1. Let G and H be groups.

   (a) Give an example where G and H are both cyclic, but $G \times H$ is not.

   (b) If $G \times H$ is a cyclic group, prove that G and H are both cyclic.

   (c) Recall that $\mathbb{R}^\times$ is the multiplicative group of units of $\mathbb{R}$. Define an explicit isomorphism $f : \mathbb{R}^\times \to \mathbb{R} \times \mathbb{Z}_2$.

(a) $\mathbb{Z}_2 = \langle [1]_3 \rangle$ is cyclic

but $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. It can not be generted by any element among its 4 elements by either addition or multiplication.

(b) Proof. Let (g, h) be the generating element such that

$\langle (g, h) \rangle = G \times H$

Take arbitrary $m \in G$ and $n \in H$

So $(m, n) = (g, h)$ for some integer k

so $m = g^k$, $n = h^k$

Therefore $G = \langle g \rangle$, $H = \langle h \rangle$ are cyclic groups.

(c) $\mathbb{R}^\times = \{ a \neq 0 \mid a \in \mathbb{R} \}$.

define φ $\mathbb{R}^\times \to \mathbb{R} \times \mathbb{Z}_2$ as mapping

$$a \longmapsto \begin{cases} (\ln|a|, [1]_2) & \text{if } a < 0 \\ (\ln|a|, [0]_2) & \text{if } a > 0. \end{cases}$$

note that $\mathbb{R} \times \mathbb{Z}_2$ is a additive group.

while $\mathbb{R}^\times$ is a multiplicative group.

Take arbitrary $a, b \in \mathbb{R}^{\times}$,

$$\varphi(a)+\varphi(b) = (\ln|a|, m) + (\ln|b|, n)$$
$$= (\ln|ab|, m+n)$$

where $m = [0]_2$ if $a>0$, $m = [1]_2$ if $a<0$

and so is n.

So $m+n = [0]_2$ if $\text{sign}(m) = \text{sign}(n)$

i.e. if $ab>0$

$m+n = [1]_2$ if $\text{sign}(m) \neq \text{sign}(n)$

i.e. if $ab<0$

$\varphi(ab) = (\ln|ab|, s)$ where $s = [0]_2$ if $ab>0$

$s = [1]_2$ if $ab<0$

so $s = m+n$

Therefore $\varphi(a)+\varphi(b) = \varphi(ab)$, φ is a homomorphism.

Assume $\varphi(a) = \varphi(b)$ then

$$\varphi(a-b) = \varphi(a) - \varphi(b) = (0, [0]_2)$$

So $\ln|a| = \ln|b|$ and $\text{sign}(a) = \text{sign}(b)$

so $a = b \implies \varphi$ is injective

Let $(m, n) \in \mathbb{R} \times \mathbb{Z}_2$ be arbitrary.

Consider $a = e^{m} \cdot (-1)^{y}$, where $y=0$ if $n = [0]_2$

$y=1$ if $n = [1]_2$

So $\varphi(a) = (m, n) \implies \varphi$ is surjective

There φ is isomorphism.

2. Let $S^1 \subset \mathbb{C}$ be the unit circle; that is

$$S^1 = \{z \in \mathbb{C} \ : \ |z| = 1\}.$$

(a) Prove that S^1 is a subgroup of $\mathbb{C}^\times$.

(b) For every positive integer n, find an element of order n in S^1.

(c) Find an element of infinite order in S^1.

(a) Proof. As $\mathbb{C}$ is a field, every element except 0 is a unit in $\mathbb{C}$, so

So since $0 \notin S^1$ $(|0| \neq 1)$ and $S^1 \subseteq \mathbb{C}$, $S^1 \subseteq \mathbb{C}^\times$

Therefore it suffices to show that

① $1 \in S^1$

② Every element in S^1 has its multiplicative inverse also in S^1

① is true because $|1| = 1$

②: $\forall$ $a+bi \in S$, consider $a-bi \in S$ since $\sqrt{a^2+b^2} = 1$

$(a+bi)(a-bi) = a^2+b^2 = 1$, $a-bi$ is the multiplicative inverse of $a+bi$

Therefore we have proved S^1 is a subgroup of $\mathbb{C}^\times$

(b) Note that by Euler's formula,

$e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$, so $e^{2\pi i} \in S^1$ and is the identity

So for $\underbrace{\text{arbitrary } n \in \mathbb{Z}_{\geq 1}}$, consider $e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in S^1$

because $(\cos\frac{2\pi}{n})^2 + (\sin\frac{2\pi}{n})^2 = 1$

And note that $\underline{(e^{\frac{2\pi i}{n}})^n = e^{2\pi i} = 1}$

So the order of $e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ is n,

(c) Consider $e^{\sqrt{2}\pi i} = \cos\sqrt{2}\pi + i\sin\sqrt{2}\pi$

$\forall n \in \mathbb{Z}_{\geq 1}$, $(e^{\sqrt{2}\pi i})^n = e^{\sqrt{2}\pi i n} \neq e^{2k\pi i}$ since $\sqrt{2}$ is irrational, so its order is infinite

3. Let R be a commutative ring, and consider the group $\mathrm{GL}_2(R)$ of units in the ring of 2×2 matrices $\mathrm{M}_2(R)$ with coefficients in R.

(a) Suppose that

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in \mathrm{M}_2(R)$$

and all the entries are in an ideal $I \subsetneq R$. Prove that A is not a unit.

(b) Prove that for any matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(R)$$

there is a matrix B such that

$$AB = BA = \det(A)I_2.$$

(c) (This is the hard problem) Prove that a matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(R)$$

is a unit in $\mathrm{M}_2(R)$ if and only if $\det(A)$ is a unit.

(a) Assume for sake of contradiction that

A is a unit, then $\exists B \in M_2(R)$ s.t. $AB = BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

where 1 is the multiplicative identity of R.

Denote B by $\begin{bmatrix} m & n \\ p & q \end{bmatrix}$

Then $\begin{bmatrix} am+bp & an+bq \\ cm+dp & cn+dq \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Since $a, b \in I$ and $m, p \in R$, $am, bp \in I$

so $am+bp \in I$ since I is closed under addition

Therefore $1 \in I$, so $I = R$, which contradicts with $I \subsetneq R$

So A is not a unit.

(b) For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(R)$

consider $B = \operatorname{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in M_2(R)$

$AB = BA = \begin{bmatrix} ad-bc & ba-ab \\ ab-ba & da-cb \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix}$

since R is commutative,

$= (ad-bc)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \det(A)\, I_2$

(c) Since R is a commutative ring, it still applies that $\det(AB) = \det(A)\det(B)$ where $A, B \in M_2(R)$.
by calculation.

① Claim: if A is a unit in $M_2(R)$, then $\det(A)$ is a unit in R.

Proof Assume $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(R)$ is a unit.

Then $\exists C = \begin{bmatrix} m & n \\ p & q \end{bmatrix} \in M_2(R)$ s.t. $AC = CA = I_2$

So $\det(A)\det(C) = \det(I_2) = 1$ in R

$\det(C)\det(A) = \det(I_2) = 1$ in R

Therefore $\det(A)$ is a unit in R by definition.

② Claim: if $\det(A)$ is a unit in R then A is a unit in $M_2(R)$

Proof. Assume $\det(A)$ is a unit in R

then $\exists m \in R$ s.t. $m\det(A) = \det(A)m = 1$ in R

by (b) we know, $\exists B \in M_2(R)$ s.t.

$BA = AB = \det(A) I_2$

So consider $C = (\det(A))^{-1} B = mB$

$\Rightarrow CA = AC = (m\det(A)) I_2 = I_2$

Therefore A is a unit in $M_2(R)$.

By ①②, A is a unit in $M_2(R)$ iff $\det(A)$ is a unit in R.

4. Let p be a prime number and consider the field $\mathbb{Z}_p$.

(a) Show that a 2×2 matrix $A \in \mathrm{M}_2(\mathbb{Z}_p)$ is not a unit if and only if "the columns are linearly dependent."

(b) Show that the set of upper triangular invertible matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$ forms a subgroup of order $p(p-1)^2$, which is non-abelian when $p \neq 2$.

(c) Compute the order of $\mathrm{GL}_2(\mathbb{Z}_p)$.

(d) Show that the diagonal invertible matrices form an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of order $(p-1)^2$.

(e) Find an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ of order p. Make sure to show this is a subgroup.

(a) Claim ① $A \in M_2(\mathbb{Z}_p)$ is not a unit if the columns are linearly dependent.

Proof Assume the columns of $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ are linearly dependent.

then $m\begin{bmatrix} a \\ c \end{bmatrix} + n\begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ where $m, n \in \mathbb{Z}_p$ and are not both 0.

WLOG assume $m \neq 0$.

So since $\mathbb{Z}_p$ is a field (p is prime), $\exists m^{-1} \in \mathbb{Z}_p$

So $\begin{bmatrix} a \\ c \end{bmatrix} = -m^{-1}n\begin{bmatrix} b \\ d \end{bmatrix} \Rightarrow \det(A) = \underbrace{ad - bc = 0}_{\text{is not a unit.}}$

Since $\mathbb{Z}_p$ is a field and for sure a commutative ring, by problem 3 we have proved $A \in M_2(\mathbb{Z}_p)$ is a unit iff $\det(A) \in \mathbb{Z}_p$ is a unit.

So A is not a unit.

Claim ② if $A \in M_2(\mathbb{Z}_p)$ is not a unit, then the columns are linearly dependent.

Assume $A \in M_2(\mathbb{Z}_p)$ is not a unit and assume columns are not linearly dependent

so $\det(A) \neq [0]_p$

let $\det(A) = m$, then consider

$$B = m^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \Rightarrow AB = BA = I_2,$$

which contradicts with A not being a unit.

So the columns are linearly dependent.

Therefore we can conclude that $A \in M_2(\mathbb{Z}_p)$ is not a unit iff columns of A are linearly dependent.

(b) the set of upper triangular invertible matrices in $GL_2(\mathbb{Z}_p)$

is $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| \begin{array}{l} a, b, c \in \mathbb{Z}_p \\ \text{and } a, c \neq [0]_p \end{array} \right\} \leq GL_2(\mathbb{Z}_p)$

Since ① $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$

② $\forall A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$, since $a, c \neq 0$,

take $B = (ac)^{-1}\begin{bmatrix} c & -b \\ 0 & a \end{bmatrix} \in S$ we have

$AB = BA = I_2$, so every element in S has its inverse also in S.

So S is a subgroup of $GL_2(\mathbb{Z}_p)$

$|S| = p(p-1)^2$ since for $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in S$, there are $p-1$ different choices for a, $p-1$ different choices for c (since $a, c \neq 0$) and p different choices for b. The three choices are independent, so there are $p(p-1)^2$ elements in S.

Take $\begin{bmatrix} 1 & 1 \\ 0 & p-1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in S$

$$\begin{bmatrix} 1 & 1 \\ 0 & p-1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & p-1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & p-1 \end{bmatrix} = \begin{bmatrix} 1 & p \\ 0 & p-1 \end{bmatrix}$$

Since $\begin{bmatrix} 1 & 1 \\ 0 & p-1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & p-1 \end{bmatrix}$ if $p \neq 2$

S is nonabelian when $p \neq 2$.

When $p=2$, consider arbitrary $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, \begin{bmatrix} m & n \\ 0 & p \end{bmatrix} \in S$,

Since $a, c, m, p \neq 0 \Rightarrow a, c, m, p = 1$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\begin{bmatrix} m & n \\ 0 & p \end{bmatrix} = \begin{bmatrix} am & an+bp \\ 0 & cp \end{bmatrix} = \begin{bmatrix} 1 & b+n \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} m & n \\ 0 & p \end{bmatrix}\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} am & bm+cn \\ 0 & cp \end{bmatrix} = \begin{bmatrix} 1 & b+n \\ 0 & 1 \end{bmatrix}$$

So S is abelian iff $p=2$.

(c) By (a) we can conclude that $A \in M_2(\mathbb{Z}_p)$ is a unit (i.e. $A \in GL_2(\mathbb{Z}_p)$) iff columns of A are linearly independent.

Therefore we first choose an arbitrary non-zero vector $\begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{Z}_p^2$: there are (p^2-1) choices

Then we choose an arbitrary vector $\vec{v}$ which is linearly independent with it (by scalars in $\mathbb{Z}_p$), i.e. $\vec{v} \notin \left\{ k \begin{bmatrix} a \\ b \end{bmatrix} \middle| k \in \mathbb{Z}_p \right\}$

so there are (p^2-p) choices for the second column

So $|GL_2(\mathbb{Z}_p)| = (p^2-1)(p^2-p)$

(d) The set of diagonal invertible matrices is

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in M_2(\mathbb{Z}_p) \middle| a, b \neq 0 \right\}$$

There are $p-1$ choices for a and $p-1$ choices for b, so $|S| = (p-1)^2$

Now we show it is a subgroup of $GL_2(\mathbb{Z}_p)$

① $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$

② $\forall A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in S$, since $a, b \neq 0$, consider $B = (ab)^{-1} \begin{bmatrix} b & 0 \\ 0 & a \end{bmatrix}$

so $BA = I_2$. $\Longrightarrow$ A has an inverse.

Therefore S is a subgroup of $GL_2(\mathbb{Z}_p)$ whose order is $(p-1)^2$

Note that S is also abelian because $\forall A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in S$, $AB = BA = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}$

(e) $\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$ is a subgroup of $GL_2(\mathbb{Z}_p)$ whose order is p.

This is a subgroup of $GL_2(\mathbb{Z}_p)$ guaranteed by the generation of cyclic subgroup by an element in the group.

And note the $\left| \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \right|$ = the order of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $GL_2(\mathbb{Z}_p)$ as we have proved.

Since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^p = \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$

and $\forall\, 1 \leq n \leq p-1$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \neq I_2$

So $\left| \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \right| = p$.