Homework 8 Solutions

(1)

($\Longrightarrow$) Suppose that $x-c$ is a divisor of $f(x)$ in $F[x]$. Then $f(x)=(x-c)g(x)$ where $g(x)\in F[x]$. Then

$$f(c)=(c-c)g(c)=0\cdot g(c)=0.$$

So, c is zero of $f(x)$.

($\Longleftarrow$) Suppose that $f(c)=0$ where $c\in F$. By the division algorithm in $F[x]$, there exist $q(x), r(x)\in F[x]$ with

$$f(x)=(x-c)\cdot q(x)+r(x)$$

where $\text{degree}(r(x))<\deg(x-c)=1$. Hence $r(x)=d$ where d is a constant from F. That is, $f(x)=(x-c)q(x)+d$. Since $f(c)=0$ we have $0=f(c)=(c-c)q(c)+d=d$. Thus, $f(x)=(x-c)q(x)$. Thus, $x-c$ divides $f(x)$ in $F[x]$.

~~Homework 8 Solutions~~

2

(a) Let $f(x) = x^2 + \overline{1}$ in $\mathbb{Z}_3[x]$.

Then $f(\overline{0}) = \overline{0}^2 + \overline{1} = \overline{1} \neq \overline{0}$

$f(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{2} \neq \overline{0}$

and $f(\overline{2}) = \overline{2}^2 + \overline{1} = \overline{5} = \overline{2} \neq \overline{0}$.

Since $\deg(f) = 2$ and f has no zeros in $\mathbb{Z}_3$, $f(x)$ is irreducible in $\mathbb{Z}_3[x]$.

(b) Let $g(x) = x^2 + \overline{2}$ in $\mathbb{Z}_3[x]$.

Then $g(\overline{1}) = \overline{1}^2 + \overline{2} = \overline{3} = \overline{0}$.

Hence we may factor $g(x)$.

$$\begin{array}{r|l} & x + \overline{1} \\ \hline x + \overline{2} & x^2 + \overline{2} \\ & -(x^2 - \overline{x}) \\ \hline & x + \overline{2} \\ & -(x + \overline{2}) \\ \hline & \overline{0} \end{array}$$

$x - \overline{1} = x + \overline{2}$

Hence,

$$x^2 + \overline{2} = (x + \overline{1})(x + \overline{2})$$

(c) Let $h(x) = x^2 + x + \bar{1}$ in $\mathbb{Z}_3[x]$.
Note that $h(\bar{1}) = \bar{1}^2 + \bar{1} + \bar{1} = \bar{3} = \bar{0}$.
Hence we may factor $h(x)$. That is,
$x - \bar{1} = x + \bar{2}$ is a factor of $x^2 + x + \bar{1}$.

$$\begin{array}{r|l}
 & x + \bar{2} \\ \hline
x + \bar{2} & x^2 + x + 1 \\
 & -(x^2 + \bar{2}x) \\ \hline
 & \underbrace{-x + \bar{1}}_{\bar{2}x + \bar{1}} \\
 & -(\bar{2}x + \bar{1}) \\ \hline
 & \bar{0}
\end{array}$$

So,
$x^2 + x + \bar{1} = (x + \bar{2})(x + \bar{2})$

(d) Let $f(x) = x^4 + \bar{4}$ in $\mathbb{Z}_5[x]$.
Then $f(\bar{1}) = \bar{1}^4 + \bar{4} = \bar{5} = \bar{0}$. Hence $x - \bar{1} = x + \bar{4}$
is a factor of $x^4 + \bar{4}$.

$$\begin{array}{r|l}
 & x^3 + x^2 + x + 1 \\ \hline
x + \bar{4} & x^4 + \bar{4} \\
 & -(x^4 + \bar{4}x^3) \\ \hline
 & x^3 + \bar{4} \\
 & -(x^3 + \bar{4}x^2) \\ \hline
 & x^2 + \bar{4} \\
 & -(x^2 + \bar{4}x) \\ \hline
 & x + \bar{4} \\
 & -(x + \bar{4}) \\ \hline
 & \bar{0}
\end{array}$$

So, $x^4 + \bar{4} = (x + \bar{4})(x^3 + x^2 + x + \bar{1})$

Let $g(x) = x^3 + x^2 + x + 1$.

Then $g(\bar{2}) = \bar{2}^3 + \bar{2}^2 + \bar{2} + \bar{1} = \bar{8} + \bar{4} + \bar{3} = \overline{15} = \bar{0}$.

Hence $x - \bar{2} = x + \bar{3}$ is a factor of $x^3 + x^2 + x + \bar{1}$

$$
\begin{array}{r l}
 & x^2 + \bar{3}x + \bar{2} \\
x + \bar{3} \,\big) & x^3 + x^2 + x + \bar{1} \\
 & -(x^3 + \bar{3}x^2) \\
\hline
 & -\bar{2}x^2 + x + \bar{1} \\
 & \bar{3}x^2 + x + \bar{1} \\
 & -(\bar{3}x^2 + \bar{4}x) \\
\hline
 & \bar{2}x + \bar{1} \\
 & -(\bar{2}x + \bar{1}) \\
\hline
 & \bar{0}
\end{array}
$$

So,

$$x^4 + \bar{4} = (x + \bar{4})(x^3 + x^2 + x + 1)$$
$$= (x + \bar{4})(x + \bar{3})(x^2 + \bar{3}x + \bar{2})$$

Let $h(x) = x^2 + \bar{3}x + \bar{2}$. Then $h(\bar{3}) = \bar{3}^2 + \bar{3} \cdot \bar{3} + \bar{2} = \overline{20} = \bar{0}$.

Hence $x - \bar{3} = x + \bar{2}$ is a factor of $x^2 + \bar{3}x + \bar{2}$.

$$
\begin{array}{r l}
 & x + \bar{1} \\
x + \bar{2} \,\big) & x^2 + \bar{3}x + \bar{2} \\
 & -(x^2 + \bar{2}x) \\
\hline
 & x + \bar{2} \\
 & -(x + \bar{2}) \\
\hline
 & \bar{0}
\end{array}
$$

Hence,

$$x^4 + \bar{4} = (x + \bar{4})(x + \bar{3})(x + \bar{2})(x + \bar{1})$$

(3) Let $p=5$. Then 5 is prime and
5 divides -5, 195, and 10.
But 5^2 does not divide 10. Hence, by Eisenstein's
criteria $x^5-5x^3+195x+10$ is
irreducible in $\mathbb{Q}[x]$.

---

(4) Let $p=2$. Then 2 divides 2
and 2^2 does not divide 2.
By Eisenstien's criteria, x^2-2 is
irreducible in $\mathbb{Q}[x]$.

---

(5) Let $p=5$. Then 5 divides 10
and 5^2 does not divide 10.
By Eisenstein's criteria, $x^{10}-10$
is irreducible in $\mathbb{Q}[x]$.

⑥ Consider the field $\mathbb{Z}_2$.
Let $p(x) = x^2 + x + \overline{1}$. Since

$$p(\overline{0}) = \overline{0}^2 + \overline{0} + \overline{1} = \overline{1} \neq \overline{0}$$

and $p(\overline{1}) = \overline{1}^2 + \overline{1} + \overline{1} = \overline{3} \neq \overline{0}$

and degree $(p(x)) = 2$ we know that $p(x)$ is irreducible in $\mathbb{Z}_2[x]$ and hence is maximal. Thus $\mathbb{Z}_2[x]/\langle p(x) \rangle$ is a field. Let $I = \langle x^2 + x + \overline{1} \rangle$. Then

$$\mathbb{Z}_2[x]/I = \{\overline{0}+I, \overline{1}+I, x+I, \overline{1}+x+I\}$$

Thus, $\mathbb{Z}_2[x]/I$ is a field of size 4.

(7) Consider the field $\mathbb{Z}_2$.

Let $p(x) = x^3 + x + \bar{1}$.

Then $p(\bar{0}) = \bar{0}^3 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$

and $p(\bar{1}) = \bar{1}^3 + \bar{1} + \bar{1} = \bar{3} \neq \bar{0}$.

Since degree$(p(x)) = 2$ and $p(x)$ has no zeroes in $\mathbb{Z}_2$ we know that $p(x)$ is irreducible in $\mathbb{Z}_2[x]$. Let $I = \langle x^3 + x + \bar{1} \rangle$. Hence, I is maximal and $\mathbb{Z}_2[x]/I$ is a field.

Also,

$$\mathbb{Z}_2[x]/I = \{\bar{0}+I,\ \bar{1}+I,\ x+I,\ (\bar{1}+x)+I,\ x^2+I,\ (\bar{1}+x^2)+I,\ (x+x^2)+I,\ (\bar{1}+x+x^2)+I\}.$$