Name: Huize Shi - A92122910
Discussion: A04
Homework: 2

---

1. (a) Find all the solutions of $x^2 - x - 2$ in $\mathbb{Z}_{17}$.

$$x^2 - x - 2 = (x-2)(x+1)$$

Since 17 is prime, we know that $\mathbb{Z}_{17}$ is a field which is also a integral domain. This means that $\mathbb{Z}_{17}$ has no zero divisors which means there are only two zeros, 2 and 16.

(b) Does $x^2 - x - 2$ have only two zeros in $\mathbb{Z}_{18}$? No, since 18 is a composite, we know that besides 2 and 17, $x - 2 = 9$, $x = 11$, and $x + 1 = 2$, $x = 1$ make at least one other pair of zeros since $9 \cdot 2 = 0$ $(mod\ 18)$.

2. By Lemma prooved in class, given ring R, if $ord(1_R) < \infty$, $Char(R) = ord(1_R)$.

Characteristic of $\mathbb{Z}_4 \times \mathbb{Z}_6$

$$\begin{aligned} 1_{\mathbb{Z}_4 \times \mathbb{Z}_6} &= (1_{\mathbb{Z}_4}, 1_{\mathbb{Z}_6}) \\ ord(1_{\mathbb{Z}_4 \times \mathbb{Z}_6}) &= LCM\left(ord(1_{\mathbb{Z}_4}), ord(1_{\mathbb{Z}_6})\right) \\ &= LCM(4, 6) = 12 \end{aligned}$$

Characteristic of $\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_9$

$$\begin{aligned} 1_{\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_9} &= (1_{\mathbb{Z}_6}, 1_{\mathbb{Z}_8}, 1_{\mathbb{Z}_9}) \\ 1_{\mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_9} &= LCM\left(ord(1_{\mathbb{Z}_6}), ord(1_{\mathbb{Z}_8}), ord(1_{\mathbb{Z}_9})\right) \\ &= LCM(6, 8, 9) = 72 \end{aligned}$$

3. (a) Show $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ is a field:

$(\mathbb{Q}[\sqrt{2}], +)$ **is Abelian Group:**

Associative:

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

Identity:

$$
\begin{aligned}
0 &= (0+0\sqrt{2}) \\
(a+b\sqrt{2}) + (0+0\sqrt{2}) &= a+b\sqrt{2} \\
(0+0\sqrt{2}) + (a+b\sqrt{2}) &= a+b\sqrt{2}
\end{aligned}
$$

Inverse:

$$
\begin{aligned}
(a+b\sqrt{2}) + (-a-b\sqrt{2}) = (0+0\sqrt{2}) = 0 \\
(-a-b\sqrt{2}) + (a+b\sqrt{2}) = (0+0\sqrt{2}) = 0
\end{aligned}
$$

Abelian:

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

$(\mathbb{Q}[\sqrt{2}], \cdot)$ **is Associative:**

$$
\begin{aligned}
&((a+b\sqrt{2})\cdot(c+d\sqrt{2}))\cdot(e+f\sqrt{2}) \\
=&(ac+(ad+bc)\sqrt{2}+2bd)\cdot(e+f\sqrt{2}) \\
=&((ac)e+(ad+bc+(ac)f+(ad)e+(bc)e+2(bd)f)\sqrt{2}+2((ad)f+(bc)f+bd+(bd)e)) \\
=&(a(ce)+(ad+bc+a(cf)+a(de)+b(ce)+2b(df))\sqrt{2}+2(a(df)+b(cf)+bd+b(de))) \\
=&(a+b\sqrt{2})(ce+(cf+de)\sqrt{2}+2df) \\
=&(a+b\sqrt{2})\cdot((c+d\sqrt{2})\cdot(e+f\sqrt{2}))
\end{aligned}
$$

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ **is distributive:**

$$
\begin{aligned}
&(a+b\sqrt{2})\cdot((c+d\sqrt{2})+(e+f\sqrt{2})) \\
=&(a+b\sqrt{2})\cdot(c+d\sqrt{2}+e+f\sqrt{2}) \\
=&ac+ad\sqrt{2}+ae+af\sqrt{2}+b\sqrt{2}c+2bd+b\sqrt{2}e+2bf \\
=&(ac+ad\sqrt{2}+b\sqrt{2}e+2bf)+(ae+af\sqrt{2}+b\sqrt{2}c+2bd) \\
=&(a+b\sqrt{2})\cdot(c+d\sqrt{2})+(a+b\sqrt{2})\cdot(e+f\sqrt{2})
\end{aligned}
$$

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ **has unity:**

$$(a + b\sqrt{2}) \cdot (1 + 0\sqrt{2}) = a + b\sqrt{2}$$
$$(1 + 0\sqrt{2}) \cdot (a + b\sqrt{2}) = a + b\sqrt{2}$$

Hence $(1 + 0\sqrt{2}) = 1$ is the unity.

$(\mathbb{Q}[\sqrt{2}], +, \cdot)$ **has multiplicative inverse:**

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\end{aligned}$$

Since $\mathbb{Q}$ is a field (therefore closed under addition, multiplication, and has multiplicative inverse), the inverse shown above is of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$.

(b) Prove that $\mathbb{Q}[\sqrt{2}]$ is the filed of fractions of $\mathbb{Z}[\sqrt{2}]$ ($\mathbb{Q}[\sqrt{2}]$ is proven to be a field in part a).

Define Ring homomorphism: $\theta : \mathbb{Z}[\sqrt{2}] \mapsto \mathbb{Q}[\sqrt{2}]$ by $\theta(a + b\sqrt{2}) = \frac{a}{1} + \frac{b}{1}\sqrt{2}$ where $a, b \in \mathbb{Z}$.

Proof. θ is a ring homomorphism:
θ preserves addition:

$$\begin{aligned}\theta\left((a + b\sqrt{2}) + (c + d\sqrt{2})\right) &= \theta\left((a + c) + (b + d)\sqrt{2})\right) \\ &= \frac{a + c}{1} + \frac{b + d}{1}\sqrt{2} \\ &= \frac{a}{1} + \frac{b}{1}\sqrt{2} + \frac{c}{1} + \frac{d}{1}\sqrt{2} \\ &= \theta(a + b\sqrt{2}) + \theta(c + d\sqrt{2})\end{aligned}$$

θ preserves multiplication:

$$\begin{aligned}\theta\left((a + b\sqrt{2}) \cdot (c + d\sqrt{2})\right) &= \theta((ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= \frac{ac + 2bd}{1} + \frac{ad + bc}{1}\sqrt{2} \\ &= \frac{ac}{1} + \frac{ad}{1}\sqrt{2} + \frac{bc}{1}\sqrt{2} + \frac{2bd}{1} \\ &= (\frac{a}{1} + \frac{b}{1}\sqrt{2}) \cdot (\frac{c}{1} + \frac{d}{1}\sqrt{2}) \\ &= \theta(a + b\sqrt{2}) \cdot \theta(c + d\sqrt{2})\end{aligned}$$

□

Any element in $\mathbb{Q}[\sqrt{2}]$ has the form $\theta(a+b\sqrt{2})\theta(a+b\sqrt{2})^{-1}$ where $a, b \in \mathbb{Z}$
Let $\frac{a}{b} + \frac{c}{d}\sqrt{2}$ be a generic element of $\mathbb{Q}[\sqrt{2}]$.

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d}\sqrt{2} &= \theta(e+f\sqrt{2})\theta(g+h\sqrt{2})^{-1} \\
&= (\frac{e}{1} + \frac{f}{1}\sqrt{2}) \cdot (\frac{g}{g^2-2h^2} - \frac{h}{g^2-2h^2}\sqrt{2}) \\
&= \frac{eg}{g^2-2h^2} - \frac{eh}{g^2-2h^2}\sqrt{2} + \frac{fg}{g^2-2h^2}\sqrt{2} - \frac{2fh}{g^2-2h^2} \\
&= \frac{eg-2fh}{g^2-2h^2} + \frac{fg-eh}{g^2-2h^2}\sqrt{2}
\end{aligned}$$

Hence shown any element in $\mathbb{Q}[\sqrt{2}]$ has the form $\theta(a+b\sqrt{2})\theta(a+b\sqrt{2})^{-1}$ where $a, b \in \mathbb{Z}$.

4. *Proof.* Show $f : \mathbb{Z}[\sqrt{2}] \mapsto \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ by $f(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ is isomorphism of rings:

Homomorphism:

Preserve addition:

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

Preserve multiplication:

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

Injective: Define inverse of f:

$$f^{-1} : \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\} \mapsto \mathbb{Z}[\sqrt{2}]$$
$$f^{-1}\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \right) = a + b\sqrt{2}$$

This is well defined because f^{-1} maps every element of the domain to a single value in the codomain.
Hence shown $f : \mathbb{Z}[\sqrt{2}] \mapsto \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ by $f(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ is isomorphism of rings. □

5. Suppose A is a unital commutative ring of characteristic $p > 0$ where p is prime.

Proof. Show that $\forall x, y \in A, (x + y)^p = x^p + y^p$

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

Since A is of order p, $a \in A, pa = 0$. Since we know $\binom{p}{0}$ and $\binom{p}{p}$ are 1_A, it is suffice to show $p \mid \binom{p}{i}, i \in (0, p)$, since that would result in $1_A \cdot x^p + 0 + \cdots + 0 + 1_A \cdot y^p = x^p + y^p$.

$$\begin{aligned} \binom{p}{i} &= \frac{p!}{i!(p-i)!} \\ &= \frac{p \cdot (p-1) \cdot \ldots (p-i+1)}{i!} \end{aligned}$$

Since p is prime, and $i < p$, none of the factors in $i!$ can divide p. However, $\binom{p}{i}$ is an integer, therefore p must be a factor in $\binom{p}{i}$, hence $pdivide\binom{p}{i}$.
Hence shown given A is a unital commutative ring of characteristic $p > 0$ where p is prime $\forall x, y \in A, (x + y)^p = x^p + y^p$. □

6. (a) Find a zero-divisor in $\mathbb{Z}_5[i] = \{a + bi \mid a, b \in \mathbb{Z}_5\}$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = 0 \text{ in } \mathbb{Z}_5$$
$$ac \overset{5}{\equiv} bd$$
$$ad \overset{5}{\equiv} -bc$$

$$(3 + i) \cdot (4 + 2i) = (12 - 2) + (6 + 4)i = 10 + 10i \overset{5}{\equiv} 0$$

(b) Show that $x^2 + 1$ has no zero in $\mathbb{Z}_7$.

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

There is no 0 in $\mathbb{Z}_7$.

(c) Show that if either $a \neq 0$ or $a \neq 0$ in $\mathbb{Z}_7$, then $a^2 + b^2 \neq 0$.
Since addition is commutative, without loss of generality, it is sufficient to show if $a \neq 0$, then $a^2 + b^2 = a^2(1 + \frac{b}{a}^2)$. By part b, we know $1 + \frac{b}{a}^2 \neq 0$. Since we assume $a \neq 0 \Rightarrow a^2 \neq 0$, we conclude $a^2 + b^2 \neq 0$.

(d) Show that $\mathbb{Z}_7[i] = \{a + bi \mid a, b \in \mathbb{Z}_7\}$ is a field.
Since 7 is prime, we know $\mathbb{Z}_7$ is a field, therefore we can conclude that $\mathbb{Z}_7[i]$ has multiplicative inverse.

Integral domain: Show no-zero divisors:

$$\begin{aligned} (a+bi)(c+di) &= 0 \\ \Rightarrow (a+bi)(a-bi)(c-di) &= 0 \\ \Rightarrow (a^2+b^2)(c^2+d^2) &= 0 \text{ in } \mathbb{Z}_7 \end{aligned}$$

By part c, we know either a or b and c or d are $\neq 0$, then the product is not zero. This means either $a + bi = 0$ or $c + d = 0$.