LSU Algebra Test Bank Soln

Rings

Modules

Linear Alg.

R7. Show that $\mathbb{Z}[i]/\langle 1+i\rangle$ is isomorphic to $\mathbb{F}_2$.

Soln: Let $\varphi : \mathbb{Z}[i] \to \mathbb{F}_2$ be the morphism $\varphi(a+ib) = a+b \pmod 2$

$a+ib \mapsto a+b$

$\varphi((a+ib)(c+id)) = \varphi(ac-bd+i(ad+bc)) = ac-bd+ad+bc \pmod 2 = ac+bd+ad+bc \pmod 2$

$\varphi(a+ib)\,\varphi(c+id) = (a+b)(c+d) \pmod 2$

Claim: $\ker\varphi = \langle 1+i\rangle$

$1+i \in \ker\varphi$. Let $a+ib \in \ker\varphi \Rightarrow a+b \equiv 0 \pmod 2$

$a+ib = 2(x+iy) + a'+b'i$ where $a', b' \in \{0,1\}$

$a+b \equiv 0 \pmod 2 \Leftrightarrow a'+b' \equiv 0 \pmod 2$

$a'=1 \Rightarrow b'=1$, $a'=0 \Rightarrow b'=0$ $\Rightarrow a+ib = 2(x+iy)$ or $2(x+iy)+(1+i)$

$(1+i) \mid 2 \Rightarrow a+ib \in \langle 1+i\rangle \Rightarrow \ker\varphi = \langle 1+i\rangle$

By First Isomorphism Theorem: $\dfrac{\mathbb{Z}[i]}{\langle 1+i\rangle} \cong \mathbb{F}_2$

R8. Consider $\mathbb{Z}[x]$

(a) Find all units of $\mathbb{Z}[x]$.

Let $f(x)\,g(x) = 1$ Since $\mathbb{Z}$ is integral domain $\Rightarrow \deg(f), \deg(g) = 0$

$\Rightarrow f, g$ are constant polynomial

This implies units of $\mathbb{Z}[x]$ = units of $\mathbb{Z} = \{\pm 1\}$

(b) Describe an easy way to recognize the elements of $I = \langle 2, x \rangle$

$f(x) \in (2, x) \Rightarrow f(x) = 2g(x) + x\,h(x)$

Let $g(x) = a_0 + a_1 x + \cdots + a_n x^n \Rightarrow f(x) = 2a_0 + x(h(x) + a_1 + a_2 x + \cdots + a_n x^{n-1})$

ie. constant term of $f(x)$ is even. Inverse is also true.

So, elements of I have even constant term.

(c) Find prime ideal of $\mathbb{Z}[x]$ that is not maximal.

(x) is prime ($\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ I.d)

$(x) \subsetneq (2, x)$. So (x) is not maximal.

Q9. Find all irreducible polynomial of degree 4 over $\mathbb{F}_2$.

Sol^n: If $f(x)$ is a reducible poly. of degree 4, either f has a root or it is a product of 2 degree 2 irreducible poly.

Irr. poly of degree 2 : x^2+x+1. (it has no root $\Rightarrow$ irr)

So, Let $f(x)$ be irr. poly of deg 4 $\Rightarrow f(x) = x^4+ax^3+bx^2+cx+d$

$f(x)$ has no root $\Rightarrow f(0) \neq 0 \Rightarrow d = 1$

$f(1) \neq 0 \Rightarrow 1+a+b+c+1 = 1 \rightarrow a+b+c = 1$

and $f(x) \neq (x^2+x+1)^2 = x^4+x^2+1$

All possible combination of (a,b,c) with $a+b+c=1$ & $(a,b,c) \neq (0,1,0)$

are : $(1,1,1) \rightarrow x^4+x^3+x^2+x+1$

$(1,0,0) \rightarrow x^4+x^3+1$

$(0,0,1) \rightarrow x^4+x+1$

R.10. $R = \mathbb{Z}[\sqrt{-10}]$

(a) Show R is not PID.

$10 = 2 \cdot 5 = -(\sqrt{-10})(\sqrt{-10})$ where each element is irreducible.
So, R is not UFD $\Rightarrow$ not PID.

(b) Let $P = \langle 7, 5+\sqrt{-10} \rangle$. Show that $R/P \cong \mathbb{F}_7$

Let $\varphi : R \to \mathbb{F}_7$ be a homomorphism
$a+b\sqrt{-10} \mapsto a+2b \pmod 7$

$(a+b\sqrt{-10})(c+d\sqrt{-10})$
$= (ac - 10bd + \sqrt{-10}(ad+bc))$
$ac-10bd+(\sqrt{-10})(ad+bc) \mapsto$
$= ac+4bd+2(ad+bc) \pmod 7$
$= (a+2b)(c+2d) \pmod 7$

Claim: $\ker \varphi = P$

$P \subseteq \ker \varphi$ trivial.

Let $a+b\sqrt{-10} \in \ker \varphi \Rightarrow a+2b \equiv 0 \pmod 7$
$a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + a'+b'\sqrt{-10}$ where $a', b' \in \{0, 1, \cdots, 6\}$

Checking all the possibilities:

$(a',b') = (0,0)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) \in P$
$(a',b') = (5,1)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + (5+\sqrt{-10}) \in P$
$(a',b') = (3,2)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + 3+2\sqrt{-10} = 7(x'+y') + 2(5+\sqrt{-10}) \in P$
$(a',b') = (1,3)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + 1+3\sqrt{-10} = 7(x'+y'\sqrt{-10}) + 15+3\sqrt{-10} \in P$
$(a',b') = (6,4)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + 6+4\sqrt{-10} = 7(x'+y'\sqrt{-10}) - 1-3\sqrt{-10} \in P$
$(a',b') = (4,5)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + 4+5\sqrt{-10} = 7(x'+y'\sqrt{-10}) - 3-2\sqrt{-10} \in P$
$(a',b') = (2,6)$: $a+b\sqrt{-10} = 7(x+y\sqrt{-10}) + 2+6\sqrt{-10} = 7(x'+y'\sqrt{-10}) - 5-\sqrt{-10} \in P$

So, $P = \ker \varphi \Rightarrow R/P \cong \mathbb{F}_7$ by FIT.

R.11. R is integral domain. X is indeterminate.

(a) R is a field $\Rightarrow R[x]$ is PID.

We can show that $R[x]$ is an Euclidean Domain $\Rightarrow$ PID.
where $N(f(x)) = \deg(f(x))$

Let $f(x), g(x) \in R[x]$. $g(x) = f(x)\,q(x) + r(x)$ where $\deg(r(x)) < \deg f$ or $r = 0$

This is true by division algorithm.

(b) $R[x]$ is a PID $\Rightarrow R$ is a fd.

Let $k \in R$. $k \neq 0$

Let (k, x) be an ideal in $R[x]$. By assumption $(k, x) = (g(x))$

This implies $g(x) \mid k \Rightarrow k = g(x)\,g'(x) \Rightarrow \deg(g(x)) = 0$
$\Rightarrow g(x) = c$ constant

$g(x) \mid x \Rightarrow c \mid x \Rightarrow x = c \cdot h(x)$ $\quad h(x) = a_1 x + a_0$ (deg 1)
$\Rightarrow a_0 = 0$ and $a_1 = c^{-1}$

$\Rightarrow (k, x) = (1) \Rightarrow k\,a(x) + x\,b(x) = 1 \Rightarrow b(x) = 0,\ a(x) = k^{-1}$

$\Rightarrow k$ is a unit $\Rightarrow R$ is a field.

R.12. (a) Prove that Euclidean Domain ⇒ PID

Let N be the norm. I be an ideal. Let $a \in I$ be an element such that $N(a)$ is minimum in I. (a non zero)

↖ By Well ordering Principle.

Let $x \in I$ claim: $x = qa$

Assume $x \neq 0$ (otherwise $x = 0 \cdot a$) $x = qa + r$ by E.D. $N(r) < N(a)$ or $r = 0$

$r \in I \Rightarrow r = 0$ since $N(a)$ is minimum

$= x - qa$

So, we get $I = (a)$

(b) Give an example of UFD but not PID.

$\mathbb{Z}[x]$, $(2, x)$ can't be generated by single element.

R.13(a) Show that $\forall n \in \mathbb{N}$, $\exists$ irr poly $P_n(x) \in \mathbb{Q}[x]$ of deg. n.

Remember, Eisenstein's Criterion & Gauss Lemma.

If $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Q}[x]$ with integer coeff. such that

$\exists$ a prime p with (i) $p \mid a_0, \cdots, p \mid a_{n-1}$; then f is irreducible.

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$

By this criterion, $P_n(x) = x^n + 2$ is irr. in $\mathbb{Q}[x]$

(b) Is it true for $\mathbb{R}$.

This is not true for $\mathbb{R}$. Since max degree of irr. poly over $\mathbb{R}$ is 2.

eg. x^2+1 is irr. over $\mathbb{R}$.

R.14. R comm. Ring with Identity. $I \trianglelefteq R$ ideal. $\sqrt{I} := \{a \in R : \exists n \in \mathbb{N} \text{ s.t } a^n \in I\}$

(a) Prove that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

($\subseteq$) $a \in \sqrt{I \cap J} \Rightarrow \exists n \in \mathbb{N}$ s.t $a^n \in I \cap J \Rightarrow a^n \in I, J \Rightarrow a \in \sqrt{I}, \sqrt{J} \Rightarrow a \in \sqrt{I} \cap \sqrt{J}$

($\supseteq$) $a \in \sqrt{I} \cap \sqrt{J} \Rightarrow \exists k_1, k_2 \in \mathbb{N}$ s.t $a^{k_1} \in I, a^{k_2} \in J \Rightarrow a^{\max(k_1, k_2)} \in I \cap J$
$\Rightarrow a \in \sqrt{I \cap J}$

(b) P is prime ideal of R, $r \in \mathbb{N}$, Find $\sqrt{P^r}$.

Claim: $\sqrt{P^r} = \sqrt{P} = P$

($\supseteq$) $x \in P \Rightarrow x^r \in P^r \Rightarrow x \in \sqrt{P^r}$

($\subseteq$) $x \in \sqrt{P^r} \Rightarrow x^k \in P^r$ for some $k \in \mathbb{N} \Rightarrow x^k \in P \Rightarrow x \in P$ or $x^{k-1} \in P$
$\Rightarrow x \in P$ or $x^{k-2} \in P$
$\cdots \Rightarrow x \in P$ or $x \in P$

$\Rightarrow x \in P \Rightarrow \sqrt{P} = P \supseteq \sqrt{P^r}$

(c) $\sqrt{I}$ where $I = \langle 108 \rangle$ in $\mathbb{Z}$

$108 = 3^3 \times 2^2$, $\sqrt{I} = \sqrt{\langle 3^3 \rangle} \cap \sqrt{\langle 2^2 \rangle} = \langle 3 \rangle \cap \langle 2 \rangle = \langle 6 \rangle$

R.15.(a) Show that $\frac{\mathbb{Z}[i]}{\langle 3+i \rangle} \cong \mathbb{Z}/10\mathbb{Z}$

$\langle 3+i \rangle = (1+i)(2-i)$ $\quad (1+i, 2-i) \supseteq 2, 3 = (1+i+2-i) \Rightarrow 1 \in (1+i, 2-i)$

$\Rightarrow (1) = (1+i, 2-i)$

By CRT. $\frac{\mathbb{Z}[i]}{\langle 3+i \rangle} \cong \frac{\mathbb{Z}[i]}{\langle 1+i \rangle} \times \frac{\mathbb{Z}[i]}{\langle 2-i \rangle} \cong \mathbb{F}_2 \times \mathbb{F}_5$

(b) Is $\langle 3+i \rangle$ maximal?

No, $\langle 3+i \rangle \subsetneq \langle 1+i \rangle$ Alternatively, $\mathbb{Z}/10\mathbb{Z}$ is not Field

$\Rightarrow \langle 3+i \rangle$ is not maximal

R.16. $R = \mathbb{Z}[x]$

(a) Is R a UFD?

Yes, $\mathbb{Z}$ UFD $\Rightarrow \mathbb{Z}[x]$ UFD.

(b) Is R a PID?

No, Consider the ideal $(2, x)$

(c) Find $R^\times$ = group of units of R

Units of $\mathbb{Z}[x]$ = Units of $\mathbb{Z}$ = $\{\pm 1\}$

(d) Find a prime ideal of R which is not maximal

(x) is prime since, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is integral domain

not a field $\Rightarrow (x)$ not maximal

(e) Find a maximal ideal of R.

$(2, x)$ is maximal, since $\mathbb{Z}[x]/(2,x) \cong \mathbb{F}_2$ field.

R17. $a \in R$ is nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$.

(a) R is comm. with identity. set of nilpotent forms an ideal.

$I = \{a : a^n = 0 \text{ for some } n \in \mathbb{N}\}$ • $a, b \in I \Rightarrow \exists n_1, n_2 \in \mathbb{N}$ s.t $a^{n_1} = b^{n_2} = 0$

$(a+b)^{n_1+n_2} = 0$ (Uses commutativity)

• $a \in I$, $r \in R \Rightarrow (ar)^n = a^n r^n = 0 \Rightarrow ar \in I$.

(b) Describe all of the nilpotent elements in the ring $\mathbb{C}[x]/\langle f(x)\rangle$ where $f(x) = (x-1)(x^2-1)(x^3-1)$

$f(x) = (x-1)^3(x+1)(x^2+x+1) = (x-1)^3(x+1)(x-\mu_3)(x-\bar{\mu}_3)$

By CRT we have $\frac{\mathbb{C}[x]}{(f(x))} \cong \frac{\mathbb{C}[x]}{\langle (x-1)^3\rangle} \times \frac{\mathbb{C}[x]}{\langle (x+1)\rangle} \times \frac{\mathbb{C}[x]}{\langle (x-\mu_3)\rangle} \times \frac{\mathbb{C}[x]}{\langle x-\bar{\mu}_3\rangle}$

Nilpotent element of $\mathbb{C}[x]/\langle (x-1)^3\rangle$ is $g(x)(x-1) + \langle (x-1)^3\rangle$

So, Nilpotent element of $\mathbb{C}[x]/\langle f(x)\rangle$ is $g(x)(x-1)(x+1)(x^2+x+1) + \langle f(x)\rangle$ for any $g(x) \in \mathbb{C}[x]$.

(c) If R is not commutative (a) may not hold.

Consider $R = M_2(\mathbb{R})$ $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ie $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}$ $\begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}^2 = \begin{pmatrix} 0 & ac \\ 0 & c^2 \end{pmatrix}$

Put $a = c = 1$, $d = b = 0$ ie. $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$; $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$

So, $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin I$ ie. not an ideal.

R18. Let R be a ring. R^* set of units of R, $M = R \setminus R^*$. If M is an ideal of R, prove that M is maximal and moreover the only max. ideal.

- $M \trianglelefteq R$, Let $M \subsetneq M' \subseteq R$, $x \in M'$ s.t $x \notin M \Rightarrow x \in R^* \Rightarrow M' = (1) = R$

  So. M is maximal ideal of R.

- Let M_1 be another maximal ideal

  $x \in M_1 \Rightarrow x$ is not a unit $\Rightarrow x \in M \Rightarrow M_1 \subseteq M \Rightarrow M_1 = M$

R19.(a) R · PID. $I, J \neq 0$ ideals of R · $IJ = I \cap J$ iff $I + J = R$

($\Leftarrow$) $I + J = R$ $\quad IJ \subseteq I \cap J$ always · $I \cap J \subseteq (I+J)(I \cap J)$

$\subseteq 1 \cdot (I \cap J) + J(I \cap J)$

$\Rightarrow IJ = I \cap J$ $\quad \subseteq IJ + IJ \subseteq IJ$

Alternatively, $a + b = 1$ where $a \in I, b \in J$.

↳ $x \in I \cap J \Rightarrow xa + xb = x$, $xa \in IJ$, $xb \in IJ \Rightarrow xa + xb \in IJ$

$\Rightarrow x \in IJ$

($\Rightarrow$) $I = (a)$ $J = (b)$ $IJ = (ab)$ $I \cap J = (\text{lcm}(a,b))$

$(ab) = (\text{lcm}(a,b)) \Rightarrow ab = \text{lcm}(a,b)$

We have $\text{lcm}(a,b)\,\gcd(a,b) = ab \Rightarrow \gcd(a,b) = 1 \Rightarrow I + J = (1)$

(b) Show that $\mathbb{Z}/900\mathbb{Z} \cong \mathbb{Z}/100\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ as rings.

$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/100\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ $\quad$ φ has full image with kernel $900\mathbb{Z}$

$a \longmapsto (a \bmod 100, a \bmod 9)$ $\quad$ (by CRT)

So, we have the isomorphism.

(c) $I = \langle x^2+2, 5\rangle \leq \mathbb{Z}[x]$, $J = \langle x^2+2, 3\rangle \leq \mathbb{Z}[x]$. Show that I is maximal but J is not.

$\dfrac{\mathbb{Z}[x]}{\langle x^2+2, 5\rangle} \cong \dfrac{\mathbb{F}_5[x]}{(x^2+2)}$ $\quad$ x^2+2 is irreducible over $\mathbb{F}_5[x]$ (since $\nexists$ any root)

$\Rightarrow \dfrac{\mathbb{F}_5[x]}{(x^2+2)} \cong \mathbb{F}_{25}$ field $\Rightarrow I$ is maximal.

$\dfrac{\mathbb{Z}[x]}{\langle x^2+2, 3\rangle} \cong \dfrac{\mathbb{F}_3[x]}{(x^2+2)} \cong \dfrac{\mathbb{F}_3[x]}{(x^2-1)} \cong \dfrac{\mathbb{F}_3[x]}{(x-1)} \times \dfrac{\mathbb{F}_3[x]}{(x+1)} \cong \mathbb{F}_3 \times \mathbb{F}_3$ not a field

$\Rightarrow J$ is not max.

$J \subsetneq (x+1, 3)$ or $(x-1, 3)$

R20. $F \subseteq K$ subfield. $f(x), g(x) \in F[x] \setminus \{0\}$. Prove that gcd of $f(x)$ & $g(x)$ in $F[x]$ is same as gcd in $K[x]$

Let $h(x)$ = gcd of f, g in $F[x]$
$h'(x)$ = gcd of f, g in $K[x]$

$h(x) \mid f(x)$, $h(x) \mid g(x)$ in $K[x] \Rightarrow h(x) \mid h'(x)$ in $K[x]$

$h(x) = a(x)f(x) + b(x)g(x)$ where $a, b \in F[x]$ [by PID $\Rightarrow (f, g) = (h)$]

$h'(x) \mid f(x), g(x) \Rightarrow h'(x) \mid h(x)$ in $K[x] \Rightarrow h(x) = h'(x)$ upto ass. in $K[x]$

R21. Find the gcd of $x^3 - 6x^2 + x + 4$, $x^5 - 6x + 1$ in $\mathbb{Q}[x]$

$f(x) = x^3 - 6x^2 + x + 4$ $\qquad x^5 - 6x + 1 = g(x)$
$= x^3 - x^2 - 5x^2 + 5x - 4x + 4$
$= x^2(x-1) - 5x(x-1) - 4(x-1)$ $\qquad (x-1) \nmid (x^5 - 6x + 1)$
$= (x-1)(x^2 - 5x - 4)$

roots of $f(x) = 1, \dfrac{5 \pm \sqrt{25+16}}{2} = 1, \dfrac{5 \pm \sqrt{41}}{2}$

No common roots $\Rightarrow$ gcd $= 1$

R22(a) Define $\varphi: \mathbb{C}[x,y] \to \mathbb{C}[T]$. Show that $\ker\varphi = \langle y^2 - x^3 \rangle$

$x \mapsto T^2$

$y \mapsto T^3$

$(y^2-x^3) \subseteq \ker\varphi$ (obvious)

Let $f(x,y) \neq 0 \in \ker\varphi$, $f(x,y) \in \mathbb{C}[x][y]$

Let $f(x,y) = a_0 + y\,g(x) + (y^2-x^3)\,h(x,y)$ by Euclid's Algorithm

$\varphi(f) = 0 \Rightarrow a_0 + T^3 g(T^2) = 0 \Rightarrow a_0 = 0,\ g(T^2) = 0 \Rightarrow g(x) = 0$

(b) Find $\operatorname{Im}\varphi$

Claim: $\operatorname{Im}\varphi = \mathbb{C}[T^2, T^3] = \{f(T) = a_0 + a_1 T + \cdots + a_n T^n : a_1 = 0\}$

Let $a_0 + a_2 T^2 + \cdots + a_n T^n \in \mathbb{C}[T]$

$$= \varphi(a_0 + a_2 x + a_3 y + a_4 x^2 + a_5 xy + \cdots + a_{2k} x^k + a_{2k+1} x^{k+1} y)$$

Let $f(x,y) \in \mathbb{C}[x,y]$

$$f(x,y) = g(y) + x\,h(x,y) = a_0 + \cdots + a_n y^n + x\,h(x,y)$$

$\varphi(f) = a_0 + T^3(\cdots) + T^2(\cdots)$ i.e. coeff. of $T = 0$

R23. Prove that $\mathbb{Z}[\sqrt{-2}]$ is ED

Let $N(a+b\sqrt{-2}) = a^2+2b^2 = (a+b\sqrt{-2})(a-b\sqrt{-2})$

Claim: This is a norm function. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. Find q, r s.t. $\alpha = q\beta + r$ with $r=0$ or $N(r) < N(\beta)$

Let $\alpha = a+b\sqrt{-2}$ $\beta = c+d\sqrt{-2}$

$$\frac{\alpha}{\beta} = \frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = q_1 + \sqrt{-2}(q_2) \quad \text{where } q_1, q_2 \in \mathbb{Q}$$

Choose integer m, n s.t. $|q_1 - m| \leq 1/2$ $|q_2 - n| \leq 1/2$

$$\alpha = \beta(m+n\sqrt{-2}) + r$$

$$\Rightarrow r = \beta\left(\frac{\alpha}{\beta} - m - n\sqrt{-2}\right) \Rightarrow N(r) = N(\beta)\, N\left(q_1 - m + (q_2 - n)\sqrt{-2}\right)$$

$$\leq N(\beta)\left(1/4 + 2\,1/4\right) = \frac{3}{4}N(\beta) < N(\beta)$$

R24. Let $m,n \in \mathbb{Z}\setminus\{0\}$. Prove that $\gcd(m,n)$ in $\mathbb{Z}$ is same as gcd in $\mathbb{Z}[i]$.

Let $(m,n)=(d)$ in $\mathbb{Z}$ & $(m,n)=(\alpha)$ in $\mathbb{Z}[i]$

$d \mid m, d \mid n$ in $\mathbb{Z}[i] \Rightarrow d \mid \alpha$ in $\mathbb{Z}[i]$

$d = am+bn$ in $\mathbb{Z} \Rightarrow d = a(\alpha m') + b(\alpha n') = \alpha(am'+bn')$ in $\mathbb{Z}[i] \Rightarrow \alpha \mid d$ in $\mathbb{Z}[i]$

$\Rightarrow d = \alpha$ upto associates in $\mathbb{Z}[i]$

Generalize this result to Euclidean domains.

Actually, PID is enough. Let $R \subseteq S$ be 2 PID. gcd of a,b in R is same as gcd of a,b in S.

Let d_1 = gcd of a,b in R $\Rightarrow d_1 \mid a, d_1 \mid b$ in R

d_2 = gcd of a,b in S $\Rightarrow d_2 \mid a, d_2 \mid b$ in S

$d_1 \mid a, d_1 \mid b$ in $R \Rightarrow$ in $S \Rightarrow d_1 \mid d_2$ in S

$d_1 = ax+by$ in R ie. $x,y \in R \subseteq S \Rightarrow d_2 \mid (ax+by) \Rightarrow d_2 \mid d_1$ in S

$\Rightarrow d_1 = d_2$ in S (upto associates)

R25. Prove that the center of matrix ring $M_n(\mathbb{R})$ is the set of scalar matrices

Let E_{ij} be the matrix with ij-th entry 1 rest 0.

Let $A \in C(M_n(\mathbb{R}))$

$$E_{kk}A = AE_{kk}$$

$$(E_{kk}A)_{ij} = \sum_{\nu=1}^{n} e_{i\nu}\, a_{\nu j} = \begin{cases} a_{kj} & i=k \\ 0 & i \neq k \end{cases}$$

$$(AE_{kk})_{ij} = \sum_{\nu=1}^{n} a_{i\nu}\, e_{\nu j} = \begin{cases} a_{ik} & j=k \\ 0 & j \neq k \end{cases}$$

$\Rightarrow$ A is diagonal (only a_{kk} survives)

$E_{ij}A = AE_{ij} \Rightarrow a_{ii} = a_{jj}$ $\forall\, i,j$

So, $A = cI_n$

R26. $R_1 = \mathbb{F}_p[x]/\langle x^2-2\rangle \quad R_2 = \mathbb{F}_p[x]/\langle x^2-3\rangle$

Determine if $R_1 \cong R_2$ for $p = 2, 5, 11$

$p=2$

$$R_1 = \frac{\mathbb{F}_2[x]}{(x^2-2)} = \frac{\mathbb{F}_2[x]}{(x^2)}$$

$$R_2 = \frac{\mathbb{F}_2[x]}{\langle x^2-3\rangle} = \frac{\mathbb{F}_2[x]}{((x-1)^2)}$$

} Isomorphic

$p=5$

$$R_1 = \frac{\mathbb{F}_5[x]}{(x^2-2)} \quad x^2-2 \text{ irr in } \mathbb{F}_5[x] \Rightarrow R_1 \cong \mathbb{F}_{25}$$

$$R_2 = \frac{\mathbb{F}_5[x]}{(x^2-3)} \quad x^2-3 \text{ irr in } \mathbb{F}_5[x] \Rightarrow R_2 \cong \mathbb{F}_{25}$$

} Iso

$p=11$

$$R_1 = \frac{\mathbb{F}_{11}[x]}{(x^2-2)} \quad x^2-2 \text{ irr in } \mathbb{F}_{11}[x] \Rightarrow R_1 \cong \mathbb{F}_{121}$$

$$R_2 = \frac{\mathbb{F}_{11}[x]}{(x^2-3)} = \frac{\mathbb{F}_{11}[x]}{(x-5)(x+5)} \cong \frac{\mathbb{F}_{11}[x]}{(x-5)} \times \frac{\mathbb{F}_{11}[x]}{(x+5)} \cong \mathbb{F}_{11} \times \mathbb{F}_{11}$$

$R_1 \not\cong R_2$

R27 (a) Show that the only automorphism of $\mathbb{R}$ is the identity.

Let $\phi: \mathbb{R} \to \mathbb{R}$ be a ring homomorphism. $\phi(1) = 1 \Rightarrow \phi(n) = n \ \forall n \in \mathbb{N}$

This implies $\phi(n) = n \ \forall n \in \mathbb{Z}$ $\left[\phi(-1) = -1 \text{ since } \underset{1}{\phi(1)} + \phi(-1) = 0\right]$

$\phi\left(\frac{1}{n}\right)\phi(n) = \phi(1) = 1$

$\Rightarrow \phi(1/n) = 1/n \quad \forall n \in \mathbb{Z} \setminus \{0\} \Rightarrow \phi(q) = q \ \forall q \in \mathbb{Q}$

Let $x > 0 \Rightarrow \phi(x) = \left(\phi(\sqrt{x})\right)^2 > 0$

So $a > b \Rightarrow a - b > 0 \Rightarrow \phi(a) - \phi(b) > 0 \Rightarrow \phi(a) > \phi(b)$

So, if $\forall x, y \in \mathbb{Q}$ s.t $x < r < y$; $x < \phi(r) < y$

This implies $\phi(r) = r \Rightarrow \phi = id$

(b) $\phi: \mathbb{C} \to \mathbb{C}$ s.t $\phi(r) = r \ \forall r \in \mathbb{R}$ implies $\phi = id$ or conjugation.

$\phi(a + ib) = a + \phi(i)\, b$ So, $\phi(i)$ determines the morphism

$\left(\phi(i)\right)^2 = \phi(-1) = -1 \Rightarrow \phi(i) = i$ or $-i$

So, if $\phi(i) = i \Rightarrow \phi = id$ and if $\phi(i) = -i$ $\phi =$ conjugation

R28. (a) Find all ideals of the ring $\mathbb{Z}/24\mathbb{Z}$.

Let $\pi: \mathbb{Z} \to \mathbb{Z}/24\mathbb{Z}$ be the ring homomorphism.

We know ideals of $\mathbb{Z}/24\mathbb{Z}$ corresponds to ideals of $\mathbb{Z}$ containing $24\mathbb{Z}$.

i.e. the ideals are: $2\mathbb{Z}/24\mathbb{Z}$, $3\mathbb{Z}/24\mathbb{Z}$, $4\mathbb{Z}/24\mathbb{Z}$, $6\mathbb{Z}/24\mathbb{Z}$, $8\mathbb{Z}/24\mathbb{Z}$, $12\mathbb{Z}/24\mathbb{Z}$ and $\{0\}$ and $\mathbb{Z}/24\mathbb{Z}$.

(b) Find all ideals of the ring $\dfrac{\mathbb{Q}[x]}{(x^2+2x-2)}$

by Eisenstein's Criterion, x^2+2x-2 is irr $\Rightarrow$ It is a field

So only ideals are (0) & (1)

R29. R integral domain. Show that $R[x]^\times = R^\times$

Let $f(x)$ be a unit of $R[x] \Rightarrow \exists g(x)$ s.t. $f(x)g(x) = 1$

By comparing deg (integral domain $\neq$) $\deg f(x) = 0$, $\deg g(x) = 0$

$\Rightarrow f(x) = a_0 \in R$ $g(x) = a_0' \in R$ s.t. $a_0 a_0' = 1 \Rightarrow a_0 \in R^\times$

$\Rightarrow f(x) = a_0 \in R^\times$

R30. Express the polynomial $x^4 - 2x^2 - 3$ as product of irr. poly over

$\mathbb{Q}$: $x^4 - 2x^2 - 3 = (x^2 - 3)(x^2 + 1)$ Since the roots are not in $\mathbb{Q}$ these are irr.

$\mathbb{R}$: $x^4 - 2x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})(x^2 + 1)$

$\mathbb{C}$: $x^4 - 2x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})(x - i)(x + i)$

$\mathbb{F}_5$: $x^4 - 2x^2 - 3 = (x^2 - 3)(x^2 + 1) = (x^2 - 3)(x - 2)(x + 2)$

R31. Let $\omega = (1+\sqrt{-3})/2 \in \mathbb{C}$ and $R = \{a+b\omega : a,b \in \mathbb{Z}\}$

(a) Show that R is a subring of $\mathbb{C}$.

We only have to check multiplication:

$$\begin{aligned}(a+b\omega)(c+d\omega) &= ac + \omega(bc+ad) + \omega^2 bd \\ &= ac + \omega(bc+ad) + bd\left(\frac{1-3+2\sqrt{-3}}{4}\right) \\ &= ac + \omega(bc+ad) + bd\left(-\tfrac{1}{2} + \tfrac{\sqrt{-3}}{2}\right) \\ &= (ac-bd) + \omega(bc+ad+bd) \in R\end{aligned}$$

(b) Show that R is an Euclidean Domain with norm $N(z) = z\bar{z}$

$$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) = a^2+b^2+ab(\omega+\bar{\omega}) = a^2+b^2+ab$$

$\alpha = a+b\omega \quad \beta = c+d\omega \qquad \frac{\alpha}{\beta} = \frac{a+b\omega}{c+d\omega} = \frac{(a+b\omega)(c+d\bar{\omega})}{c^2+d^2+cd} = q_1 + q_2\omega$

where $q_1, q_2 \in \mathbb{Q}$

Choose m, n s.t. $|q_1 - m| \le 1/2, |q_2 - n| \le 1/2$

$a+b\omega = (c+d\omega)(m+n\omega) + r$

$r = (c+d\omega)\left(\frac{\alpha}{\beta} - m - n\omega\right)$

$\Rightarrow N(r) = N(c+d\omega)\, N\left(\frac{\alpha}{\beta} - m - n\omega\right)$

$= N(c+d\omega)\left((q_1-m)^2 + (q_2-n)^2 + (q_1-m)(q_2-m)\right)$

$\le N(c+d\omega)\left(1/4 + 1/4 + 1/4\right) < N(c+d\omega)$

R32. Let I be an ideal gen. by an irr poly of deg 2 in $\mathbb{R}[x]$.
Prove that $\frac{\mathbb{R}[x]}{I} \cong \mathbb{C}$.

Let $I = (x^2+ax+b)$ irreducible. Let α_1, α_2 be the roots in $\mathbb{C}$

$\varphi: \mathbb{R}[x] \to \mathbb{C}$
$x \mapsto \alpha_1$

Image should be a fd containing $\mathbb{R}$ in $\mathbb{C}$
ie. $\mathbb{C}$
kernel $= I$ [$I \subseteq$ kernel, I maximal $\Rightarrow I =$ kernel]

First Iso. thm $\Rightarrow$ result.

R33. Show that $M_2(\mathbb{R})$ has only 2 sided ideals $\langle 0\rangle$ and $M_2(\mathbb{R})$

Assume $\langle 0\rangle \subsetneq I \subsetneq M_2(\mathbb{R})$ be a 2 sided ideal.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$ with $a \neq 0$ (WLOG)

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

So $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I$$

$\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I \Rightarrow I = M_2(\mathbb{R})$

R34. R comm. ring with identity. $a \in R$ unit $b \in R$ nilpotent. Show that $a+b$ is a unit.

a unit $\Rightarrow \exists u$ s.t $aua = 1$, b nilpotent $\Rightarrow \exists n \in \mathbb{N}$ s.t $b^n = 0$

$(a+b) = a(1 + a^{-1}b)$; $(a^{-1}b)^n = 0$

Let $y = 1 - a^{-1}b + (a^{-1}b)^2 - (a^{-1}b)^3 + \cdots + (-1)^n (a^{-1}b)^n + 0 \cdots$

$= (1 - ub + u^2b^2 + \cdots + (-1)^{n-1} u^{n-1} b^{n-1})$

$$(1+ub)y = (1 - ub + u^2b^2 + \cdots + (-1)^{n-1}u^{n-1}b^{n-1} + (-1)^n u^n b^n)$$
$$+ ub - u^2b^2 + \cdots + (-1)^{n-1}u^{n-1}b^{n-1} \quad (\to 0)$$

$= 1$

So, $(a+b)^{-1} = uy$

R35. (a) $f: R \to S$ ring homomorphism. $P \trianglelefteq S$ prime, show that $f^{-1}(P)$ prime.

Let $ab \in f^{-1}(P)$ with $a \notin f^{-1}(P)$

$f(ab) \in P \Rightarrow f(a)f(b) \in P \quad a \notin f^{-1}(P) \Rightarrow f(a) \notin P$

$\Rightarrow f(b) \in P \Rightarrow b \in f^{-1}(P)$

(b) M is maximal. Is $f^{-1}(M)$ maximal?

No, if f is not surjective. e.g. $f: \mathbb{Z} \hookrightarrow \mathbb{Q}$, $M = \{0\} \trianglelefteq \mathbb{Q}$

★ If f is surjective, $\frac{R}{f^{-1}(M)} \cong \frac{\mathrm{Im}(f)}{M} \cong \frac{S}{M} \cong F$ field $(\Rightarrow f^{-1}(M)$ max$)$