Thursday 11/21/19.

Q3 a.

We have a ring hom $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}$

$$f(x) \longmapsto f(7).$$

$\ker\varphi = (x-7)$ by the division algorithm.

φ is clearly surjective.

So $\mathbb{Z}[x]/(x-7) \xrightarrow{\sim} \mathbb{Z}$ by F.I.T.

b.

Consider the ring hom $\varphi: \mathbb{R}[x] \longrightarrow \mathbb{C}$

$$f(x) \longmapsto f(3i)$$

<u>Claim</u>: $\ker\varphi = (x^2+9)$:-

$f(3i) = 0 \Rightarrow 0 = \overline{f(3i)} = f(\overline{3i}) = f(-3i)$

So $f(x) = (x-3i)(x+3i)\cdot g(x) = (x^2+9)\cdot g(x)$, some $g(x) \in \mathbb{R}[x]$.

(Conversely $x^2+9 \in \ker\varphi$ ✓). $\square$ for Claim.

Now φ surjective $\Rightarrow$ $\mathbb{R}[x]/(x^2+9) \xrightarrow{\sim} \mathbb{C}$ by F.I.T. $\square$.

c. $\mathbb{Q}[x]/(x^2+5x-14) = \mathbb{Q}[x]/((x+7)(x-2)) \underset{CRT}{\cong} \mathbb{Q}[x]/(x+7) \times \mathbb{Q}[x]/(x-2)$

coprime in $\mathbb{Q}[x]$

$\cong \mathbb{Q} \times \mathbb{Q}$

$(f,g) \longmapsto (f(-7), g(2))$ cf. Q3a.

d. $\mathbb{Z}[i]/(3+4i) \cong \left(\mathbb{Z}[x]/(x^2+1)\right)/(3+4x)$

$= \mathbb{Z}[x]/(x^2+1, 3+4x) = \mathbb{Z}/25\mathbb{Z}[x]/(3+4x) = \mathbb{Z}/25\mathbb{Z}[x]/(x-18) \simeq \mathbb{Z}/25\mathbb{Z}$ $\square$.

$-6\cdot 4 = 1 \bmod 25$

$4^2(x^2+1) = (4x+3)(4x-3) + 25$

$\rightsquigarrow 25 \in (x^2+1, 3+4x)$, & $(x^2+1, 3+4x) = (25, 3+4x)$

(note $\gcd(4^2, 25) = 1$)

e. $\mathbb{Z}[x]/(6,2x-1) = \mathbb{Z}[x]/(3,2x-1) = \mathbb{Z}/3\mathbb{Z}[x]/(2x-1) = \mathbb{Z}/3\mathbb{Z}[x]/(x-2) \simeq \mathbb{Z}/3\mathbb{Z}.$

$2\cdot 2 = 1 \bmod 3$

$3\cdot(2x-1) = 6x-3$

$\Rightarrow (6,2x-1) = (3,2x-1)$

f. $\mathbb{Z}[x]/(2x^2-4,\,4x+5)$ $\cancel{= \mathbb{Z}/7\mathbb{Z}[x]/(2x^2-4,\,4x+5)}$ $= \mathbb{Z}/7\mathbb{Z}[x]/(x+3) \simeq \mathbb{Z}/7\mathbb{Z}.$ □

$2\cdot(2x^2-4) = x(4x+5) + (-5x-8)$

$= (x-1)(4x+5) + (-x-3)$

$(4x+5) = 4\cdot(x+3) - 7$

$\Rightarrow$ $\cancel{7 \in (2x^2-4,\,4x+5)}$

$(2x^2-4,\,4x+5) = (x+3,\,7)$

(note $\gcd(2,7)=1$)

g. $\mathbb{Z}[x]/(x^2-3,\,2x-4) = \frac{\mathbb{Z}[x]}{2\mathbb{Z}}/(x^2+1) = \mathbb{Z}/2\mathbb{Z}[x]/((x+1)^2)$

$\simeq \mathbb{Z}/2\mathbb{Z}[t]/(t^2)$

$4\cdot(x^2-3) = (2x-4)(2x+4) + 4.$

Better $2\cdot(x^2-3) = (2x-4)(x+2) + 2.$

$\Rightarrow (x^2-3,\,2x-4) = (2,\,x^2+1)$

h. $\mathbb{Z}[x]/(x^2+3,\,5) = \mathbb{Z}/5\mathbb{Z}[x]/(x^2+3)$

x^2+3 is irred. mod 5 (squares mod 5 are $0,1,4$, $\neq 2$, so x^2+3 has no roots mod 5)

So $\mathbb{Z}/5\mathbb{Z}[x]/(x^2+3)$ is a field (because $(x^2+3) \subset \mathbb{Z}/5\mathbb{Z}[x]$ is maximal) of order $5^2 = 25$ by the division algorithm.

4b. $$\begin{aligned} \psi : \mathbb{C}[x,y] &\longrightarrow \mathbb{C}[t] \\ x &\longmapsto t^2-1 \\ y &\longmapsto t\cdot(t^2-1) \end{aligned}$$

Note $y^2 - x^2(x+1) \in \ker\psi$:

$$y^2 - x^2(x+1) \longmapsto t^2\cdot(t^2-1)^2 - (t^2-1)^2(t^2-1+1) = 0 \checkmark$$

<u>Claim</u> $\ker\psi = (y^2 - x^2(x+1))$.

<u>Proof</u>: suppose $f \in \ker\psi$; write $f = q\cdot(y^2-x^2(x+1)) + r$, $q, r \in \mathbb{C}[x,y] = (\mathbb{C}[x])[y]$,

$r = 0$ or $\deg_y r < \deg_y(y^2 - x^2(x+1)) = 2$

by the division algorithm.

So $r = a(x)\cdot y + b(x)$, $a, b \in \mathbb{C}[x]$.

$f, y^2 - x^2(x+1) \in \ker\psi \Rightarrow r \in \ker\psi$

i.e. $\underbrace{a(t^2-1)\cdot t(t^2-1)}_{\text{odd powers of } t} + \underbrace{b(t^2-1)}_{\text{even powers of } t} = 0.$

$\Rightarrow a(x) = b(x) = 0 \Rightarrow r = 0 \Rightarrow y^2 - x^2(x+1) \mid f$, $\square$ for Claim.

So by FIT $$\mathbb{C}[x,y]/(y^2 - x^2(x+1)) \xrightarrow{\sim} \psi(\mathbb{C}[x,y]) \subset \mathbb{C}[t]$$
$$\psi(\mathbb{C}[x,y]) = \mathbb{C}[t^2-1, t\cdot(t^2-1)]$$

We have $\psi(\mathbb{C}[x,y]) = \{ g \in \mathbb{C}[t] \mid g(1) = g(-1) \}$:-

$\subset$ ✓

$\supset$: Say $g(1) = g(-1) = c \in \mathbb{C}$.

Then $g(t) - c = (t^2-1)\cdot h(t) \Rightarrow g(t) \in \psi(\mathbb{C}[x,y])$ $\square$.

$t^{2k} = ((t^2-1)+1)^k$, $t^{2k+1} = t\cdot t^{2k}$

5.

If $I = (n)$, $n \in \mathbb{Z}$, then $\mathbb{Z}[x]/(n) = \mathbb{Z}/n\mathbb{Z}[x]$, not a field,

so I is not maximal.

If $I = (f)$, $\deg f > 0$, $f = \overset{0}{\underset{\#}{a_n}}x^n + \dots + a_1 x + a_0$,

pick $p \in \mathbb{N}$ prime s.t. $p \nmid a_n$.

Then $(f) \subsetneq (p, f)$ & $\mathbb{Z}[x]/(p,f) = \mathbb{Z}/p\mathbb{Z}[x]/(\bar{f}) \neq (0)$,

so $I = (f)$ is not maximal. $\square$.

7.

$(a,b) \in \underset{\text{ideal}}{K} < R \times S \implies (a,0) = (1,0)\cdot(a,b) \in K$

& $(0,b) = (0,1)\cdot(a,b) \in K$

And conversely $(a,0), (0,b) \in K \implies (a,b) = (a,0) + (0,b) \in K$.

Thus $K = I \times J$ where $I = \{a \in R \mid (a,0) \in K\}$

$J = \{b \in S \mid (0,b) \in K\}$

Conversely, if $I, J < R, S$ ideals, then $K := I \times J < R \times S$ is an ideal ✓.

(closed under scalar mult, & subgroup under +.) $\square$

9.

Let $\varphi : \mathbb{Z} \to R$ be the canonical homomorphism

As an abelian group, $(R, +) \simeq \mathbb{Z}/15\mathbb{Z}$ (an (abelian) group of order 15 is cyclic)

~~Then~~ We claim: $\ker\varphi = 15\mathbb{Z}$, then $\mathbb{Z}/15\mathbb{Z} \xrightarrow{\sim} \varphi(\mathbb{Z}) < R$ by FIT, so φ is surjective

& $\mathbb{Z}/15\mathbb{Z} \xrightarrow{\sim} R$ as rings.

~~Indeed~~ To show the claim, let $\ker\varphi = n\mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \varphi(\mathbb{Z}) < R$ & $n \mid 15$. by Lagrange.

Writing g for a generator of $(R,+) \simeq \mathbb{Z}/15\mathbb{Z}$, we have $n \cdot g = \underbrace{g + \dots + g}_{n} = \underbrace{(1 + \dots + 1)}_{n} \cdot g = \varphi(n)\cdot g = 0$

so $15 \mid n$. Thus $n = 15$. $\square$.

Q10. a.

R commutative

$$F(ab) = (ab)^p = a^p b^p = F(a)F(b)$$

$$F(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i \cdot b^{p-i} = a^p + b^p$$

Binomial theorem is valid in a commutative ring.

because $p \mid \binom{p}{i}$ for $0<i<p$ & $p=0$ in R.

b. $R = \mathbb{Z}/_{p\mathbb{Z}}[x]$

$$f = \sum_{i=0}^{n} a_i x^i \in R.$$

$$F(f) = f^p = \left(\sum_{i=0}^{n} a_i x^i\right)^p = \sum_{i=0}^{n} a_i^p (x^i)^p = \sum_{i=0}^{n} a_i x^{pi} \quad \square.$$

$a^p = a$ for $a \in \mathbb{Z}/_{p\mathbb{Z}}$.

11. a. $(1+a)\cdot(1-a+a^2-\dots+(-a)^{n-1}) = 1 \pm a^n = 1 + (-1)^{n-1} a^n = 1$

if $a^n = 0$. $\square$

b. $0 \in N$ ✓

$a, b \in N \Rightarrow \exists\, n \in \mathbb{N}.\ a^n = b^n = 0$

$$\Rightarrow (a+b)^{2n-1} = \sum_{i=0}^{2n-1} \binom{2n-1}{i} a^i b^{2n-1-i} = 0.$$

$\Rightarrow (a+b) \in N.$

$a \in N$, $r \in R$ $\Rightarrow$ $ra \in N$: say $a^n = 0$, then $(ra)^n = r^n a^n = 0$.

Thus N is an ideal.

c. Let $\bar{a} \in R/_N$. If $\bar{a}$ is nilpotent, $\bar{a}^n = 0$, some $n \in \mathbb{N}$.

$\bar{a} = a+N$ i.e. $a^n \in N$, so $(a^n)^m = 0$, some $m \in \mathbb{N}$.

So $a^{nm} = 0$, $a \in N$, $\bar{a} = 0$. $\square$.

12. $\varphi: \mathbb{Z} \to F$ the canonical hom.

F field $\Rightarrow$ F integral domain $\Rightarrow$ $\ker\varphi = (0)$ or (p), $p \in \mathbb{N}$ prime.

(Proof: by FIT $\mathbb{Z}/\ker\varphi \hookrightarrow F$, so $\mathbb{Z}/\ker\varphi$ is an integral domain,

& $\ker\varphi = (n)$ $\Rightarrow$ $n = 0$ or p, prime.)

If $\ker\varphi = (p)$ then $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$, $F_0 = \mathbb{Z}/p\mathbb{Z}$

Otherwise $\mathbb{Z} \overset{\varphi}{\hookrightarrow} F$ $\rightsquigarrow$ $\mathbb{Q} = ff(\mathbb{Z}) \hookrightarrow F$ by universal property
$a/b \mapsto \varphi(a)\cdot\varphi(b)^{-1}$ of fraction field,

& $\mathbb{Q} = F_0$. $\square$.

13. (a) Maximal ideals in $\mathbb{Z}/n\mathbb{Z}$ $\leftrightarrow$ maximal ideals in $\mathbb{Z}$ containing $n\mathbb{Z}$
$= \{(p) \mid p \mid n,\ p \text{ prime}\}$

So $\mathbb{Z}/n\mathbb{Z}$ local $\Leftrightarrow$ $n = p^\alpha$, p prime.

(b) R local, maximal ideal M.

<u>Claim</u>: $R^\times = R \setminus M$.

<u>Proof</u>: $a \in R^\times$ $\Leftrightarrow$ $(a) = R$ $\Rightarrow$ $a \notin M$ (otherwise $(a) < M$)

Conversely, suppose $a \notin M$. ~~$\exists$ maximal~~ If $(a) \neq R$ then $\exists$ maximal ideal M' s.t. $(a) < M'$ (any proper ideal of a ring R is contained in a maximal ideal). R local $\Rightarrow$ $M' = M$ $\Rightarrow$ $a \in M$ #. So $(a) = R$, $a \in R^\times$. $\square$

(c) If $I \subsetneq J < R$ ideal then $J \cap R\setminus I \neq \emptyset$, so J contains a unit by our assumption, & so $J = R$. Thus I is maximal.
Similarly if $J < R$ ideal, $J \not< I$, then $J = R$. So I is the unique maximal ideal, &

R is local. $\square$

14. a. We use 6.13c.

Let $f = a_0 + a_1 x + a_2 x^2 + \ldots \in \mathbb{C}[[x]] \setminus (x)$,

i.e. $a_0 \neq 0$.

We show f is a unit:

want to find $g = b_0 + b_1 x + b_2 x^2 + \ldots \in \mathbb{C}[[x]]$ s.t.

$$f \cdot g = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots$$
$$= 1 + 0 \cdot x + 0 \cdot x^2 + \ldots$$
$$= 1$$

i.e. $a_0 b_0 = 1$, $a_0 b_1 + a_1 b_0 = 0$, ..

Can solve inductively for $b_0, b_1, b_2, \ldots$ using $\underset{\mathbb{C}}{\overset{}{a_0}} \neq 0$. $\square$

b.

If $f \in \mathbb{C}[[x]]$, $f = \underset{\neq 0}{a_k} x^k + a_{k+1} x^{k+1} + \ldots$

$$= x^k \cdot \underbrace{(a_k + a_{k+1} x + \ldots)}_{\text{unit by a}}$$

So $(f) = (x^k)$

Similarly, $\underset{= (x^{k_\alpha} \mid \alpha \in A)}{(f_\alpha \mid \alpha \in A)} = (x^k)$ where $k = \min_{\alpha \in A} k_\alpha$

So the ideals of $\mathbb{C}[[x]]$ are (x^k), $k \in \mathbb{Z}_{\geq 0}$ & (0).

c. $a, b \in \mathbb{C}[[x]]$, $b \neq 0$.

Then $\frac{a}{b} = \frac{a}{u \cdot x^k} = c \cdot x^{-k}$, $c \in \mathbb{C}[[x]]$. Thus ff $\mathbb{C}[[x]]$ is the ring of formal Laurent series. $\square$

(u: unit)