Cavallaro, Jeffery
Math 221b
Homework #1

1). Let A be an abelian group. Prove that $\mathrm{End}(A)$ is a ring with pointwise addition and composition as multiplication.

Assume $\phi, \mu, \gamma \in \mathrm{End}(A)$
ϕ, μ, and γ are functions on A
Assume $a \in A$

$\phi(a) \in A$
$\mu(a) \in A$
But A is a group, so by closure:
$(\phi + \mu)(a) = \phi(a) + \mu(a) \in A$

$\therefore \mathrm{End}(A)$ is closed under addition.

$(\phi\mu)(a) = \phi(\mu(a)) \in A$

$\therefore \mathrm{End}(A)$ is closed under multiplication (composition).

A is a group and is thus associative under addition:

$$\begin{aligned}
((\phi + \mu) + \gamma)(a) &= (\phi + \mu)(a) + \gamma)(a) \\
&= (\phi(a) + \mu(a)) + \gamma(a) \\
&= \phi(a) + (\mu(a) + \gamma(a)) \\
&= \phi(a) + (\mu + \gamma)(a) \\
&= (\phi + (\mu + \gamma))(a)
\end{aligned}$$

$\therefore \mathrm{End}(A)$ is associative under addition.

And likewise for multiplication (composition):

$$\begin{aligned}
((\phi\mu)\gamma)(a) &= (\phi\mu)(\gamma(a)) \\
&= \phi(\mu(\gamma(a))) \\
&= \phi((\mu\gamma)(a)) \\
&= (\phi(\mu\gamma))(a)
\end{aligned}$$

$\therefore \mathrm{End}(A)$ is associative under multiplication (composition).

A is a group, so $0 \in A$ is a two-sided additive identity for A
Let 0_A be the zero (trivial) endomorphism
$0_A \in \mathrm{End}(A)$
$(\phi + 0_A)(a) = \phi(a) + 0_A(a) = \phi(a) + 0 = \phi(a)$
$(0_A + \phi)(a) = 0_A(a) + \phi(a) = 0 + \phi(a) = \phi(a)$

Therefore 0_A is a two-sided additive identity for $\mathrm{End}(A)$.

Let $\phi' = -\phi$
Since A is a group it is closed under additive inverses, so:
$\phi'(a) = -\phi(a) \in A$
Assume $b \in A$
$\phi'(a+b) = -\phi(a+b) = -(\phi(a)+\phi(b)) = -\phi(a) + (-\phi(b)) = \phi'(a) + \phi'(b)$
ϕ' is a homomorphism, and hence an endomorphism
$\phi' \in \mathrm{End}(A)$
$(\phi' + \phi)(a) = \phi'(a) + \phi(a) = -\phi(a) + \phi(a) = 0 = 0_A(a)$
$(\phi + \phi')(a) = \phi(a) + \phi'(a) = \phi(a) + (-\phi(a)) = 0 = 0_A(a)$
So ϕ' is a two-sided additive inverse for ϕ

$\therefore \mathrm{End}(A)$ is closed under additive inverses.

$\therefore \mathrm{End}(A)$ is a group.

A is an abelian (commutative) group:

$$(\phi + \mu)(a) = \phi(a) + \mu(a) = \mu(a) + \phi(a) = (\mu + \phi)(a)$$

$\therefore \mathrm{End}(A)$ is an abelian group.

ϕ is a group homomorphism, so:

$$\begin{aligned}
(\phi(\mu+\gamma))(a) &= \phi((\mu+\gamma)(a)) \\
&= \phi(\mu(a)+\gamma(a)) \\
&= \phi(\mu(a)) + \phi(\gamma(a)) \\
&= (\phi\mu)(a) + (\phi\gamma)(a) \\
&= (\phi\mu + \phi\gamma)(a)
\end{aligned}$$

$\therefore$ left distributivity holds.

Likewise:

$$\begin{aligned}
((\mu+\gamma)\phi)(a) &= (\mu+\gamma)(\phi(a)) \\
&= \mu(\phi(a)) + \gamma(\phi(a)) \\
&= (\mu\phi)(a) + (\gamma\phi)(a) \\
&= (\mu\phi + \gamma\phi)(a)
\end{aligned}$$

$\therefore$ right distributivity holds.

So $\mathrm{End}(A)$ is an additive abelian group, is associative under multiplication (composition), and the distributive properties hold

$\therefore \mathrm{End}(A)$ is a ring.

2). a). Let R be a ring with $1 \neq 0$. Prove: $R^\times$ is a group.

R is ring and thus is associative under multiplication
$R^\times \subset R$

$\therefore R^\times$ inherits multiplicative associativity.

$1 \in R$
$1 \cdot 1 = 1$
1 is a unit
$1 \in R^\times$

$\therefore R^\times \neq \emptyset$

Assume $r, s \in R^\times$
By construction: $r^{-1}, s^{-1} \in R^\times$
$r, s, r^{-1}, s^{-1} \in R$
By closure, $rs, s^{-1}r^{-1} \in R$
1 is a two-sided identity for R
$(rs)(s^{-1}r^{-1}) = r(ss^{-1})r^{-1} = r1r^{-1} = rr^{-1} = 1$
$(s^{-1}r^{-1})(rs) = s^{-1}(r^{-1}r)s = s^{-1}1s = s^{-1}s = 1$
So $s^{-1}r^{-1}$ is a two-sided multiplicative inverse for rs in R
rs is a unit
$rs \in R^\times$

$\therefore R^\times$ is closed under multiplication.

$r1 = 1r = r$
$\therefore 1$ is a two-sided identity for $R^\times$.

By construction, $R^\times$ is closed under multiplicative inverses.

$\therefore R^\times$ is a multiplicative group.

b). Prove: $M_2(\mathbb{Z})^\times = \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$

It is known that $\mathbb{Z}$ is a commutative ring with unity 1
It is also known that $M_2(\mathbb{Z})$ is a ring with unity I_2

Assume $B \in M_2(\mathbb{Z})$
Let $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, a, b, c, d \in \mathbb{Z}$
$\det(B) = ad - bc \in \mathbb{Z}$ (closure)

$\implies$ Assume $B \in M_2(\mathbb{Z})^\times$

By construction, B is a unit
So B is invertible and $B^{-1} \in M_2(\mathbb{Z})^\times$
$BB^{-1} = I_2$
$\det(BB^{-1}) = \det(I_2) = 1$
$\det(B)\det(B^{-1}) = 1$
Thus, $\det(B)$ and $\det(B^{-1})$ must be units in $\mathbb{Z}$

But $\mathbb{Z}^\times = \{\pm 1\}$
So $\det(B) = \pm 1$

$\therefore B \in \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$

$\Longleftarrow$ Assume $B \in \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$

$\det(B) = ad - bc = \pm 1 \neq 0$
So B is invertible and B^{-1} exists
$B^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$
But $ad - bc = \pm 1$ and $a, (-b), (-c), d \in \mathbb{Z}$, so $B^{-1} \in M_2(\mathbb{Z})$
So B and B^{-1} are multiplicative inverses in $M_2(\mathbb{Z})$
B is a unit in $M_2(\mathbb{Z})$

$\therefore B \in M_2(\mathbb{Z})^\times$

$\therefore M_2(\mathbb{Z})^\times = \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$

c). Prove: $\forall\, n \in \mathbb{Z}^+, (\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid (a, n) = 1\}$

Assume $n \in \mathbb{Z}^+$

It is known that $(\mathbb{Z}/n\mathbb{Z})^\times$ is ring with unity $1 + nZ$

$$\begin{aligned}
a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times \quad &\Longleftrightarrow \quad \exists\, b + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times, (a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z} = 1 + n\mathbb{Z} \\
&\Longleftrightarrow \quad ab \equiv 1 \pmod{n} \\
&\Longleftrightarrow \quad \exists\, k \in \mathbb{Z}, ab - 1 = kn \\
&\Longleftrightarrow \quad ba + (-k)n = 1 \text{ has solutions in } \mathbb{Z} \\
&\Longleftrightarrow \quad (a, n) = 1 \qquad \text{(Bézout)} \\
&\Longleftrightarrow \quad a + n\mathbb{Z} \in \{a + n\mathbb{Z} \mid (a, n) = 1\}
\end{aligned}$$

d). Prove: $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

It is known that $\mathbb{Z}$ is a ring with unity 1
It is also known that $\mathbb{Z}[i]$ is a ring with unity $1 + i0 = 1$
$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$
$|a + ib|^2 = a^2 + b^2 \in \mathbb{Z}$ (closure)

$\Longrightarrow$ Assume $z \in \mathbb{Z}[i]^\times$

$\exists z' \in \mathbb{Z}[i]^\times, zz' = 1$
$|zz'| = 1$
$|zz'|^2 = 1$
$|z|^2 |z'|^2 = 1$
But $|z|^2, |z'|^2 \in \mathbb{Z}$
So $|z|^2$ and $|z'|^2$ are units in $\mathbb{Z}$
But both are ≥ 0
So $|z|^2 = |z'|^2 = 1$
But $|z| \in \mathbb{R}$ and $|z| \geq 0$

So $|z| = 1$, the unit circle
But the only lattice points on the unit circle are $\{\pm 1, \pm i\}$

$\therefore z \in \{\pm 1, \pm i\}$

$\Longleftarrow$ Assume $a + ib \in \{\pm 1, \pm i\}$

$1 = 1 + i0 \in \mathbb{Z}[i]$
$1 \cdot 1 = 1$

$-1 = -1 + i0 \in \mathbb{Z}[i]$
$(-1) \cdot (-1) = 1$

$i = 0 + i1 \in \mathbb{Z}[i]$
$-i = 0 + i(-1) \in \mathbb{Z}[i]$
$i \cdot (-i) = 1$

$\therefore \{\pm 1, \pm i\} \subseteq \mathbb{Z}[i]^\times$

$\therefore \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

3). Prove: Every finite integral domain is a field.

Assume F is a finite integral domain
F is a commutative ring with unity $1 \neq 0$

Assume $a \in F, a \neq 0$
Let $L_a : F \to F$ be defined by $L_a(x) = ax$

Assume $L_a(x) = L_a(y)$
$ax = ay$
But F is an integral domain, so the cancellation laws hold
$x = y$
$\therefore L_a$ is one-to-one.

But F is finite, so L_a is also onto
$\therefore L_a$ is a bijection on F.

$1 \in F$
$\exists\, x \in F, L_a(x) = 1$
$ax = 1$
But F is cummutative so $xa = 1$
So x is a multiplicative inverse for a
Thus every non-zero element of F has a multiplicative inverse

$\therefore F$ is a field.