Exam 1 Key:

1) Show $S = \{1, 2, \dots, p-1\}$ where p is a prime is a group under multiplication mod p.

closed: If $ab \equiv 0 \bmod p$ then $p \mid a$ or $p \mid b$. As p does not divide any element of S, this set is closed under multiplication modulo p.

associative: multiplication is associative

identity: $1 \in S$ is the identity

inverses: for $a \in S$, $\exists s, t \in \mathbb{Z}$ such that $as + pt = 1$. Thus $a^{-1} \equiv s \bmod p$.

2) The order of an element a in a group G is the least $n \in \mathbb{N}$ such that $a^n = e$. If no such n exists, we say a has infinite order.

The order of $8 \in U(13)$ is 4 as:

$$8^1 = 8 \bmod 13$$
$$8^2 \equiv 64 \equiv 12 \equiv -1 \bmod 13$$
$$8^3 \equiv 8^1 \cdot 8^2 \equiv 8 \cdot -1 \equiv -8 \equiv 5 \bmod 13$$
$$8^4 \equiv 8^2 \cdot 8^2 \equiv (-1)(-1) \equiv 1 \bmod 13$$

3) We have $\begin{bmatrix} 3 & 2 \\ 2 & 4 \end{bmatrix} \in GL(2, \mathbb{Z}_{13})$ as $3 \cdot 4 - 2 \cdot 2 = 8 \not\equiv 0 \bmod 13$

$$\begin{bmatrix} 3 & 2 \\ 2 & 4 \end{bmatrix} = 8^{-1} \begin{bmatrix} 4 & -2 \\ -2 & 3 \end{bmatrix} = 5 \begin{bmatrix} 4 & 11 \\ 11 & 3 \end{bmatrix} = \begin{bmatrix} 20 & 55 \\ 55 & 15 \end{bmatrix}$$

note: As $8^4 \equiv 1$, we have $8^3 \equiv 8^{-1}$

$$= \begin{bmatrix} 7 & 3 \\ 3 & 2 \end{bmatrix}$$

④ Suppose G is a group for which $aba^{-1}b^{-1} = e$ $\forall a, b \in G$. Prove G is abelian.

Proof:
Let $a, b \in G$. Then $ba = eba$

$= (aba^{-1}b^{-1})ba$

$= aba^{-1}a$

$= ab.$ ∎

⑤ Suppose G is an abelian group and that H & K are subgroups. Show

$HK = \{hk \mid h \in H, k \in K\}$

is a subgroup of G.

Proof: As H & K are subgroup, they both contain the identity. Thus HK also contains the identity so $HK \neq \emptyset$. Let $a, b \in HK$. Thus $\exists\, h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$. Then $b^{-1} = (h_2k_2)^{-1} = k_2^{-1}h_2^{-1} = h_2^{-1}k_2^{-1}$ as G is abelian. Then:

$ab^{-1} = h_1k_1h_2^{-1}k_2^{-1}$

$= h_1h_2^{-1}k_1k_2^{-1}$ (as G is abelian again).

As H is a subgroup, $h_1h_2^{-1} \in H$ and likewise $k_1k_2^{-1} \in K$. Thus $ab^{-1} \in HK$ and so HK is a subgroup ∎