdots g_{n-1}g_n)\left(g_{n+1}g_{n+1}^{-1}\right)\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) \quad \text{by associativity} \\ &= (g_1g_2\cdots g_{n-1}g_n)(e)\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) \quad \text{by definition of } g_{n+1}^{-1} \\ &= (g_1g_2\cdots g_{n-1}g_n)\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) \quad \text{by definition of } e \\ (g_1g_2\cdots g_{n-1}g_ng_{n+1})\left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) &= e \quad \text{by inductive hypothesis} \qquad (7) \\ &= g_{n+1}^{-1}g_{n+1} \quad \text{by definition of } g_{n+1}^{-1} \\ &= \left(g_{n+1}^{-1}\right)(e)(g_{n+1}) \quad \text{by definition of } e \\ &= \left(g_{n+1}^{-1}\right)\left(\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right)(g_1g_2\cdots g_{n-1}g_n)\right)(g_{n+1}) \\ &\quad \text{by inductive hypothesis} \\ (g_1g_2\cdots g_{n-1}g_ng_{n+1})\left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) &= \left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right)(g_1g_2\cdots g_{n-1}g_ng_{n+1}) \quad \text{by associativity} \qquad (8)\end{aligned}$$

So by **Base case**, (7), and (8), $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$ and $(g_1g_2\cdots g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1} \implies (g_1g_2\cdots g_ng_{n+1})^{-1} = g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}$.

So the inverse of $g_1g_2\cdots g_n$ is $g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}$ for all $n \in \mathbb{N}$. □

**Exercise 3.30.** Show that if $a^2 = e$ for all elements $a$ in a group $G$, then $G$ must be abelian.

*Proof.* Let $a, b \in G$. Then $(a \circ b) \in G$ by the assumption that $G$ is a group. Then $a, b, (a \circ b) \in G \implies a^2 = b^2 = (a \circ b)^2 = e$ by the assumption that $a^2 = e$ for all elements $a$ in $G$. Then

$$
\begin{aligned}
(a \circ b)^2 = e &\implies (a \circ b) \circ (a \circ b) = e \quad \text{by definition of exponentiation} \\
&\implies (b \circ a) \circ [(a \circ b) \circ (a \circ b)] = (b \circ a) \circ e \quad \text{by Proposition 3.2 (that } e \text{ is unique) and definition of } e, \text{ as } (b \circ a) \in G \\
&\implies [(b \circ a) \circ (a \circ b)] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by associativity of elements of } G \\
&\implies [((b \circ a) \circ a) \circ b] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by associativity of elements of } G \\
&\implies [(b \circ (a \circ a)) \circ b] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by associativity of elements of } G \\
&\implies [(b \circ e) \circ b] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by assumption that } a \circ a = e \text{ for all } a \in G \\
&\implies [b \circ b] \circ (a \circ b) = b \circ a \quad \text{by definition of } e \\
&\implies e \circ (a \circ b) = b \circ a \quad \text{by assumption that } a \circ a = e \text{ for all } a \in G \\
&\implies a \circ b = b \circ a \quad \text{by definition of } e
\end{aligned}
$$

So for any $a, b \in G$, the definition of $G$ implies that $(a \circ b)^2 \in G$. So $(a \circ b)^2 = e$ because $(a \circ b)^2 \in G$. We have shown that $(a \circ b)^2 = e \implies a \circ b = b \circ a$ for all $a, b \in G$. So if $a^2 = e$ for all elements $a \in G$ then $G$ must be abelian. □

**Exercise 3.35.** Compute the subgroups of the symmetry of a square.

*Proof.* The symmetries of a square are given by $\rho = \left(\begin{smallmatrix} a & b & c & d \\ b & c & d & a \end{smallmatrix}\right)$, $\rho^2 = \left(\begin{smallmatrix} a & b & c & d \\ c & d & a & b \end{smallmatrix}\right)$, $\rho^3 = \left(\begin{smallmatrix} a & b & c & d \\ d & a & b & c \end{smallmatrix}\right)$, $\rho^4 = id = \left(\begin{smallmatrix} a & b & c & d \\ a & b & c & d \end{smallmatrix}\right)$, $\mu_{x=0} = \left(\begin{smallmatrix} a & b & c & d \\ d & c & b & a \end{smallmatrix}\right)$, $\mu_{y=0} = \left(\begin{smallmatrix} a & b & c & d \\ b & a & d & c \end{smallmatrix}\right)$, $\mu_{y=x} = \left(\begin{smallmatrix} a & b & c & d \\ c & b & a & d \end{smallmatrix}\right)$, and $\mu_{y=-x} = \left(\begin{smallmatrix} a & b & c & d \\ a & d & c & b \end{smallmatrix}\right)$. Then the sub-groups are the trivial sub-groups:

$$\langle id \rangle = \{id\} \tag{9}$$

and

$$\langle D_8 \rangle = \left\{\rho, \rho^2, \rho^3, \mu_{x=0}, \mu_{y=0}, \mu_{y=x}, \mu_{y=-x}, id\right\} \tag{10}$$

and the proper non-trivial sub-groups:

$$\langle \rho \rangle = \left\langle \rho^3 \right\rangle = \left\{\rho, \rho^2\rho^3, id\right\} \tag{11}$$
$$\left\langle \rho^2 \right\rangle = \left\{\rho^2, id\right\} \tag{12}$$
$$\langle \mu_{x=0} \rangle = \{\mu_{x=0}, id\} \tag{13}$$
$$\langle \mu_{y=0} \rangle = \{\mu_{y=0}, id\} \tag{14}$$
$$\langle \mu_{y=x} \rangle = \{\mu_{y=x}, id\} \tag{15}$$

and

$$\langle \mu_{y=-x} \rangle = \{\mu_{y=-x}, id\}. \tag{16}$$

Furthermore,

$$\left\langle \rho^2 \right\rangle \cup \langle \mu_{x=0} \rangle \cup \langle \mu_{y=0} \rangle = \left\{\rho^2, \mu_{x=0}, \mu_{y=0}\right\} \tag{17}$$

and

$$\left\langle \rho^2 \right\rangle \cup \langle \mu_{y=x} \rangle \cup \langle \mu_{y=-x} \rangle = \left\{\rho^2, \mu_{y=x}, \mu_{y=-x}\right\} \tag{18}$$

are proper sub-groups as $id \in$ (17) and $id \in$ (18), any element in (17) and (18) is its own inverse, and (17) and (18) are closed under composition as can be seen in the Cayley table below.

Besides by theorem from class that $g \in D_8$ implies that $\langle g \rangle := \{g^n | n \in \mathbb{N}\}$ is a subgroup of $D_8$ it is clear from the Cayley table that each of these forms a sub-group of $D_8$, including (17) and (18):

| $\circ$ | $id$ | $\rho$ | $\rho^2$ | $\rho^3$ | $\mu_{x=0}$ | $\mu_{y=0}$ | $\mu_{y=x}$ | $\mu_{y=-x}$ |
|---|---|---|---|---|---|---|---|---|
| $id$ | $id$ | $\rho$ | $\rho^2$ | $\rho^3$ | $\mu_{x=0}$ | $\mu_{y=0}$ | $\mu_{y=x}$ | $\mu_{y=-x}$ |
| $\rho$ | $\rho$ | $\rho^2$ | $\rho^3$ | $id$ | $\mu_{y=x}$ | $\mu_{y=-x}$ | $\mu_{y=0}$ | $\mu_{x=0}$ |
| $\rho^2$ | $\rho^2$ | $\rho^3$ | $id$ | $\rho$ | $\mu_{y=0}$ | $\mu_{x=0}$ | $\mu_{y=-x}$ | $\mu_{y=x}$ |
| $\rho^3$ | $\rho^3$ | $id$ | $\rho$ | $\rho^2$ | $\mu_{y=-x}$ | $\mu_{y=x}$ | $\mu_{x=0}$ | $\mu_{y=0}$ |
| $\mu_{x=0}$ | $\mu_{x=0}$ | $\mu_{y=-x}$ | $\mu_{y=0}$ | $\mu_{y=x}$ | $id$ | $\rho^2$ | $\rho^3$ | $\rho$ |
| $\mu_{y=0}$ | $\mu_{y=0}$ | $\mu_{y=x}$ | $\mu_{y=0}$ | $\mu_{y=-x}$ | $\rho^2$ | $id$ | $\rho$ | $\rho^3$ |
| $\mu_{y=x}$ | $\mu_{y=x}$ | $\mu_{x=0}$ | $\mu_{y=-x}$ | $\mu_{y=0}$ | $\rho$ | $\rho^3$ | $id$ | $\rho^2$ |
| $\mu_{y=-x}$ | $\mu_{y=-x}$ | $\mu_{y=0}$ | $\mu_{y=x}$ | $\mu_{x=0}$ | $\rho^3$ | $\rho$ | $\rho^2$ | $id$ |

□

**Exercise 3.40.** Prove that

$$G = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are both not } 0 \right\}$$

is a sub-group of $\mathbb{R}^*$ under the group operation of multiplication.

*Proof.* By theorem from class, for $G \subseteq \mathbb{R}^*$ to be a sub-group of $\mathbb{R}^*$, it is sufficient to show

1. For all $h_1, h_2 \in G$, $h_1 \cdot h_2 \in G$.
2. There exists $e \in G$ such that $h_1 \cdot e = h_1 = e \cdot h_1$ for all $h_1 \in G$.
3. For all $h_1 \in G$ there exists $h_1^{-1} \in G$ such that $h_1 \cdot h_1^{-1} = e = h_1^{-1} \cdot h_1$.

1. To show $G$ is closed, take $h_1, h_2 \in G$. Clearly $h_1 \neq 0$ and $h_2 \neq 0$ so $h_1 \cdot h_2 \neq 0$. So

$$\begin{aligned} h_1 \cdot h_2 &= \left(a_1 + b_1\sqrt{2}\right) \cdot \left(a_2 + b_2\sqrt{2}\right) \\ &= a_1a_2 + a_1b_2\sqrt{2} + b_1a_2\sqrt{2} + 2b_1b_2 \quad \text{by the distributive property} \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \quad \text{by distributive, associative laws} \end{aligned}$$

   and $\left[(a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}\right] \in G$.

2. To show the multiplicative identity is in $G$, take $a = 1$ and $b = 0$. Then $1 + 0\sqrt{2} \in G$ and $1 + 0\sqrt{2} = 1$ and 1 is the multiplicative identity in $\mathbb{R}^*$.

3. To show that each element in $G$ has an inverse, given $h_1 = a + b\sqrt{2}$ its inverse is given by $h_1^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ as

$$\begin{aligned}
&h_1 \cdot h_1^{-1} = h_1^{-1} \cdot h_1 \quad \text{because multiplication is commutative in } \mathbb{R}^* \\
&h_1^{-1} \cdot h_1 = \left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right)\left(a + b\sqrt{2}\right) \\
&= \left(\frac{a - b\sqrt{2}}{a^2-2b^2}\right)\left(a + b\sqrt{2}\right) \\
&= \frac{a^2 - ab\sqrt{2}}{a^2-2b^2} + \frac{ab\sqrt{2} - 2b^2}{a^2-2b^2} \quad \text{by distributive law} \\
&= \frac{a^2-2b^2}{a^2-2b^2} \\
&= 1
\end{aligned}$$

and 1 is the multiplicative identity. Notice that the inverse is well defined: $h_1^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \neq 0$ as not both $a$ and $b$ are zero. Furthermore, the denominator is not zero as $a^2 - 2b^2 = 0 \implies a = b\sqrt{2}$ which violates the assumption that $a, b \in \mathbb{Q}$. So $\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right) \in G$ exists and is well defined.

So we have shown that $G$ is a sub-group of $\mathbb{R}^*$ under multiplication. □

**Exercise 3.43.** List the sub-groups of the quaternion group, $Q_8$.

*Proof.* By definition, $Q_8 := \{\pm 1, \pm I, \pm J, \pm K\}$ such that $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$ and $IK = -J$. Then the sub-groups of $Q_8$ are $\langle 1\rangle = \{1\}$, $\langle -1\rangle = \{-1, 1\}$, $\langle I\rangle = \{I, -1, -I, 1\}$, $\langle J\rangle = \{J, -1, -J, 1\}$, $\langle K\rangle = \{K, -1, -K, 1\}$, and $\langle Q_8\rangle = \{\pm 1, \pm I, \pm J, \pm K\}$ □

**Exercise 3.44.** Prove that the intersection of two sub-groups of a group $G$ is also a sub-group of $G$.

*Proof.* Let $H_1, H_2 \in G$ be sub-groups of $G$. Consider $H_1 \cap H_2 = \Gamma$.
By theorem from class, for $\Gamma \subseteq G$ to be a sub-group of $G$, it is sufficient to show

1. For all $g_1, g_2 \in \Gamma$, $g_1 \circ g_2 \in \Gamma$.
2. There exists $e \in \Gamma$ such that $g_1 \circ e = g_1 = e \circ g_1$ for all $g_1 \in \Gamma$.
3. For all $g_1 \in \Gamma$ there exists $g_1^{-1} \in G$ such that $g_1 \circ g_1^{-1} = e = g_1^{-1} \circ g_1$.

1. Let $g_1, g_2 \in \Gamma$. Then $g_1, g_2 \in H_1$ and $g_1, g_2 \in H_2$ as $\Gamma = H_1 \cap H_2$. Then $g_1 \circ g_2 \in H_1$ and $g_1 \circ g_2 \in H_2$ by the assumption that $H_1$ and $H_2$ are sub-groups of $G$.
   $g_1 \circ g_2 \in H_1$ and $g_1 \circ g_2 \in H_2 \implies g_1 \circ g_2 \in \Gamma$ by definition of $\Gamma$. So $g_1, g_2 \in \Gamma \implies g_1 \circ g_2 \in \Gamma$. So $\Gamma$ is closed under $\circ$.
2. $e \in H_1$ and $e \in H_2$ by the assumption that $H_1$ and $H_2$ are sub-groups. Then $e \in \Gamma$ by definition of $\Gamma$. So $e \in \Gamma$. This also proves that $\Gamma \neq \emptyset$.
3. Let $g_1 \in \Gamma$. Then $g_1 \in H_1$ and $g_1 \in H_2$ by definition of $\Gamma$. Then $g_1^{-1} \in H_1$ and $g_1^{-1} \in H_2$ by assumption that $H_1$ and $H_2$ are sub-groups of $G$. So $g_1^{-1} \in H_1$ and $g_1^{-1} \in H_2 \implies g_1^{-1} \in \Gamma$. So $g_1 \in \Gamma \implies g_1^{-1} \in \Gamma$.

So we have shown that $\Gamma$ is a sub-group of $G$ under $\circ$. □