Please show your work and use words to explain your steps where appropriate.

Problem 1 (10pts) Let D be an integral domain with $a, b, c \in D$. Prove that if $a \neq 0$ and $ab = ac$ then $b = c$.

Suppose $a \neq 0$ and $ab = ac$ for some $a, b, c \in D$ an $\int$-domain. Observe $ab - ac = 0$ hence $a(b-c) = 0$. Since $a \neq 0$ we find $b - c \neq 0 \Rightarrow b - c$ is a zero divisor. But, D has no zero-divisors $\therefore b - c = 0$ whence, $\underline{b = c}$.

Problem 2 (10pts) Let $\langle a, b\rangle = \{ra + sb \mid r, s \in R\}$ where R is a ring and $a, b \in R$. Prove $\langle a, b\rangle$ forms an ideal of R.

Let $x, x' \in \langle a,b\rangle$ hence $x = ra + sb$ and $y = r'a + s'b$ for $r, s, r', s' \in R$. Note $x - x' = ra + sb - (r'a + s'b) = (r-r')a + (s-s')b \in \langle a,b\rangle$ as $r - r', s - s' \in R$ once more since R is a ring. Next, suppose $\lambda \in R$ then $\lambda x = \lambda(ra + sb) = (\lambda r)a + (\lambda s)b \in \langle a,b\rangle$ as $\lambda r, \lambda s \in R$ as R is closed under multiplication. Finally note $\langle a, b\rangle \neq \emptyset$ as $a, b \in R$ hence $aa + ab \in \langle a,b\rangle$ etc. In summary, $\langle a,b\rangle$ forms an ideal. -(using Th$^{\underline{m}}$ 3.2.2)-

Problem 3 (10pts) Let $R = \langle 3, x\rangle$ where $x \in \mathbb{N}$. Prove that either $R = \langle 3\rangle$ or $R = \mathbb{Z}$.

Notice $\mathbb{Z}/\langle 3\rangle = \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$ is a field hence $\langle 3\rangle$ is a maximal ideal. Since $\langle 3\rangle \subset \langle 3, x\rangle$ we find $\langle 3, x\rangle = \langle 3\rangle$ or $\langle 3, x\rangle = \mathbb{Z}$ by maximality.

(can also prove by detailed gcd-type argument)(but, ↑ easier)

Problem 4 (10pts) Let R be a ring and A an ideal of R. Prove that $(x + A)(y + A) = xy + A$ provides a well-defined operation on $R/A = \{x + A \mid x \in R\}$.

Suppose $x + A = x' + A$ and $y + A = y' + A$ thus $x - x', y - y' \in A$.
Note,

$$(x'+A)(y'+A) = x'y' + A \quad \text{whereas} \quad (x+A)(y+A) = xy + A$$

we need $x'y' + A = xy + A$. Use the uber-closure of A to see that:

$$x'y' - xy = \underbrace{(x'-x)y'}_{\in A} - \underbrace{x(y-y')}_{\in A} \in A \quad \therefore \quad \underline{x'y' + A = xy + A}.$$

Problem 5 (10pts) Give an example of a field with 25 elements.

Consider x^2+x+1 in $\mathbb{Z}_5[x]$. Set $x=0,1,2,3,4$ and observe none give $x^2+x+1=0$ $\Rightarrow$ $x^2+x+1 \in \mathbb{Z}_5[x]$ is irreducible

$\therefore$ $\mathbb{Z}_5[x]/\langle x^2+x+1\rangle$ forms field and $\underbrace{\dfrac{\mathbb{Z}_5[x]}{\langle x^2+x+1\rangle} \approx \left\{a+b\alpha \;\middle|\; \begin{matrix}\alpha^2+\alpha+1=0\\ a,b\in\mathbb{Z}_5\end{matrix}\right\}}_{\text{field with 25-elements.}}$

Problem 6 (10pts) Is $\mathbb{R}[x]/\langle x^2-3\rangle$ a field ? Explain.

Notice $x^2-3 = (x-\sqrt{3})(x+\sqrt{3})$

hence $\underbrace{(x-\sqrt{3}+\langle x^2-3\rangle)(x+\sqrt{3}+\langle x^2-3\rangle)}_{\text{ZERO DIVISORS !}} = x^2-3+\langle x^2-3\rangle = \langle x^2-3\rangle.$

$\therefore$ $\dfrac{\mathbb{R}[x]}{\langle x^2-3\rangle}$ not a field.

Problem 7 (10pts) Show that $i+\sqrt{2}$ is algebraic over $\mathbb{R}$.

$$\alpha = i+\sqrt{2} \Rightarrow \alpha-\sqrt{2} = i$$
$$\Rightarrow \alpha^2-2\alpha\sqrt{2}+2 = -1$$
$$\Rightarrow \alpha^2-2\alpha\sqrt{2}+3 = 0$$

Observe $P(x) = x^2-2x\sqrt{2}+3 \in \mathbb{R}[x]$ and $P(\alpha)=0$

thus $\alpha = i+\sqrt{2}$ is algebraic over $\mathbb{R}$.

Problem 8 (15pts) Explain why the following polynomials are irreducible over $\mathbb{Q}$,

(a.) $x^5+10x^4+15x^2+20$

observe $5|10$, $5|15$, $5|20$ yet $5^2 \nmid 20$

thus $x^5+10x^4+15x^2+20$ is irred. over $\mathbb{Q}$ by Eisenstein's Criterion.

(b.) x^3+x+1

Modulo 2, $0^3+0+1=1$, $1^3+1+1=1$ thus $\overline{P(x)} = x^3+x+1$ is irred. in $\mathbb{Z}_2[x]$

Thus x^3+x+1 is irred. over $\mathbb{Q}$.

Problem 9 (10pts) Find the degree of $\alpha=\sqrt[5]{2}$ over $\mathbb{Q}$ and find a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

$\operatorname{irr}(\sqrt[5]{2},\mathbb{Q}) = x^5-2$ by Eisenstein with $P=2$.

$\mathbb{Q}(\alpha) = \{a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4 \mid a,b,c,d,e\in\mathbb{Q}\}$

basis $\underline{\{1, \sqrt[5]{2}, 2^{2/5}, 2^{3/5}, 2^{4/5}\} = \{1, \sqrt[5]{2}, \sqrt[5]{4}, \sqrt[5]{8}, \sqrt[5]{16}\}}$.

Problem 10 (20pts) Let R be a commutative ring with unity and let A be an ideal of R. Prove the quotient ring R/A is an integral domain if and only if A is a prime ideal.

Observe R/A is an factor ring as A ideal. Observe $(1+A)(x+A) = x+A$ for all $x+A \in R/A$ hence $1+A$ is the identity in R/A. We also know $A + (x+A) = x+A$ $\forall x+A \in R/A$ thus A is the zero in R/A.

$\Rightarrow$] R/A is an integral domain. Let $a, b \in R$ and $ab \in A$ consider $(a+A)(b+A) = ab + A = A \Rightarrow a+A = A$ or $b+A = A$ as R/A has no zero-divisors. Consequently $a \in A$ or $b \in A$ hence A is a prime ideal.

$\Leftarrow$] Suppose A is a prime ideal. Notice R/A is a ring with unity $1+A$ and zero A. Moreover $\frac{R}{A}$ is commutative ring. It remains to show R/A has no zero-divisors. Consider, $(a+A)(b+A) = A$ hence $ab + A = A \Rightarrow ab \in A \Rightarrow a \in A$ or $b \in A$ as A prime. Thus $a+A = A$ or $b+A = A$ $\therefore$ R/A is integral domain.//

Problem 11 (10pts) Let F be a field and suppose $p(x) \in F[x]$ is irreducible. Prove $\langle p(x) \rangle$ is a maximal ideal.

Consider I an ideal of $F[x]$ for which $\langle p(x) \rangle \subseteq I \subseteq F[x]$.

Note, F a field $\Rightarrow F[x]$ is a PID $\therefore \exists g(x) \in F[x]$ for which $I = \langle g(x) \rangle$. Consider then $\langle p(x) \rangle \subseteq I = \langle g(x) \rangle$ implies $p(x) \in \langle g(x) \rangle$ $\therefore \exists k(x) \in F[x]$ s.t. $p(x) = k(x)\, g(x)$.

Note, $p(x)$ irreducible and $p(x) = k(x)\, g(x)$ implies ~~at~~ least that either $k(x)$ or $g(x)$ is a unit in $F[x]$.

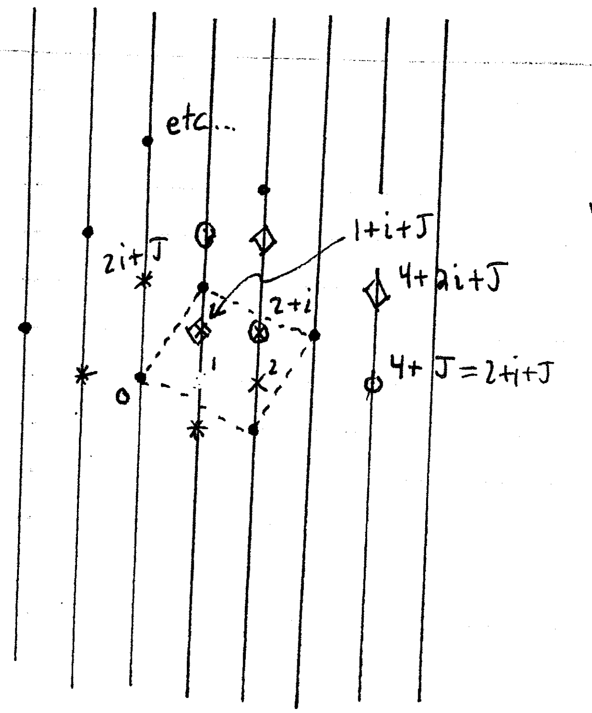
1.) if $k(x) \in U(F[x]) = F^{\times}$ then $k(x) = c \neq 0$, $c \in F$ hence $p(x) = c\, g(x)$ or $g(x) = \frac{1}{c} p(x) \Rightarrow g(x) \in \langle p(x) \rangle$ and we find $\langle p(x) \rangle = \langle g(x) \rangle = I$. -(associates $p(x)$, $g(x)$ generate same ideal)-

2.) if $g(x) \in F^{\times}$ then $g(x) = c \neq 0$, $c \in F$ and $1 = \left(\frac{1}{c}\right) c \in \langle g(x) \rangle \Rightarrow \langle g(x) \rangle = F[x]$ $\therefore$ $I = F[x]$

In conclusion, $p(x)$ irred. over F implies $\langle p(x) \rangle$ is maximal.//

$(1+i)(2+i) = 2+3i-1 = 1+3i \qquad (1+i)(1+i) = 1+2i-1 = 2i$

Problem 12 (15pts) Consider $J = \langle 1+2i \rangle$ in $\mathbb{Z}[i]$. How many elements are in $\mathbb{Z}[i]/J$? Make a multiplication table for the units in $\mathbb{Z}[i]/J$ and identify which group is isomorphic to the group of units in $\mathbb{Z}[i]/J$.



Since $\mathbb{Z}[i]$ is integral domain we have $\langle 1+2i \rangle = \langle \alpha \rangle$ for $\alpha = -1-2i,\ i-2,\ -i+2$

$$\boxed{\mathbb{Z}[i]/J = \{J,\ 1+J,\ 2+J,\ 1+i+J,\ 2+i+J\}}$$

$\boxed{5-\text{elements.}}$

$U(\mathbb{Z}[i]/J)$	$1+J$	$2+J$	$1+i+J$	$2+i+J$
$1+J$	$1+J$	$2+J$	$1+i+J$	$2+i+J$
$2+J$	$2+J$	$2+i+J$	$1+J$	$1+i+J$
$1+i+J$	$1+i+J$	$1+J$	$2+i+J$	$2+J$
$2+i+J$	$2+i+J$	$1+i+J$	$2+J$	$1+J$

(Sorry so slanted)

$U(5)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$1 \longleftrightarrow 1+J$
$2 \longleftrightarrow 2+J$
$3 \longleftrightarrow 1+i+J$
$4 \longleftrightarrow 2+i+J$

$\boxed{\text{isomorphic to } U(5)}$

Problem 13 (20pts) Define $\psi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}$ by $\psi(f(x)) = (f(1), f(-1))$. You are given ψ is a ring homomorphism.

(a.) Show that Ψ is a surjection.

(b.) Calculate Ker(Ψ).

(c.) Is Ker(Ψ) a prime ideal of $\mathbb{Q}[x]$? Explain.

(a.) Let $(m,n) \in \mathbb{Q} \times \mathbb{Q}$ and consider $f(x) = a + bx \in \mathbb{Q}[x]$

note $f(1) = a+b$ and $f(-1) = a-b$ hence we need to solve

$$\begin{aligned} a+b &= m \\ a-b &= n \end{aligned} \implies \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} m \\ n \end{bmatrix} \therefore \begin{bmatrix} a \\ b \end{bmatrix} = \frac{-1}{2}\begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} m \\ n \end{bmatrix}$$

set $a = \frac{1}{2}(m+n)$ and $b = \frac{1}{2}(m-n)$ and observe

$$f(1) = \tfrac{1}{2}(m+n) + \tfrac{1}{2}(m-n) = m$$
$$f(-1) = \tfrac{1}{2}(m+n) - \tfrac{1}{2}(m-n) = n$$

$\therefore f$ is a surjection as $f(x) = \frac{1}{2}(m+n) + \frac{1}{2}(m-n)x \in \mathbb{Q}[x]$ maps to $(m,n) \in \mathbb{Q} \times \mathbb{Q}$ under $\psi(f(x)) = (f(1), f(-1))$.

Continued

(b.) Calculate $\mathrm{Ker}(\psi)$ for $\psi : \mathbb{Q}[x] \longrightarrow \mathbb{Q} \times \mathbb{Q}$ where $\psi(f(x)) = (f(1), f(-1))$

$f(x) \in \mathrm{Ker}(\psi) \Rightarrow f(1) = 0$ and $f(-1) = 0$

$\Rightarrow x-1$ and $x+1$ are factors of $f(x)$; $f(x) = (x-1)(x+1)\, g(x)$ for some $g(x) \in \mathbb{Q}[x]$

Consequently, $\boxed{\mathrm{Ker}(\psi) = \langle (x-1)(x+1) \rangle = \langle x^2 - 1 \rangle.}$

(c.) Observe $\mathbb{Q} \times \mathbb{Q}$ is <u>not</u> an integral domain as $(1,0)(0,1) = (0,0)$ yet $(1,0), (0,1) \neq (0,0)$

Consequently, as the 1st isomorphism Th$^{\underline{m}}$ for rings provides

$$\mathbb{Q}[x] / \mathrm{Ker}\,\psi \approx \psi(\mathbb{Q}[x]) \overset{\text{part (a.)}}{=} \mathbb{Q} \times \mathbb{Q}$$

$$\Rightarrow \mathbb{Q}[x] / \langle x^2 - 1 \rangle \approx \mathbb{Q} \times \mathbb{Q}$$ ← not an integral domain

$\therefore$ <u>$\langle x^2 - 1 \rangle = \mathrm{Ker}\,\psi$ is not a prime ideal</u>.

In particular $(x+1)(x-1) \in \langle x^2 - 1 \rangle$ but neither $x+1$ nor $x-1$ is in $\langle x^2 - 1 \rangle$.