SOLUTION TO LECTURE 26 PROBLEMS 103 – 108

$\boxed{P103}$ Check (i) assoc. mult. (ii.) the left dist prop.

$$
\begin{aligned}
(i.)\ [a,b]\big([c,d][e,f]\big) &= [a,b][ce, df] && : \text{def}^{n} \text{ of mult. in } S/\sim \\
&= [a(ce), b(df)] && \text{associativity in integral domain.} \\
&= [(ac)e, (bd)f] \\
&= [ac, bd][e,f] && : \text{def}^{n} \text{ of mult. in } S/\sim \\
&= \big([a,b][c,d]\big)[e,f]. && : \text{def}^{n} \text{ of mult. in } S/\sim
\end{aligned}
$$

$$
\begin{aligned}
(ii.)\ \big([b_1, b_2] + [c_1, c_2]\big)[a_1, a_2] &= \big([b_1c_2 + b_2c_1, b_2c_2]\big)[a_1, a_2] && : \text{def}^{n} \text{ of } + \text{ in } S/\sim \\
&= [(b_1c_2 + b_2c_1)a_1, (b_2c_2)a_2] \\
&= \underline{[b_1c_2a_1 + b_2c_1a_1, b_2c_2a_2]}\ \text{I}
\end{aligned}
$$

Likewise,

$$
\begin{aligned}
[b_1, b_2][a_1, a_2] + [c_1, c_2][a_1, a_2] &= [b_1a_1, b_2a_2] + [c_1a_1, c_2a_2] \\
&= [(b_1a_1)(c_2a_2) + (b_2a_2)(c_1a_1), (b_2a_2)(c_2a_2)] \\
&= [a_2(b_1c_2a_1 + b_2c_1a_1), a_2(b_2c_2a_2)] \\
&= \underline{[b_1c_2a_1 + b_2c_1a_1, b_2c_2a_2]}\ \text{II}
\end{aligned}
$$

Comparing I and II we find the desired left-distributive property.

P104 Let F be a field and $a \in F$ and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $x-a$ is a factor of $f(x)$

$\Rightarrow$ Suppose a is a zero of $f(x) \in F[X]$ where F is a field.
Apply Cor. 3.4.10 we find $f(x) = (x-a)\,q(x) + r(x)$
has $r(x) = f(a)$. But, a a zero means $f(a) = 0$
thus $f(x) = (x-a)\,q(x)$.

$\Leftarrow$ Suppose $f(x) = (x-a)\,g(x)$ then $f(a) = (a-a)\,g(a) = 0$
thus a is a zero of $f(x)$.

P105 Gallian # 20 from p. 279

- find all ring homomorphisms from $\mathbb{Z}_6 \to \mathbb{Z}_6$
- notice #8 guides us, $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ a ring-homomorphism has the form $\phi(x) = ax$ where $a^2 = a$

So what are sol^{n}s to $a^2 = a$ in $\mathbb{Z}_6$?

$$\left.\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 4 \neq 2 \\ 3^2 &= 9 = 3 \\ 4^2 &= 16 = 4 \\ 5^2 &= 25 = 1 \end{aligned}\right\} \quad a = 0,1,3,4 \text{ will do nicely.}$$

$$\left.\begin{aligned} \phi_0(x) &= 0 \\ \phi_1(x) &= x \\ \phi_3(x) &= 3x \\ \phi_4(x) &= 4x \end{aligned}\right\} \quad \boxed{\phi_0, \phi_1, \phi_3, \phi_4 \text{ homomorphisms from } \mathbb{Z}_6 \to \mathbb{Z}_6}$$

P105 continued:

determine ring homomorphisms from $\mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{30}$

Notice $\phi : \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{30}$ a ring homomorphism is an additive homomorphism with added prop. $\phi(xy) = \phi(x)\phi(y)$.

From $\boxed{P72}$ we recall

$$\phi([x]_{20}) = [mx]_{30} \quad \text{where } 30 \mid m(20)$$

For $30 \mid 20m$ we need $20m = 30j$ for some $j \in \mathbb{N}$

$\iff 2m = 3j$ for some $j \in \mathbb{N}$

Hence,
$$\left.\begin{array}{l} m = 3, \ j = 2 \\ m = 6, \ j = 4 \\ m = 9, \ j = 6 \\ m = 12, \ j = 8 \\ m = 15, \ j = 10 \\ m = 18, \ j = 12 \\ m = 21, \ j = 14 \\ m = 24, \ j = 16 \\ m = 27, \ j = 18 \end{array}\right\}$$
$m = 30, \ j = 20$

potential homomorphisms

$$\phi_{3k}(x) = 3kx$$

for $k = 1, 2, 3, \dots, 10$. But, we also need $\forall x, y \in \mathbb{Z}_{20}$,

$$\phi_{3k}(xy) = \phi_{3k}(x)\,\phi_{3k}(y)$$

$$3kxy = (3kx)(3ky)$$

Thus, we need $3k = (3k)^2$ (set $x = y = 1$ for instance)

that is, $3k = 9k^2$ (in $\mathbb{Z}_{30}$)

We find $1, 3, 4, 6, 8, 9$ do not solve $3k = 9k^2 \mod 30$. But $k = 10, 2, 5, 7,$ do solve $3k = 9k^2$

Thus $\boxed{\phi_{30}, \ \phi_6, \ \phi_{15}, \ \phi_{21} \text{ are all the homomorphisms } \phi_m(x) = mx \ \forall x \in \mathbb{Z}_{20}}$

P106 # 40 from p. 280

Show homomorphism from a field onto a ring with more than one element must be isomorphism

Let $\phi: F \longrightarrow R$ be ring homomorphism where F is field and R has more than $0 \in R$. Also we assume $\phi(F) = R$. We have $\phi(0) = 0$ since ϕ is a ring homomorphism. Suppose $\exists\, x \neq y$ in F such that $\phi(x) = \phi(y) \Rightarrow \phi(x) - \phi(y) = 0$ then $\phi(x-y) = 0$ where $x - y \neq 0$ hence $(x-y)^{-1} \in F$ exists and $(x-y)(x-y)^{-1} = 1$

Hence, $\phi(1) = \phi(x-y)\,\phi((x-y)^{-1}) = 0$.

But $\phi(x) = \phi(1 \cdot x) = \phi(1)\phi(x) = 0 \quad \forall x \in F$

So we find $\phi(F) = \{0\} \neq R$. (contradiction)

Therefore, $\nexists\, x \neq y$ such that $\phi(x) = \phi(y)$. In other words, ϕ is injective and as we assumed surjective homomorphism it follows ϕ is an isomorphism of rings.

P107 # 63 p. 281

Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$, $\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$

(a.) $$\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = \phi\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix} \right)$$
$$= (a+c) - (b+d)$$
$$= a - b + c - d$$
$$= \phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) + \phi\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right)$$

$$\phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = \phi\left(\left[\begin{array}{c|c} ac + bd & ad + bc \\ \hline bc + ad & bd + ac \end{array}\right] \right)$$
$$= (ac + bd) - (bc + ad)$$
$$= a(c - d) - b(c - d)$$
$$= (a - b)(c - d)$$
$$= \phi\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) \phi\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix}\right).$$

Thus $\phi : R \longrightarrow \mathbb{Z}$ is ring homomorphism.

(b.) $\text{Ker}\, \phi = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \, a - b = 0 \right\} = \underline{\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| \, a \in \mathbb{Z} \right\}}$.

(c.) Note $a \in \mathbb{Z}$ has $\phi\left(\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\right) = a \therefore \phi(R) = \mathbb{Z}$.

1^{st} isomorphism Th^{m} provides $R/\text{Ker}\,\phi \approx \phi(R) = \mathbb{Z}$.

(d.) Is Ker ϕ a prime ideal? <u>YES</u>, its quotient produces $\mathbb{Z}$ which is an integral domain. (<u>Th^{m} 14.3</u>)

(e.) Ker ϕ is <u>not</u> a maximal ideal since $R/\text{Ker}\,\phi \approx \mathbb{Z}$ and $\mathbb{Z}$ is not a field.

(Th^{m} 14.4)

$\boxed{P108}$ Gallian #12 from pg. 291 | in $\mathbb{Z}_7[x]$,

$$
\begin{array}{r}
4x^2+3x-1 \\
3x^2+2x+1 \overline{\big) 5x^4+3x^3+1} \\
\underline{5x^4+x^3+4x^2} \\
2x^3-4x^2+1 \\
\underline{9x^3+6x^2+3x} \\
-3x^2-3x+1 \\
\underline{-3x^2-2x-1} \\
-x+2
\end{array}
$$

($3\lambda = 5$ for $\lambda = 4$
as $12 = 5 \bmod 7$)

Thus, $5x^4+3x^3+1 = \underbrace{(4x^2+3x-1)}_{q(x)}(3x^2+2x+1) + \underbrace{2-x}_{r(x)}$

quotient *remainder*.