M5420 F15 TEST 4 SOL.

1. (a) x^2+1 irred in $\mathbb{Q}[x]$ (no roots is sufficient to see this)
so $\mathbb{Q}[x]/(x^2+1)$ is a $\boxed{\text{FIELD}}$

(b) $\boxed{\text{Not an Int. Dom}}$: $3 \cdot 5 = 0$ but $3 \neq 0$ and $5 \neq 0$
(Using the iso $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$)
<u>OR</u>: $(1,0)\cdot(0,1) = 0$ but neither factor is 0.

(c) $\mathbb{Z}_3$ is a field (3 is prime)
so $\mathbb{Z}_3[x]$ is an $\boxed{\text{Int Dom}}$, not a field.

(d) x^3+x+1 is reducible since $x=1$ is a root in $\mathbb{Z}_3$
So $\boxed{\text{Not an Int. Dom}}$

~~2. Proof Let F be a field and a,b ∈ F~~

2. Let F be a field and $a, b \in F$, with $ab=0$.
If $a=0$, we're done. If $a \neq 0$ $\exists\, a^{-1} \in F$ and
$b = a^{-1}ab = a^{-1} \cdot 0 = 0.$ //

3. Let $R \xrightarrow{\pi} R/I$ be the projection hom $\pi(x) = x+I$.
If m is an ideal in R/I then $\pi^{-1}(m)$ is an ideal in I s.t. $I \subseteq \pi^{-1}(m) \subseteq R$. Since I is maximal, $\pi^{-1}(m) = I$, so $m=0$, or $\pi^{-1}(m) = R$, so $m = R/I$.
Thus R/I has no non-trivial proper ideals, and hence, is a field.

3. (alt. proof.)

Suppose $x+I \neq 0+I$ in R/I. That is, $x \notin I$. Then $(x)+I$ is an ideal of R with

$$I \subseteq (x)+I \subseteq R.$$

Since I is maximal, $(x)+I = I$ or $(x)+I = R$. But $x \notin I$ so $(x)+I \neq I$. Therefore $1 \in R$ can be written as $1 = a+b$ with $a = rx$ for some r and $b \in I$. Then

$$\begin{aligned}(r+I)(x+I) &= rx+I \\ &= (rx+b)+I \\ &= 1+I\end{aligned}$$

so $(x+I)^{-1} = r+I$. Thus R/I is a field. //

(See next page for another proof.)

4. To find the multiplicative inverse, we can use the Euclidean algorithm

$$x^3+x+1 = (x+1)(x^2+x) + 1$$

$$\begin{array}{r|l} & \quad x^2+x \\ \hline x+1 & x^3 \qquad +x+1 \\ & x^3+x^2 \\ \hline & \quad x^2+x+1 \\ & \quad x^2+x \\ \hline & \qquad\quad +1 \end{array}$$

So $1 = (x+1)(x^2+x) + (x^3+x+1)$

$\equiv (x+1)(x^2+x)$

mod (x^3+x+1)

Thus $(x+1)^{-1} = x^2+x$.

<u>Alt proof</u>:

$x^1 = x$

$x^2 = x^2$

$x^3 = x+1$

$\cancel{x^4}$

Since $\mathbb{Z}_2[x]/(x^3+x+1)$ has 8 elements, its mult. group $(\quad)^\times$ has 7 elements, so $x^7 = 1$.

Hence $(x+1)x^4 = x^3x^4 = 1$

so $x^4 = (x+1)^{-1}$.

<u>2nd alt proof</u>: continue on:

$x^4 = x^2+x$

$x^5 = x^3+x^2 = x^2+x+1$

$x^6 = x^3+x^2+x = x+1+x^2+x = x^2+1$

$x^7 = x^3+x = 1$

So $x^4 = x^2+x$ is $(x+1)^{-1} = (x^3)^{-1}$.

5. $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}_6 \oplus \mathbb{Z}_9$ $\qquad \phi(1) = (1,1)$

Now $\phi(k) = (k,k) = (0,0)$ iff $k \equiv 0 \ (6)$
and $k \equiv 0 \ (9)$

This is equivalent to $k \equiv 0 \ (\operatorname{lcm}(6,9) = 18)$.

So $\boxed{\operatorname{Ker}(\phi) = (18)}$, the principal ideal gen by 18.

The $\boxed{\text{image is isomorphic to } \mathbb{Z}_{18}}$.

As a subset of $\mathbb{Z}_6 \oplus \mathbb{Z}_9$, it is

0,0	0,6	0,3
1,1	1,7	1,4
2,2	2,8	2,5
3,3	3,0	3,(
4,4	4,1	4,
5,5	5,2	5,