Math 103B HW2 Solution.

1. (a) $x^2 - x - 2 = (x+1)(x-2) = 0$

17 is prime $\Rightarrow \mathbb{Z}_{17}$ is integral domain

$\Rightarrow x+1 = 0$ or $x - 2 = 0$.

$\Rightarrow x = 16$ or $x = 2$ are the two solutions.

(b) 18 is not prime, $\mathbb{Z}_{18}$ has zero divisors.

For example, $3 \neq 0$. $6 \neq 0$ but $3 \times 6 = 0$.

Except for $x = 2$ and $x = 16$, $x = 5$ is also a solution since $(5+1)(5-2) = 0$.

2. We denote the charateristic of a ring by c.

- For $\mathbb{Z}_4 \times \mathbb{Z}_6$.

$\forall (m,n) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, $12(m,n) = (12m, 12n) = (0,0) \Rightarrow c \leq 12$

On the other hand, $c \cdot (1,0) = (c,0) = (0,0) \Rightarrow 4 \mid c$.
$c \cdot (0,1) = (0,c) = (0,0) \Rightarrow 6 \mid c$
$\Bigg\} \Rightarrow 12 \mid c$ $\Bigg\} \Rightarrow c = 12$.

- For $\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_9$.

$\forall (m,n,k) \in \mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_9$, $72(m,n,k) = (72m, 72n, 72k) = (0,0,0) \Rightarrow c \leq 72$

On the other hand, $c \cdot (1,0,0) = (c,0,0) = (0,0,0) \Rightarrow 6 \mid c$
$c \cdot (0,1,0) = (0,c,0) = (0,0,0) \Rightarrow 8 \mid c$
$c \cdot (0,0,1) = (0,0,c) = (0,0,0) \Rightarrow 9 \mid c$
$\Bigg\} \Rightarrow 72 \mid c$

$\Rightarrow c = 72$.

Remark: you could also use the fact that the characteristic of a unital ring is the order of the unity if it's finite. So to compute characteristic, it's enough to figure out the order of $(1,1)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$ and $(1,1,1)$ in $\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_9$.

3. (a) · First since $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$

We know $\mathbb{Q}[\sqrt{2}]$ is closed under addition and multiplication.

· $\mathbb{Q}[\sqrt{2}]$ inherits its addition and multiplication from $\mathbb{R}$ so it automatically satiesfies $a+b = b+a$, $a+(b+c) = (a+b)+c$, $a(bc) = (ab)c$, $a(b+c) = ab+ac$ for $a, b \in \mathbb{Q}[\sqrt{2}]$.

· 0 is additive identity. for $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $-(a+b\sqrt{2}) = -a-b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

· 1 is multiplicative identity, for $a+b\sqrt{2} \underset{\neq 0}{\in} \mathbb{Q}[\sqrt{2}]$, $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}[\sqrt{2}]$.

note that $a^2-2b^2 \neq 0$ ($a+b\sqrt{2} \neq 0 \Rightarrow$ either $a \neq 0$ or $b \neq 0$. $\Rightarrow \sqrt{2} = |\frac{b}{a}|$ or $\sqrt{2} = |\frac{a}{b}|$, in either case $\sqrt{2}$ is rational, which is impossible).

$\Longrightarrow$ $\mathbb{Q}[\sqrt{2}]$ is a field.

(b) Define map

$$i : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}]$$
$$m+n\sqrt{2} \longmapsto m+n\sqrt{2}.$$

Then clearly i is injective ring homomorphism.

$\forall\ a+b\sqrt{2} = \frac{p_1}{q_1} + \frac{p_2}{q_2}\sqrt{2}$ with $p_i, q_i \in \mathbb{Z}$

$a+b\sqrt{2} = \frac{p_1q_2 + q_1p_2\sqrt{2}}{q_1q_2}$ with $q_1q_2 \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{2}]$, $p_1q_2 + q_1p_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

$\Longrightarrow$ $\mathbb{Q}[\sqrt{2}]$ is the field of fraction of $\mathbb{Z}[\sqrt{2}]$.

4. · First we check f is homomorphism.

Let $a, b, c, d \in \mathbb{Z}$.

$$f((a+b\sqrt{2}) + (c+d\sqrt{2})) = f((a+c)+(b+d)\sqrt{2}) = \begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix}$$

$$f(a+b\sqrt{2}) + f(c+d\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix}$$

$$\Longrightarrow f((a+b\sqrt{2})+(c+d\sqrt{2})) = f(a+b\sqrt{2}) + f(c+d\sqrt{2}).$$

Also, $$f((a+b\sqrt{2})(c+d\sqrt{2})) = f((ac+2bd)+(ad+bc)\sqrt{2}) = \begin{bmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{bmatrix}$$

$$f(a+b\sqrt{2}) \cdot f(c+d\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & 2(ad+bc) \\ bc+ad & 2bd+ac \end{bmatrix}$$

$$\Longrightarrow f((a+b\sqrt{2})(c+d\sqrt{2})) = f(a+b\sqrt{2}) \cdot f(c+d\sqrt{2}).$$

· Now we check f is one to one, enough to show $\ker f = \{0\}$.

Suppose $f(a+b\sqrt{2}) = 0$, $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Then $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = 0 \Rightarrow a=0,\ b=0.$ $\Longrightarrow a+b\sqrt{2} = 0 \Rightarrow \ker f = \{0\}$

· Every $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ in codomain has preimage $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Hence f is onto.

$\Rightarrow$ f is isomorphism of rings.

5. By binomial formula,

$$(x+y)^p = \binom{p}{0}x^p y^0 + \binom{p}{1}x^{p-1}y^1 + \cdots + \binom{p}{i}x^{p-i}y^i + \cdots + \binom{p}{p}x^0 y^p.$$

$\forall i,\ 0<i<p$, we have $p \mid \binom{p}{i}$.

$\Rightarrow \binom{p}{i}x^{p-i}y^i = 0 \quad \forall i.\ 0<i<p$, since A has characteristic p.

$\Rightarrow (x+y)^p = x^p + y^p$.

Remark. $\forall i$ s.t. $0<i<p$, $p \mid \binom{p}{i}$.

Proof: $\binom{p}{i} = \dfrac{p!}{i!\,(p-i)!}$

$\Rightarrow p! = \binom{p}{i}\, i!\, (p-i)!$

p divides one of the factors on the right hand side.

$p \nmid i!$. $p \nmid (p-i)!$ since $i<p$, $p-i<p$.

$\Rightarrow p$ has to divide $\binom{p}{i}$.

6. ⓐ $5 = 1^2 + 2^2 = 1-(2i)^2 = (1+2i)(1-2i)$.

$\Rightarrow$ In $\mathbb{Z}_5[i]$, $1+2i,\ 1-2i \neq 0$ but $(1+2i)(1-2i)=0$.

ⓑ

x	0	1	2	3	4	5	6
$1+x^2$	1	2	5	3	3	4	2

$\Rightarrow 1+x^2$ has no solution in $\mathbb{Z}_7$.

ⓒ We can assume $a \neq 0$ (the case $b \neq 0$ is done similarly).

$\mathbb{Z}_7$ is a field since 7 is prime and $a \neq 0$ implies it makes sense to talk about a^{-1}.

$a^2 + b^2 = a^2(1+(ba^{-1})^2) = 0 \Rightarrow 1+(ba^{-1})^2 = 0$ in $\mathbb{Z}_7$.

since $\mathbb{Z}_7$ has no zero divisor and $a \neq 0$.

But ⓑ shows that there is no such ba^{-1}.

$\Rightarrow a^2+b^2$ is never 0 in $\mathbb{Z}_7$.

ⓓ $\mathbb{Z}_7$ is finite, $i^2=-1 \Rightarrow \mathbb{Z}_7[i]$ is finite ring.

To show $\mathbb{Z}_7[i]$ is field, it's enough to show $\mathbb{Z}_7[i]$ is integral domain.

Suppose $(a+bi)(c+di) = 0$.

Then $(a-bi)(a+bi)(c+di)(c-di) = 0$

$\Rightarrow (a^2+b^2)(c^2+d^2) = 0$.

$\Rightarrow a^2+b^2 = 0$ or $c^2+d^2 = 0$

$\Rightarrow$ By c, $a=b=0$ or $c=d=0$

i.e. $a+bi = 0$ or $c+di = 0$. $\Rightarrow \mathbb{Z}_7[i]$ is an integral domain.