Midterm Review 2

Friday, February 9, 2018 9:27 PM

1. Prove or disprove that $4x^3+6x+3$ is a unit in $\mathbb{Z}/8[x]$

$(4x^3+6x+3)(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \stackrel{?}{=} 1$ (mod 8)

$(4x^3+6x+3)(6x+5)$
$= 36x^2 + 20x^2 + 18x + 30x + 15$
$= 56x^3 + 48x^2 + 15 = 1$

---

2. Let R and S be nonzero commutative rings. Describe the possible zero divisors in $R \times S$

Let $0 \in R \times S$ be $(0,0)$

(r,s) s.t., r,s are zero divisors

$(r,0)$

$(0,s)$

---

3. Let R be a commutative ring. In each case, prove or disprove that the indicated subset S of R is an ideal of R.

a) Let a and b be elements of R. Let $S = \{c \in R \mid ac \in (b)\}$

Is S is an ideal?

$c_1, c_2 \in S$

$a(c_1 + c_2) = ac_1 + ac_2 \in (b)$

$ac_1 c_2 = bkc_2 \in (b)$

$\Rightarrow c_1 + c_2,\ c_1 c_2 \in S.$

$a(-c_1) = -ac_1 = -bk \in (b)$

$\Rightarrow -c_1 \in S$

$\Rightarrow$ Subring

Then let $ac_1 = bk$

$\Rightarrow ac_1 r = bkr \in (b)$

$\Rightarrow c_1 r \in S$

And by commutativity $rc_1 \in S \Rightarrow$ Done

(b) Let X be a subset of R and let $S = \mathrm{Ann}(X) = \{r \in R \mid rx = 0 \text{ for all } x \in X\}$.

$(r_1 - r_2)x = 0$

$r_1 r_2 x = 0$

$krx = 0$

$rkx = krx = 0$

(c) Let I be an ideal of R and let $S = N(I) = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N} \text{ (} n \text{ depends on } r)\}$

pf:

$r_1^{n_1} \in I$

$r_2^{n_2} \in I$

$(r_1 r_2)^{n_1} = r_1^{n_1} r_2 \in I$

$(r_1 - r_2)^{n_1+n_2} \in I$ by $c \cdot r_1^{n_1} r_2^{n_2}$

$r_1^{n_1+n_2-k} r_2^{k}$

$n_1 + n_2 - k \geq n_1$ ✓

$n_1 + n_2 - k \leq n_1$

$\Rightarrow k \geq n_2$ ✓

$\forall t \in R,\ tr^n \in I$ by $r^n \in I$ and I is an ideal

(d) For this part only, Assume that R is the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. (with usual addition and multiplication). Let $S = \{f \in R \mid f(0) \in 2\mathbb{Z}\}$

pf: $f_1, f_2 \in S$

$f_1 - f_2(0) = f_1(0) - f_2(0) \in 2\mathbb{Z} \Rightarrow (f_1 - f_2) \in S$

$f_1 f_2(0) = f_1(0) f_2(0) \in 2\mathbb{Z} \Rightarrow f_1 f_2 \in S$

$f' \in R \quad f' f(0) = f'(0) f(0) \in 2\mathbb{Z} \Rightarrow f' f \in S$

Similar for $ff' \in S$

$\Rightarrow S$ is an ideal.

---

4. Let R be an integral domain. Suppose that $c \in R$, $c \neq 0$ and $c \notin R^\times$. Let

$I = \{p(x) \in R[x] \mid p(x) - ca \in (x) \text{ for some } a \in R\}$

(Here, (x) is the ideal of $R[x]$ generated by the element x.)

a) Prove that I is a proper ideal of $R[x]$.

pf: $1 \notin (I)$ by $1 - ca \in (x)$

$\Rightarrow 1 - ca = 0$

$\Rightarrow 1 = ca \Rightarrow c \in R^\times$ contradict.

b) Prove that I is not a principal ideal (that is, I is not of the form $(f(x))$ for a fixed $f(x) \in R[x]$). (Hint: Proof by contradiction works. Evaluation at $x=0$ can be used in some way.)

pf: Suppose I is a principal ideal.

Then if $x+1 = r(x)f(x) + ca$ for some $r(x) \in R[x]$

Let $x = 0$

$1 = 0 + ca$

$ca = 1$ Contradict.

$(f(x)) = I \Rightarrow c \in (f(x))$

$\Rightarrow x \in (f(x)) \Rightarrow c, x \in (f(x))$

$\Rightarrow x = f(x) \cdot g(x) \Rightarrow d \mid c \Rightarrow d \mid x$

$\Rightarrow \deg f(x) \leq 1$

$\Rightarrow d$ is a unit

$\Rightarrow (d) = R[x]$

Contradict with $I \subsetneq R[x]$

Lemma example: the intersection of 2 distinct prime ideals is a prime ideal

$\deg a = 0$

$\forall\, 0 \neq a$

$ca = 1$ Contradict.

$\Rightarrow \deg f_{\text{rest}} \leq 1$

$\Rightarrow d$ is a unit

$\Rightarrow (d) = R[x]$

Contradict with $2 \subsetneq R[x]$

---

5. Prove or give a counter-example : the intersection of 2 distinct prime ideals is a prime ideal

$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$

Check : $2\mathbb{N} \cap 3\mathbb{N} = 2\mathbb{N}$

---

6. Prove or disprove that $(2, x, y)$ is a maximal ideal of $\mathbb{Z}[x,y]$. (Here, $\mathbb{Z}[x,y]$ consists of polynomials in 2 variables x and y with coefficients in $\mathbb{Z}$)

pf: $\mathbb{Z}[x,y]/(2,x,y) \cong 2\mathbb{Z}$? No, but it is $\mathbb{Z}/2\mathbb{Z}$

If it is, then is $2\mathbb{Z}$ a field?

No.

Can we show: $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$?

$\mathbb{Z}[x] \longrightarrow \mathbb{Z}$

By Evaluate $x = 0$

$\varphi(f(x)) = f(0)$

$\varphi(f(x)+g(x)) = f(0)+g(0)$ ✓

$\varphi(f(x)g(x)) = f(0)g(0)$ ✓

$\Rightarrow \ker\varphi = (x)$, surjective is by $\varphi(x+z)$ where $z \in \mathbb{Z}$

$\Rightarrow \mathbb{Z}[x]/(x) \cong \mathbb{Z}$

$\mathbb{Z}[x,y]/(y) \cong \mathbb{Z}[x]$? $\mathbb{Z}$ is an integral domain $\Rightarrow \mathbb{Z}[x]$ is an integral domain

$\mathbb{Z}[x][y]/(y) \cong \mathbb{Z}[x]$?

$\Rightarrow \mathbb{Z}[x][y]/(x,y) = \mathbb{Z}$?

By setting

$\varphi(f(x,y)) = f(0,0) \Rightarrow \mathbb{Z}[x,y]/(x,y) = \mathbb{Z}$

$\mathbb{Z}[x,y]/(2,x,y) = 2\mathbb{Z}$? X

$\mathbb{Z}[x,y]/(2,x,y) \cong \mathbb{Z}/2\mathbb{Z}$

By evaluate $\varphi(f(x,y)) = f(0,0)$

$f(x,y) = x\,p(x) + y\,q(x,y) + 2\cdot k + \begin{matrix}0\\ \text{or } 1\end{matrix}$

$\mathbb{Z}[x,y]/(2,x,y) = \begin{matrix}0 + (2,x,y)\\ \text{or } 1 + (2,x,y)\end{matrix}$

$\Rightarrow \mathbb{Z}[x,y]/(2,x,y) \cong \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z}$ is a field

$\Rightarrow \mathbb{Z}[x,y]/(2,x,y)$ is a field

---

8. Prove or disprove $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ are isomorphic.

pf: $\mathbb{Z}[x]/(x^2+7) \ncong \mathbb{Z}[x]/(2x^2+7)$

x^2+7 is irreducible in $\mathbb{Z}[x]$

$2x^2+7$ is irreducible in $\mathbb{Z}[x]$

$\Rightarrow \mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ are integral domains.

$\Rightarrow \varphi(1) = 1$

$\varphi(\bar{x}^2 + \bar{7}) = \varphi(\bar{0}) = 0$

$\varphi(x^2) + \varphi(\bar{7}) = 0$

$\Rightarrow \varphi(x^2) = -7$

$\Rightarrow \varphi(x^2) = -7 = 2x^2$

$\varphi(x)\varphi(x) = -7 = 2x^2$

$\varphi(x)^2 = -7 = 2x^2$

Can assume $\varphi(x)$ has degree less than 1

Otherwise :

$(x^2+ax+b)^2 = x^4 + a^2x^2 + b^2 + 2ax^3 + \cdots = x^4 + \cdots + p(x)(2x^2+7) \neq 2x^2$

$(ax+b)^2 = a^2x^2 + 2abx + b^2$

$= (a^2-2)x^2 + 2x^2 + 2abx + b^2$

$\Rightarrow 2ab = 0$

$\Rightarrow a = 0$ or $b = 0$

$b = 0 \Rightarrow$

$\overline{a^2x^2} = \overline{2x^2}$

$\Rightarrow$

$a^2x^2 + (2x^2+7) = 2x^2 + (2x^2+7)$

$\Rightarrow a^2x^2 + 0 = 2x^2$

$\Rightarrow a^2x^2 = 2x^2$

$\Rightarrow a^2 = 2$

$\Rightarrow a \notin \mathbb{Z} \Rightarrow$ Contradict

If $a = 0$

$\Rightarrow a^2x^2 = 2x^2$

$\Rightarrow a^2 = 2$

$\Rightarrow a \notin \mathbb{Z}$ $\Rightarrow$ Contradict

If $a = 0$

$\varphi(x) = b^2$

$\Rightarrow \quad b^2 = -7$

$\Rightarrow b \notin \mathbb{Z}$, contradict.

---

9. Let $\varphi: R[x] \to \mathbb{C} \times \mathbb{C}$ be the homomorphism defined by $\varphi(x) = (i, i)$ and $\varphi(r) = (r, r)$ for $r \in R$. Determine the kernel and the image of φ.

$\varphi(x) = (i, i)$ $\quad \varphi(x^2) = (i, -1)$, $\quad \varphi(x^3) = (i, -i)$, $\varphi(x^4) = (1, 1)$

R is an field $\Rightarrow R[x]$ is P.I.D $\Rightarrow$ kernel is principal ideal.

$\varphi(a_n x^n + a_{n-1}x^{n-1} + \cdots\cdots + a_1 x + a_0) = a_n(i, i^n) + a_{n-1}(i, i^{n-1})$

$\qquad + \cdots\cdots + a_1(i, i) + (a_0, a_0)$

$a_n i^n + \cdots\cdots + a_1 i + a_0 = 0 \Rightarrow f(i) = 0$

And $a_n + a_{n-1} + \cdots\cdots + a_1 + a_0 = 0 \Rightarrow f(1) = 0$

$\ker\varphi = \quad \big((x^2+1)(x-1)\big) = \big(x^3 - x^2 + x - 1\big)$

$R[x]/\ker \cong i(R[x])$

By setting $\quad R[x] = a_2x^2 + a_1x + a_0$

$\Rightarrow \quad a_2(1, i^2) + a_1(1, i) + (a_0, a_0)$

$= a_2(1, -1) + a_1(1, i) + (a_0, a_0)$

$= (a_2 + a_1 + a_0, -a_2 + a_1 i + a_0)$

$= R \times \mathbb{C}$

---

10. Determine the maximal ideal of each of the following rings.

a) $R \times R$

b) $R[x]/(x^2)$

c) $R[x]/(x^2 - 3x + 2)$

d) $R[x]/(x^2 + x + 1)$

a) $\mathbb{R} \times \mathbb{R}$, first, we should say that $R \times R$ is not a field

$(r, 0) \neq 0$

But $(r, 0)(r_0, r_0) \neq (1, 1)$

$\Rightarrow R \times R$ is not a field

$(r, 0)(0, r) = (0, 0)$

$\Rightarrow R \times R$ is not an integral domain.

$\Rightarrow R \times R$ is only commutative.

Show: $R \times R$ only has 4 ideals: $\{(0,0)\}$, $\{(0,1)\}$, $\{(1,0)\}$, $\{(1,1)\}$

$= \{0\} \times R \quad = R \times \{0\} \quad = R \times R$

To pro this, when R is a field $\Rightarrow$ ideals of R are only (0), R

If I is an ideal in $R \times R$

then $(r_1, r_2)I \subset I$

$\Rightarrow$ If we have $I = I_1 \times I_2$

where I_1 and I_2 are just set

Then we come that $r_1 I_1 \in I_1$

$r_2 I_2 \in I_2$

$\Rightarrow I_1, I_2$ are ideals

$\Rightarrow$ There are the only 4 possibilities for I

b) $R[x]/(x^2)$, by Lattice Isomorphism Theorem

There is an bijection between the ideals containing (x^2) and others in $R[x]/(x^2)$

So $S \supset (x^2)$ is maximal in $R[x] \subset S/(x^2)$ is maximal in $R[x]/(x^2)$

$\Rightarrow S = (x)$ by (x) is irreducible in $R[x]$

And (x) is prime $\Rightarrow (x)$ is maximal $\Rightarrow (x)/(x^2)$ is maximal

c) $R[x]/(x^2 - 3x + 2) = R[x]/((x-1)(x-2))$

$(x-1)$

$(x-2)$

$(x-1)/((x-1)(x-2))$ is maximal

$(x-2)/((x-1)(x-2))$ is maximal

d) $R[x]/(x^2+x+1) \cong R(\frac{-1 \pm \sqrt{-3}}{2})$

(0) is the maximal ideal

By $x^2 + x + 1$ is irreducible

$x^2 + x + 1 = 0$

$\Rightarrow x = \frac{-1 \pm \sqrt{-3}}{2}$

$\Rightarrow R\left(\frac{-1 \pm \sqrt{-3}}{2}\right) \Rightarrow i \in R\left(\frac{-1 \pm \sqrt{-3}}{2}\right)$

$\Rightarrow R(\frac{-1 \pm \sqrt{-3}}{2}) = \mathbb{C}$

Because $\quad \frac{a_{11}}{\frac{-1+\sqrt{-3}}{2}} = \frac{\overline{a}_{11}}{\frac{-1-\sqrt{-3}}{2}}$

Then we $\varphi: R[x] \to \mathbb{C} \times \mathbb{C}$ is not going to be surjective

Cause when $\overline{f(a)} = f(\overline{a})$ By $f(x) \in R[x]$

$\Rightarrow \quad (f(a), \overline{f(a)})$

This is definitely not what $\mathbb{C} \times \mathbb{C}$ looks like.

11. Let R be the set of infinite sequences of real numbers $r=(r_1,\dots,)$ having the property that that exists $n\in\mathbb{N}$ s.t. $r_m=r_n$ for all $m>n$. (Note that n depends on the element r.) Given such an r, let $\bar{r}=r_n$

a) Define addition and multiplication of elements of R componentwise. Prove that R is a ring.

$N=\max(\text{ind}\,\bar{r}_1,\text{ind}\,\bar{r}_2)$

$a_1,a_2\in R$, $a_1+a_2=(r_1+r_1',\dots,r_{N-1}+r_{N-1}',\bar{r}_1+\bar{r}_2,\dots)$

$a_1a_2=(\text{---------})$

R is an abelian group by $-r$ exists, 0 exists, $r_1+r_2=r_2+r_1$

$r_1+r_2\in R$. $(r_1+r_2)+r_3=r_1+(r_2+r_3)$

$r_1r_2\in R$

$r_1(r_2r_3)=(r_1r_2)r_3$

$(r_1+r_2)r_3=r_1r_3+r_2r_3$

$\Rightarrow$ R is a ring

b) Indentify $R^\times$

Nonzero sequences. $r_i\neq 0$

c) Determine all of the maximal ideal of R.

---

12. Find a maximal ideal of $(\mathbb{Z}/8\mathbb{Z})[x]$

$\mathbb{Z}/8\mathbb{Z}$ is not an integral domain.

$(\mathbb{Z}/8\mathbb{Z})[x]/I$ is a field

$\mathbb{Z}[x]/8\mathbb{Z}$ is a field

$=\mathbb{Z}[x]/(8,2)$ is a field

$\Rightarrow 2=2\mathbb{Z}$ since it has to be a field

And only $\mathbb{Z}[x]/p\mathbb{Z}$ is a field

by if $\mathbb{Z}[x]/n\mathbb{Z}$ when n is not prime ✗

Consider $\overline{a}\cdot\overline{b}=\overline{0}$ which is not a field

$\Rightarrow 2=(2)$

$\mathbb{Z}_2[x]/(2)\cong\mathbb{Z}_2[x]$

$\mathbb{Z}_2[x]$ is a P.I.D, (x) is irreducible in $\mathbb{Z}_2[x]$

$\Rightarrow$ (x) is prime $\Rightarrow(x)$ is maximal, $x+1$ is also irreducible

$\varphi(f(x))=f(1)$ $\varphi(a_nx^n+\dots+a_1x+a_0+(2))=a_nx^n+\dots+a_1x+a_0$

$\Rightarrow$ $\varphi^{-1}(x)=x+(2)$

$\varphi^{-1}((x))=(x+(2))$

$\mathbb{Z}[x]/(x+1)\cong\mathbb{Z}$

$\mathbb{Z}[x]/(x)\cong\mathbb{Z}$

$\varphi(f(x))=f(0)$

$\Rightarrow (x+(2))$ is maximal in $\mathbb{Z}_2[x]/(1)$

By 4th Isomorphism Theorem

$(2)\subset I$ and I is maximal in $\mathbb{Z}_2[x]\Leftrightarrow$ same maximal in $\mathbb{Z}_2[x]$

$\Rightarrow (x+(2))$ is maximal in I

And corresponds to the $(x,2)$ which contains (2) in $\mathbb{Z}_2[x]$

---

14. Give examples of nonzero ideals $I_1\subsetneq I_2\subsetneq I_3$ of $\mathbb{Z}[x]$ such that I_1 and I_2 are prime and I_3 is not prime.

$(x,2)$ is maximal ideal by $\mathbb{Z}[x]/(x,n)\cong\mathbb{Z}/n\mathbb{Z}$, $n=2$, 2 is prime

$\Rightarrow(x,2)$ is a prime ideal in $\mathbb{Z}[x]$

$\mathbb{Z}[x]$ is U.F.D

x is irreducible $\Rightarrow x$ is prime $\Rightarrow(x)$ is prime

$(x)\subsetneq(x,4)\subsetneq(x,2)$

$(x,4)$ is not a prime by

$4\in(x,4)$

But $2\notin(x,4)$

---

15. Find a finite set of generators of each prime ideal of $\mathbb{Z}[x]$ that contains (x^2). Which of these ideals is maximal? Note that we don't have a results describing the set of prime ideals of $\mathbb{Z}[x]$. The problem can be solved without such a result.

pf: maximal ideal in $\mathbb{Z}[x]$ containing (x^2) = maximal ideal in $\mathbb{Z}[x]/(x^2)$

(x,p) containing (x^2) and (x,p) are maximal in $\mathbb{Z}[x]$

(x^2,p) is not a maximal ideal by $x^2\in(x^2,p)$, $x\notin(x^2,p)$

maximal $\Rightarrow$ prime $\Leftarrow$ integral domain (indeed, this holds $\forall$ commutative ring containing 1)

---

17. Let R be a commutative ring such that $R^2=R$. (Here, R^2 is the ideal of finite sums of products of pairs of elements of R, that is, the product ideal RR). Prove that a maximal ideal of R is a prime ideal. (Do not assume that R has 1.) (Notice this only works in rings w/ unit)

pf: Let I be a maximal ideal of $R\Rightarrow R/I$ is a field. ✗

So we can't use this here.

prime ideal. (Do not assume that R has 1) (Notice this only works on rings have unit)

pf: Let I be a maximal ideal of $R \Rightarrow R/I$ is a field. ✗

So we can't use this here.

Another try: Z is a maximal ideal of R . (Notice $R^2 \subset R$, but it is not guranteed $R \subset R^2$)

Show: $ab \in Z \Rightarrow a \in Z$ or $b \in Z$

Z is maximal

$\Rightarrow (Z, a) = R$

$(a)(b) = \sum r_1 a r_2 b$
$= \sum r_1 r_2 ab \in (ab)$

$(a)(b) = (ab) \subset Z$

If $a, b \notin Z$

$\Rightarrow (a, Z) = (b, Z) = R$

$\Rightarrow (a)+(Z) = (b)+(Z) = R$

$R^2 = R$

$\Rightarrow ((a)+(Z))((b)+(Z)) = R$

$\Rightarrow (ab) + (Z)(b) + (a)(Z) + (Z)^2 \subset Z$

Contradict with Z is maximal.

---

18. Let $\varphi: R \to S$ be a homomorphism of rings. Z maximal ideal of R and J an ideal of S.

a) Prove that $\varphi^{-1}(J) = \{r \in R \mid \varphi(r) \in J\}$ is an ideal of R that contains $\ker\varphi$.

pf: $r_1, r_2 \in \varphi^{-1}(J)$

$\Rightarrow \varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) \in J$

$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) \in J$

$\Rightarrow \varphi^{-1}(J)$ is a subring of R

$a \in R$, $r \in \varphi^{-1}(J)$

$\varphi(ar) = \varphi(a)\varphi(r) \in J$ by $\varphi(r) \in J$ and J is an ideal

J is an ideal $\Rightarrow 0 \in J$

$\Rightarrow \varphi^{-1}(0) \subset \varphi^{-1}(J)$

$\Rightarrow \ker\varphi \leq \varphi^{-1}(J)$

(b) Prove that if φ is onto, then $\varphi(Z)$ is an ideal of S. Show by example if φ is not surjective, then $\varphi(Z)$ might not be an ideal of S.

pf: $\varphi(i_1), \varphi(i_2) \in \varphi(Z)$

$\Rightarrow \varphi(i_1) - \varphi(i_2) = \varphi(i_1 - i_2) \in \varphi(Z)$

$\varphi(i_1)\varphi(i_2) = \varphi(i_1 i_2) \in \varphi(Z)$

$\Rightarrow \varphi(Z)$ is an subring

$\forall s \in S$, φ is onto, $\Rightarrow \exists r \in R$ s.t. $\varphi(r) = s$

$\Rightarrow \varphi(r)\varphi(i) = \varphi(ri) \in \varphi(Z)$

$\Rightarrow s\varphi(i) \in \varphi(Z)$

$\Rightarrow \varphi(i)s \in \varphi(Z)$

$\Rightarrow \varphi(Z)$ is an ideal of S.

Eg. $R \times \mathbb{C}$ is not an ideal in $\mathbb{C} \times \mathbb{C}$

---

19. Let $\varphi: R \to S$ be a surjective homomorphism of rings.

a) Prove that if Z is a prime ideal of R that contains $\ker\varphi$, then $\varphi(Z)$ is a prime ideal of S.

pf: $\varphi(i_1), \varphi(i_2) \in \varphi(Z)$

$\Rightarrow \varphi(i_1) - \varphi(i_2) \in \varphi(Z)$

$\varphi(i_1)\varphi(i_2) \in \varphi(Z)$

$\Rightarrow \varphi(Z)$ is a subring

Then $\varphi(Z)$ is an ideal is by surjective

To show prime,

$ab \in \varphi(Z)$

$a = \varphi(r_1)$

$b = \varphi(r_2) \Rightarrow \varphi(r_1 r_2) \in \varphi(Z)$

$\Rightarrow \varphi(r_1 r_2) = \varphi(i)$

$\Rightarrow r_1 r_2 - i \in \ker\varphi \subset Z$

$\Rightarrow r_1 r_2 \in Z$

$\Rightarrow r_1 \in Z$ or $r_2 \in Z$

$\Rightarrow \varphi(r_1) \in \varphi(Z)$
or $\varphi(r_2) \in \varphi(Z)$

b) Prove that if J is a prime ideal of S, then $\varphi^{-1}(J)$ is a prime ideal of R.

pf: $\varphi^{-1}(J)$ is an ideal containing kernel by above

then $ab \in \varphi^{-1}(J)$

$\varphi(ab) \in J \Rightarrow \varphi(a)\varphi(b) \in J$

$\Rightarrow \varphi(a) \in J$
or $\varphi(b) \in J$

$\Rightarrow a \in \varphi^{-1}(J)$
or $b \in \varphi^{-1}(J)$

c) Prove that the function $Z \to \varphi(Z)$ from the set of prime ideals of R containing kernel to the set of prime ideals of S is a bijection.

$R/\ker\varphi \cong S$

Then we know by 4th Isomorphism theorem

be an prime ideal in $R/\ker\varphi$ is bijective an prime ideal

containing $\ker\varphi$ in R. $\Rightarrow$ .....

---

20. The ring $R = 2\mathbb{Z}$ of even integers contains a maximal ideal Z such that R/Z is not a field.

$4\mathbb{Z}$ is maximal ideal of $2\mathbb{Z}$

By $4\mathbb{Z} \subseteq 2\mathbb{Z}$

$2\mathbb{Z}/4\mathbb{Z} = \{0, 2\}$ is not a field.

$\Rightarrow R/2$ is not a field.

---

21. Give an example of a ring containing exactly two maximal ideals.

The product of 2 fields $\mathbb{Q}\times\mathbb{Q}$: $\mathbb{Q}\times 0$, $0\times\mathbb{Q}$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$

$\mathbb{Z}/2\mathbb{Z} \times 0$ $\quad [\bar{0}, \bar{3}]$

$0 \times \mathbb{Z}/3\mathbb{Z}$ $\quad [\bar{2}, \bar{0}, \bar{0}]$

---

23. Let R be a commutative ring with $1\neq 0$. Let I be an ideal of R. Prove that if R contains a maximal ideal M such that $I \notin M$, then I has a maximal ideal. (Hint: What can you say about the ring $\mathbb{Z}/n\mathbb{Z}$)

M is an maximal ideal of R

$I+M = R$ by M is maximal and $I+M$ is an ideal containing M

$\Rightarrow I+M=R$

$\Rightarrow I\cap M = IM$

By $IM \subset I\cap M$

And if $\lambda \in I\cap M$

Then $\lambda \in I$, $\lambda \in M$

Notice $I+M=R$ and R is commutative containing 1

$\Rightarrow \exists\, i, m$ s.t. $1 = i+m$

then Consider $\lambda\cdot(i+m) = \lambda i + \lambda m$
$= i\lambda + \lambda m = \lambda$
$\in IM \quad \in IM$

commutative

$\Rightarrow \lambda \in IM$

$\Rightarrow I\cap M \subset IM$

$\Rightarrow I\cap M \supseteq IM$

$\Rightarrow \mathbb{Z}/M\mathbb{Z} = \mathbb{Z}/M\cap\mathbb{Z} = I+M/M = R/M$ field

---

25. a) $\mathbb{R}[x]/(x^3-x) \cong \mathbb{R}\times\mathbb{R}\times\mathbb{R}$

By $\varphi: \mathbb{R}[x] \to \mathbb{R}\times\mathbb{R}\times\mathbb{R}$

$\varphi(f(x)) = f(0)\times f(1)\times f(-1)$

b) $\mathbb{R}[x]/(x^2+x) \cong \mathbb{C}\times\mathbb{R}$

by $\varphi: \mathbb{R}[x] \to \mathbb{C}\times\mathbb{R}$

$\varphi(f(x)) = f(i)\times \underbrace{f(0)}$
$\Downarrow \qquad \Downarrow$
$x^2+1 \qquad x$

c) $\mathbb{Q}[x]/(x^2) \cong \mathbb{Q}[x]/(x^2-1)$

By $\mathbb{Q}[x]/(x^2-1) \cong \mathbb{Q}\times\mathbb{Q}$

$\varphi(f(x)) = f(1)\times f(-1)$

Then Can we show $\mathbb{Q}[x]/(x^2) \cong \mathbb{Q}\times\mathbb{Q}$

$\varphi(x^2) = \varphi(x)\varphi(x) = 0$

$\Rightarrow \varphi(x) = 0$

$\Rightarrow \ker\varphi \neq 0$

$\Rightarrow$ Not isomorphic

Or they are both $\cong \mathbb{Q}\times\mathbb{Q}$

$\mathbb{Q}[x]/(x^2-1) \cong \mathbb{Q}[x]/(x^2-2x)$

By $x^2-2x = (x-1)^2-1$

$\varphi\left(p(x)+(x^2-1)\right) = p(x-1)+\left((x-1)^2-1\right)$

---

d) $\mathbb{Z}[x]/(x^2+3,5) \cong F_3\times F_5$ ($F_5 = \mathbb{Z}/5\mathbb{Z}$)

$\mathbb{Z}[x]/(x^2+3) = \mathbb{Z}_5[x]/(x^2+3)$

$\mathbb{Z}_5[x]/(x^2+3)$

$x^2 \equiv -3$ (mod 5)

$x^2 \equiv 2$ (mod 5)

Which is impossible

So (x^2+3) is irreducible

$\mathbb{Z}_5$ is a field

$\mathbb{Z}_5[x]$ is a P.I.D

$\Rightarrow \mathbb{Z}_5[x]/(x^2+3)$ is a field

But $F_3\times F_5$ is not a field

$(1,0) \neq 0$, $(1,0) \notin (F_3\times F_5)^\times$

Notice $F_5[x]/(x^2+3) \cong \operatorname{Span}_{F_5}\{1,\sqrt{3}\} = F_5[\sqrt{3}]$

With $F_5[x] \to F_5[\sqrt{3}]$

$\varphi(f(x)) = f(\sqrt{3})$ surjective by $bx+a \to b\sqrt{3}+a$

$F_5[\sqrt{3}]$ is a field?

RHS $F_5[\sqrt{3}]$ is not that intuitive

But we could just use $\operatorname{Eval}_{\sqrt{3}}(F_5[x])$
$= \{a_0 + a_1\sqrt{3} + a_2\sqrt{3}^2 + \cdots \mid a_i \in F_5\}$
And show this is $= \operatorname{Span}_{F_5}\{1,\sqrt{3}\}$

$\mathbb{Z}(\sqrt{3}i) \cong \mathbb{Z}[x]$

With $F_3[x] \to F_3[\sqrt{-3}]$

$\varphi(f(x)) = f(\sqrt{-3})$ surjective by $bx+a \to b\sqrt{-3}+a$

$F_3[\sqrt{-3}]$ is a field?

$(a+b\sqrt{-3})(a-b\sqrt{-3})$

$= a^2+3b^2 \in F_3$

Then $(a^2+3b^2)^{-1}$ exists if $a^2+3b^2 \neq 0$

$a^2+3b^2 = 0 \Leftrightarrow a, b = 0$

$a^2+3b^2 \neq 0 \Rightarrow (a+b\sqrt{-3})(a-b\sqrt{-3})(a^2+3b^2)^{-1} = 1$

Done.

---

26. Prove that the quotient ring $\mathbb{Z}[x]/(2x)$ is isomorphic to $S = \{(f(x), n) \in F_2[x] \times \mathbb{Z} \mid f(0) \equiv n \pmod 2\}$.
(Here $F_2 = \mathbb{Z}/2\mathbb{Z}$)

$\varphi: \mathbb{Z}[x] \to \{(f(x), n) \in F_2[x] \times \mathbb{Z} \mid f(0) \equiv n \pmod 2\}$

$\varphi(f(x)) = (\bar{f}(x), f(0))$

$\varphi(f(x)) = (0, 0)$

iff $2 \mid f(x)$

and $f(0) \equiv 0 \pmod 2$

$\Rightarrow x \mid f(x)$

$\Rightarrow 2x \mid f(x)$

Then $\ker = (2x)$

$\Rightarrow \mathbb{Z}[x]/(2x) \cong S$

Also need to show φ is homomorphic

By $\varphi(f_1(x)+f_2(x)) = (\overline{f_1(x)+f_2(x)}, f_1(0)+f_2(0))$

$= (\bar{f}_1(x)+\bar{f}_2(x), f_1(0)+f_2(0))$

$= (\bar{f}_1(x), f_1(0)) + (\bar{f}_2(x), f_2(0))$

$= \varphi(f_1(x)) + \varphi(f_2(x))$

$\varphi(f_1(x)f_2(x)) = \varphi(f_1(x))\varphi(f_2(x))$

$\Rightarrow \varphi$ is homomorphism

---

28. Let n be a square-free integer. If $n < 0$, let $\sqrt{n} = i\sqrt{|n|}$. Define $R = \mathbb{Z}[\sqrt{n}] = \{a+b\sqrt{n} \mid a, b \in \mathbb{Z}\}$
Note that R is a ring, under the usual addition and multiplication of complex numbers.
Identify R as an explicit quotient of $\mathbb{Z}[x]$. That is, find an ideal I of $\mathbb{Z}[x]$ s.t.
$R \cong \mathbb{Z}[x]/I$. Justify your answer.

$\mathbb{Z}[x]/(x^2-n) \cong \mathbb{Z}[\sqrt{n}]$

$\varphi(f(x)) = (f(\sqrt{n}))$

$f(\sqrt{n}) = 0 \Rightarrow (x^2-n) \mid f(x)$

By $f(x) = (x^2-n)q(x) + r(x)$

Since x^2-n is monic and $\mathbb{Z}[x]$ is an integral domain.

$\Rightarrow f(x) = (x^2-n)q(x) + r(x)$

$0 = f(\sqrt{n}) = 0 + r(\sqrt{n})$

$\Rightarrow r(\sqrt{n}) = 0$

Here $\deg r(x) = 1$

Then $r(\sqrt{n}) = 0$

$\Rightarrow a\sqrt{n} + b = 0$

$\Rightarrow$ impossible for $a, b \in \mathbb{Z}$

$\Rightarrow \deg r(x) = 0$

$\Rightarrow r(x)$ is constant

$\Rightarrow r(x) = 0$

$\Rightarrow (x^2-n) \mid f(x)$

$\Rightarrow \ker\varphi$ is principal ideal.

---

29. Let $R = \mathbb{Z}[\sqrt{-14}]$
a) Find two different factorizations of 15 as a product of irreducibles in R.

$15 = (1+\sqrt{-14})(1-\sqrt{-14})$

$1+\sqrt{-14}$ is irreducible by

$a+\sqrt{-14}b \mid 1+\sqrt{-14}$

$\Rightarrow a-\sqrt{14}b \mid 1-\sqrt{-14}$

$\Rightarrow a^2+14b^2 \mid 15$

$\Rightarrow a = \pm 1, b = \pm 1$

$a^2 = 3$ ✗

$a^2 = 5$ ✗

$a^2 = 1$ ✓ But still...

$\frac{1+\sqrt{-14}}{1-\sqrt{-14}} = \frac{(1+\sqrt{-14})^2}{15}$

$= \frac{1-14+2\sqrt{-14}}{15}$

$= -\frac{13}{15} + \frac{2}{15}\sqrt{-14} \notin \mathbb{Z}[\sqrt{-14}]$

$\Rightarrow 1-\sqrt{-14} \nmid 1+\sqrt{-14}$

$\Rightarrow$ ...

$\Rightarrow 1-\sqrt{-14}$ is irreducible

$15 = 3 \times 5$

To show 3 and 5 is irreducible

$a+\sqrt{-14}b \mid 3$

$a^2+14b^2 \mid 9 \Rightarrow \begin{cases} a^2=9 \\ b^2=0 \end{cases}$ don't help

$\begin{cases} a^2=1 \\ b^2=0 \end{cases}$ don't help

$a^2+14b^2 \mid 25 \Rightarrow \begin{cases} a^2=25 \\ \end{cases}$ don't help

$a^2+14b^2 \mid 9 \Rightarrow$ $\begin{cases} a^2=9 \\ b^2=0 \end{cases}$ don't work

$\begin{cases} a^2=1 \\ b^2=0 \end{cases}$ don't help

$a^2+14b^2 \mid 25 \Rightarrow \begin{cases} a^2=25 \\ b^2=0 \end{cases}$ don't help

$\begin{cases} a^2=5 \\ b^2=0 \end{cases}$ ×

$\begin{cases} a^2=1 \\ b^2=0 \end{cases}$ don't help

b) Prove or disprove that every nonzero element of R that is not a unit can be written as a product of finitely many irreducibles.

If x is not a unit then $N(x) \neq \pm 1$

Thm $N(a+\sqrt{-14}b) < \infty$

If it cannot be write as a product of finitely many irreducibles.

Thm $N(a+\sqrt{14}b) \in \mathbb{Z}$ can be written as a infinite many nonunit product in $\mathbb{Z}$ $\Rightarrow$ Contradict.

c) Prove or disprove $(2, \sqrt{-14})$ is a principal ideal of R.

If $(2, \sqrt{-14}) = (d)$

$d = a+\sqrt{-14}b$

$\Rightarrow a^2+14b^2 \mid 2$

$a^2+14b^2 \mid 14$

$a^2 = 1$

$a = \pm 1$

$\Rightarrow d = 1$

But $1 \notin (2, \sqrt{-14})$ by

$2(c+\sqrt{-14}b) + \sqrt{-14}(e+\sqrt{-14}f)$

$\Rightarrow 2c-14f = 1$

$2 \mid LHS$

$2 \nmid 1$

Contradict

$\Rightarrow 1 \notin (2, \sqrt{-14})$

Or: $\forall\ i \in (2, \sqrt{-14})$

$2 \mid N(i)$

By $N(2) = 4$

$N(\sqrt{-14}) = 14$

But $2 \nmid N(\pm 1) = 1$

---

30. Let R be a Euclidean domain. Let t be the smallest value among the norms of nonzero elements. Prove that every nonzero element of norm t is a unit. Deduce that a nonzero element of norm zero (if such exists) is a unit.

$\exists\ u \in R$ s.t. $u \neq 0$, $N(u) = t$

Then $\forall\ a \in R$

$a = uq + r$

If $r \neq 0$, $N(r) < N(u)$ is impossible by t is the smallest one

$\Rightarrow r = 0$

$\Rightarrow 1 = uq + 0 \Rightarrow 1 = uq \Rightarrow u \in R^\times$

---

31. Find the greatest common divisor of $11+7i$ and $18-i$ in $\mathbb{Z}[i]$

$N(11+7i) = 121+9 = 130$

$N(18-i) = 18^2+1 = 325$

$d = \gcd(11+7i, 18-i)$

Then $\forall\ d'$ is $\gcd(11+7i, 18-i)$

$d' \mid d \Rightarrow N(d') \mid N(d)$

So $N(d) \mid 65$

$a^2+b^2 = 65 = 13 \times 5 = (2-3i)(2+3i)(1-2i)(1+2i)$

$\Rightarrow d = (2-3i)(1-2i)$

$\Rightarrow d = 2-3i-4i-6$

$= -4-7i$

$$\frac{11+7i}{4+7i} = \frac{(11+7i)(4-7i)}{65} = \frac{44+21+12i-77i}{65} = \frac{65-65i}{65} = 1-i$$

$$\frac{18-i}{4-7i} = \frac{(18-i)(4+7i)}{65} = \frac{44-21+12i+77i}{65}$$

$= \frac{23+89i}{65} \notin \mathbb{Z}[i]$

$\Rightarrow 4+7i$ is the gcd

---

32. Let $\lambda = 11+3i$. Determine all maximal ideals of $\mathbb{Z}[i]$ that contain λ. (Explain why you got all of them).

$\mathbb{Z}[i]$ is a Euclidean domain $\Rightarrow$ maximal ideals is prime and principal in $\mathbb{Z}[i]$

$\Rightarrow 2 \in (p)$

$a+bi \mid 2$

and $a+bi$ be prime in 2.

$a+bi \mid 11+3i$

$a^2+b^2 \mid 121+9 = 130$

$a^2+b^2 \mid 130 = 2 \times 5 \times 13$

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

$(2+i)(2-i)(2+3i)(2-3i)$

Choose any of them

---

32. Prove that if I is a nonzero ideal of $\mathbb{Z}[i]$, then the quotient ring $\mathbb{Z}[i]/I$ is finite

$\mathbb{Z}[i]$ is a P.I.D and Euclidean Domain

$I = (a+bi)$

$\Rightarrow \forall s \in \mathbb{Z}[i]$

$s = (a+bi)q + r$

$N(r) < N(a+bi) = a^2+b^2$

$\Rightarrow N(r)$ is finite

$\Rightarrow$ only has finite possible r Since $r \in \mathbb{Z}[i]$

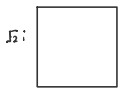
By $c^2+d^2 < a^2+b^2$ with integer solution is finite.

And for each $N(r)$ # of solution is also finite.

---

33. Let $R = \mathbb{Z}[\sqrt{-2}]$, with the norm map $N(a+b\sqrt{-2}) = a^2+2b^2$

a) Prove that N is a Euclidean Norm



$\frac{\sqrt{1+2}}{2} = \frac{\sqrt{3}}{2} < 1$

$\Rightarrow$ ------

b) Find a generator of the ideal $(85, -11+4\sqrt{-2}) = (d)$ By P.I.D

Recall : GCD

$N(85) = 85^2 = 17^2 \times 5^2$

$N(-11+4\sqrt{-2}) = 121 + 16\times 2 = 153 = 3^2 \times 17$

$\gcd(N(85), N(-11+4\sqrt{-2})) \mid 17$

Either $N(d) = 17$

$N(d) = 1$

$N(d) = 17$

$\Rightarrow a^2+2b^2 = 17$

$\begin{cases} a^2 = 9 \\ b^2 = 4 \end{cases}$

$\Rightarrow a = \pm 3$

$b = \pm 2$

$\Rightarrow \frac{3+2\sqrt{-2}}{3-2\sqrt{-2}}$

$d = \gcd(a, b)$

$\Rightarrow (d) = (a, b)$

$\Rightarrow (\underbrace{3+2\sqrt{-2}}_{\text{generator}})$

$\frac{85}{3+2\sqrt{-2}} = \frac{85(3-2\sqrt{-2})}{17}$

$= 5(3-2\sqrt{-2})$

$\frac{-11+4\sqrt{-2}}{3+2\sqrt{-2}} = \frac{(-11+4\sqrt{-2})(3-2\sqrt{-2})}{17}$

$= \frac{-33+12\sqrt{-2}+22\sqrt{-2}+16}{17}$

$= \frac{-17+34\sqrt{-2}}{17}$

$= -1+2\sqrt{-2}$

$\frac{-11+4\sqrt{-2}}{3-2\sqrt{-2}}$

$= \frac{(-11+4\sqrt{-2})(3+2\sqrt{-2})}{17}$

$= \frac{-33+12\sqrt{-2}-22\sqrt{-2}-16}{17}$

$= \frac{-49-10\sqrt{-2}}{17} \notin \mathbb{Z}[\sqrt{-2}]$

---

36. Let R be an integral domain having the property that every prime ideal of R is principal. Prove that R is a P.I.D via the steps outlined below.

a) Show, using Zorn's Lemma, that if there exist ideals that are not principal, then the set of nonprincipal ideals of R has a maximal element (under inclusion).

pf:

Let S = set of nonprincipal ideal

Then let C be the $\leq$

Every chain of S

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is a chain

And Consider $\cup I_i$, it is

an ideal, it is not principal

By if it is $\Rightarrow I_i$ is principal

$\Rightarrow \cup I_i$ is not principal

$\Rightarrow \cup I_i \in S$

and chain has this upper bound in S.

$\Rightarrow S$ has a maximal element.

b) Let I be an ideal that is maximal among principal ideals. Let $a, b \in R \setminus I$ be such that $ab \in I$. Let $J = \{c \in R \mid c(I, a) \subset I\}$. Prove that J is an ideal of R, $I \subsetneq (I, b) \subset J$ and $(I, a)J \subset I$.

pf: $a, b \in R \setminus I \Rightarrow a \in$ principal ideal, $b \in$ principal ideal. By I is maximal

To show J is an ideal

$c_1, c_2 \in J$

$\Rightarrow c_1(I, a) \subset I$

$c_2(I, a) \subset I$

$\Rightarrow c_1 ar \in I \quad \forall r \in R$

$c_2 ar \in I \quad \forall r \in R$

$\Rightarrow (c_1 - c_2) ar \in I \quad \forall r \in R.$

$c_1 c_2 ar \in I \quad \forall r \in R$

$\Rightarrow J$ is a subring

To show it is an ideal

⇒ If $car \in I$

⇒ $r'car \in I$

⇒ $r'c \in J$

⇒ J is an ideal

If $I = (I, b)$

Then $i + b \cdot 1 \in I$ by R is an integral domain, $1 \in R$.

⇒ $b \in I$

⇒ Contradict by $b \in R \setminus I$

⇒ $I \subsetneq (I, b)$

Then $(I, b) \subset J$ by

$\forall\ h \in (I, b)$

$h = i + rb$

⇒ $(i + rb)(I, a)$

$= (i + rb)I + (i + rb)a \in I$

⇒ $h \in J$

⇒ $(I, b) \subset J$

To show $(I, a)J \subset I$

By $\forall\ h \in (I, a)$

$h = i + ar$

$\forall\ c \in J$

$(i + ar)c$

$= c(i + ar) \in I$

⇒ $hc \in I$

Then $\exists hc \in I$

⇒ $(I, a)J \subset I$

c) Show that $I = (I, a)J$ is principal. (Observe that $(I, a) = (d)$ and J are principle and if $c \in I$, then $c = ed$ for some $e \in J$.)

By $I \subsetneq (I, a)$ and I is the maximal nonprincipal ideals

⇒ $(I, a) = (d)$

J is principal by $b \in J$ and $b \notin I$ ⇒ $J \not\subset I$

⇒ $(I, a)J$ is principal

$(I, a)J \subset I$ by (2)

And $I \subset (I, a)J$ by definition

⇒ $I = (I, a)J$

which means I is principal

Notice this means the maximal nonprincipal ideal is principal ⇒ every $I \in S$ is principal.

---

37. Let R be a Bézout domain.

a) Show that every finitely generated ideal of R is principal.

b) Let F be the field of fractions of R. Prove that every nonzero element of F can be written in the form a/b where $a, b \in R$ are relatively prime.

a) $(r_1, \cdots, r_n) = (r_1, r_2) + (r_3, \cdots, r_n) = (d_1) + \cdots = \cdots = (d)$

Bézout domain ⇒ $(r_1, r_2) = (d)$

$d = r_1 x + r_2 y$

and $r_1 = dk_1$

$r_2 = dk_2$

$r_1, r_2 \in (d)$

b) $\frac{r_1}{r_2}$, then suppose $d = \gcd(r_1, r_2)$

$\frac{dk_1}{dk_2} = \frac{k_1}{k_2}$ if k_1, k_2 are not relatively prime

Then $\exists\ d' \in R$ s.t. $d' \notin R^\times$

$d' \mid k_1$, $d' \mid k_2$ ⇒ $dd' \mid r_1$, $dd' \mid r_2$

⇒ d is not the gcd

Contradict.

---

38. Let $R = \mathbb{Z}[i]$

a) Prove that $R/(1+i)$ is a field of order 2.

If: $1 + i$ is irreducible in $\mathbb{Z}[i]$

By $N(1+i) = |1+i|^2 = 2$ is a prime

⇒ $N(1+i)$ is irreducible

⇒ $(1+i)$ is a prime ideal

Then by $\mathbb{Z}[i]$ is a Euclidean Domain ⇒ $\mathbb{Z}[i]$ is a P.I.D

⇒ $(1+i)$ is maximal ideal

⇒ $\mathbb{Z}[i]/(1+i)$ is a field

To show the order of a field is 2,

⇒ That field only has 0 and 1

is that any $a+bi$,

$$\frac{a+bi}{1+i} = \frac{(a-b)}{(1+i)} + \frac{b(1+i)}{1+i}$$

Or ...

$\frac{n}{1+i} \simeq 0$ if $n \equiv 0 \pmod 2$

$\frac{n}{(1+i)} = \frac{n}{2}(1-i)$

If $n \equiv 1 \pmod 2$

$n = 2k+1$

$\frac{2k}{1+i} + \frac{1}{1+i} \simeq \frac{1}{1+i}$

For ni, if $n \equiv 0 \pmod 2$ ✓

If $n \equiv 1 \pmod 2$

It to the

By $\frac{i}{1+i} = \frac{i+1-1}{i+1} = \frac{i+1}{(1+i)} - \frac{1}{i+1}$

$\frac{-1}{1+i} = 1 + -2 = 1 + (1+i)(i-1)$

$2 \in (1+i)$ $\quad -2 = (1+i)(i-1)$

$\Rightarrow -2 \in (1+i)$

$\Rightarrow \frac{i}{1+i} \simeq \frac{-1}{1+i} \simeq \frac{1}{1+i}$

b) Suppose that p is a prime and $p \equiv 3 \pmod 4$. Prove that $\mathbb{Z}/(p)$ is a field containing exactly p^2 elements.

$p \equiv 3 \pmod 4$

$\Leftrightarrow \nexists\ x^2+y^2 = p$

$\Rightarrow p$ is irreducible

Otherwise, if $p = ab$, $a, b \notin \mathbb{Z}[i]^\times$

$\Rightarrow N(ab) = N(p) = p^2$

$\Rightarrow N(a) = N(b) = p$

$\Rightarrow a\bar{a} = p$

$\Rightarrow \exists\ x^2+y^2 = p$ contradict

$\Rightarrow p$ is irreducible $\Rightarrow p$ is prime

a) (p) is maximal $\Rightarrow \mathbb{Z}[i]/(p)$ is a field.

$\mathbb{Z}[i] \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

By $\varphi(a+bi) = (\bar{a}, \bar{b})$

$\ker \varphi = (p)$ by $\bar{a} = 0, \bar{b} = 0$

$\Rightarrow p \mid a$, $p \mid b$

$\Rightarrow p \mid a+bi$

$\varphi(a+bi)/(p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (not even a field)

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is not a field.

p is a prime in $\mathbb{Z}$, and $\mathbb{Z}[i]$

$\mathbb{Z}[i]/(p)$, has order p^2

By $\mathbb{Z}[i]/(p) = \mathbb{Z}_p[i]$

$\Rightarrow$ Consider $\mathbb{Z}_p[x]$, $\mathbb{Z}_p$ is field $\Rightarrow \mathbb{Z}_p[x]$ is P.I.D

$\mathbb{Z}_p[x]/(x^2+1) \cong \mathbb{Z}_p[i]$

By x^2+1 is irreducible in $\mathbb{Z}_p[x]$ since $\nexists\ x$ s.t. $x^2 \equiv -1 \pmod p$

By if so, $x^4 \equiv 1 \pmod p$

$4 \mid p-1$

$p \equiv 1 \pmod 4$

$\Rightarrow x^2+1$ is irreducible

$\mathbb{Z}_p[x]/(x^2+1) \cong$ Evaluation

$= \mathrm{span}\{1, i\}$

$= \mathbb{Z}_p[i]$ ($\mathbb{Z}_p(i)$ and $\mathbb{Z}_p[i]$ have different definition btw)

$\Rightarrow$

c) Suppose that p is a prime and $p \equiv 1 \pmod 4$. Factor p as a product of irreducibles, $p = a\bar{a}$. Show, using C.R.T that $\mathbb{Z}/(p)$ is isomphic to $\mathbb{Z}/(a) \times \mathbb{Z}/(\bar{a})$ and is a direct product of 2 fields of order p.

$p \equiv 1 \pmod 4$

p is a prime in $\mathbb{Z}[i]$ (To be continued ...)

$\Rightarrow$

$(a)(\bar{a}) = (p)$

$\Rightarrow \mathbb{Z}/(p) = \mathbb{Z}/(a) \times \mathbb{Z}/(\bar{a})$

---

40. Let $R = \mathbb{Z}[\sqrt{-5}]$

a) Let $2 = 4 + \sqrt{-5}$. Show that $2 := (2)$ is not a prime ideal of R.

pf: Here, since we don't know if $\mathbb{Z}[\sqrt{-5}]$ is a U.F.D

2+ is another hint to do irreducible

$4 + \sqrt{-5} \mid 21$

$4 + \sqrt{-5} \mid 7 \times 7$

$4 + \sqrt{-5} \nmid 7$

By $\frac{7}{4+\sqrt{5}} = \frac{7(4-\sqrt{5})}{21} = \frac{(2-\sqrt{5})}{3} = \frac{4-\sqrt{5}}{7}$

$\Rightarrow 4+\sqrt{5}$ is not a pre

b) Find a proper ideal J of R properly containing 2. Prove or disprove that J is principal.

$J \supsetneq 2$, if J is principal $\Rightarrow (d) \supsetneq (4+\sqrt{-5})$

$\Rightarrow d \mid 4+\sqrt{-5}$

$\Rightarrow d = \pm 1$ or $4+\sqrt{-5}$

Which $d = 4+\sqrt{-5} \Rightarrow J$ is not proper containg

$d = \pm 1 \Rightarrow J$ is not a proper ideal of R.

$\Rightarrow d$ cannot be principal

$J = (4+\sqrt{5},\ 2+\sqrt{5})$

---

41. Let R be an integral domain with field of fractions F.

a) Suppose that R is a U.F.D. Show that if $f(x) \in R[x]$ is a monic polynomial and $a \in F$ is a root of $f(x)$, then $a \in R$.

pf: Suppose $f(a) = 0$, $f(x) \in R[x]$

$f(a) = 0$. $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$R[x]$ is U.F.D, $F[x]$ is U.F.D

$\exists\ F[x] \Rightarrow f(x) = (x-a)f_2(x)f_3(x)\cdots f_k(x)$

Then let $f(x) = g_1(x)g_2(x)\cdots g_k(x)$ in $R[x]$ s.t. $g_i(x)$ are monic in $R[x]$

Since $g_i(x)$ is primitive $\Rightarrow$ $g_1(x)g_2(x)\cdots g_k(x)$ is also a factorization of irreducible in $F[x]$

$\Rightarrow \exists\ u \in F$ s.t. $(x-a) = u\,g(x)$
$= u(x-r)$ for some $r \in R$, $u \in F^\times$

$x - a = ux - ur$

Since $ux = x$
$\Rightarrow u = 1$
$\Rightarrow a = r$
$\Rightarrow a \in R$

By if not, $(a_1x - b_1)(a_2x - b_2)\cdots(a_nx - b_n)$, s.t. $\pi a_i = 1$

$= \pi a_i (x - b_i a_i^{-1})$
$= \pi a_i \{ x - b_1 a_1^{-1} \}\{ x - b_2 a_2^{-1} \}\cdots\{ x - b_n a_n^{-1} \}$
$= \{ x - b_1 a_1^{-1} \}\{ x - b_2 a_2^{-1} \}\cdots\{ x - b_n a_n^{-1} \}$

b) Use part a) to prove that if n is a square-free integer that is congruent to 1 modulo 4, then $\mathbb{Z}[\sqrt{n}]$ is not a U.F.D.

pf: $n \equiv 1 \pmod 4$, n is square-free

$x^2 + bx + c = 0$

s.t. the root $a \in F[x]$

$\Rightarrow a = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$

If $b^2 - 4c \equiv n \equiv 1 \pmod 4$

$\Rightarrow b^2 - 4c = n$

$b^2 = n + 4c$

$n^2 \equiv 1 \pmod 4$

$n \equiv 1 \pmod 4$

Also, $c \in \mathbb{Z}$, $b \in \mathbb{Z}$

Let $4c = n^2 - n$

$c = \frac{n^2-n}{4} \in \mathbb{Z}$

$b^2 = n + 4c$

$= n^2$

$\Rightarrow b = n$

$x^2 + nx + \frac{n^2-n}{4} = 0$

$\frac{-n \pm \sqrt{n^2 - n^2 + n}}{2} = \frac{-n \pm \sqrt{n}}{2} \in F$

$-\frac{n}{2} \in F$

$\sqrt{n} \in F \Rightarrow \cdots$

$\frac{1}{2} \in F$

$\Rightarrow a \notin \mathbb{Z}[\sqrt{n}]$

$\Rightarrow \mathbb{Z}[\sqrt{n}]$ is not a U.F.D.

---

42. Let $f(x) = x^5 - x^4 + x - 1$ and $g(x) = x^3 - x$ in $\mathbb{Q}[x]$

a) Find a greatest common divisor $d(x)$ of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$

$\mathbb{Q}[x]$ is a P.I.D $\Rightarrow$ G.C.D
U.F.D

$g(x) = x(x-1)(x+1)$

$f(x) = x^4(x-1) + (x-1)$

$= (x^4+1)(x-1)$ x^4+1 is irreducible in $\mathbb{Q}[x]$

$\Rightarrow x - 1$ is gcd By x^4+1 is irreducible in $\mathbb{Z}[x]$ and it is primitive

b) Find polynomials $a(x)$ and $b(x)$ in $\mathbb{Q}[x]$ s.t. $d(x) = a(x)f(x) + b(x)g(x)$

$x^5 - x^4 + x - 1 = (x^3 - x)(x^2 - x + 1) - x^2 + 2x - 1$

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

$-x^2 + 2x - 1 = 2 \cdot (x - 1)$

$x^2 - x + 1$
$x^3 - x \overline{)\ x^5 - x^4 + x - 1}$
$x^5 - x^3$
$-x^4 + x^3 + x - 1$
$-x^4 + x^3$
$x^3 - x^2 + x - 1$
$x^3 - x$
$-x^2 + 2x - 1$

$-x - 2$
$-x^2 + 2x - 1 \overline{)\ x^3 - x}$
$x^3 - 2x^2 + x$
$2x^2 - 2x$
$2x - 2$

$-x^2+2x-1 \;\big|\; x^3-x$

x^3-2x^2+x

$2x^2-2x$

$2x^2-4x+2$

$2x-2$

---

43. Let R be the set of polynomials in $\mathbb{Z}[x]$ having the property that the coefficient of x is equal to 0 (that is, x^2 divides $f(x)-f(0)$)

a) Prove that R is a subdomain of $\mathbb{Z}[x]$

$f_1(x)-f_2(x) \in R$?

$(f_1(x)-f_2(x))-(f_1(0)-f_2(0))$

$=(f_1(x)-f_1(0))-(f_2(x)-f_2(0))$

$\Rightarrow x^2 \mid \cdots$

$\Rightarrow$ ✓

$f_1(x)f_2(x)-f_1(0)f_2(0)$

$x^2 \mid f_1(x)f_2(x)-f_1(0)f_2(0)$

$x^2 \mid (f_1(x)-f_1(0))(f_2(x)-f_2(0))$

$x^2 \mid f_1(x)-f_1(0)$

$x^2 \mid f_2(x)-f_2(0)$

$x^2 \mid f_1(x)f_2(x)-f_1(0)f_2(x)$

$x^2 \mid f_1(0)f_2(x)-f_1(0)f_2(0)$

$\Rightarrow x^2 \mid f_1(x)f_2(x)-f_1(0)f_2(0)$

$f_1(x)f_2(x) \in R$

$\Rightarrow$ R is a subring of $\mathbb{Z}[x]$

---

b) Express x^6 as the product of irreducibles in two different ways.

$x^6 = x^3 \cdot x^3 = x^2 \cdot x^2 \cdot x^2$

x^3 is irreducible in R by $x \notin R$

c) Find an element of R that is irreducible but not prime

x^3 is irreducible

$x^2 \mid x^6$

$x^2 \mid x^3 \cdot x^3$

But $x^2 \nmid x^3$

d) Prove that x^2 and x^3 have a greatest common divisor in R and the greatest common divisor is not a linear combination of x^2 and x^3

$1 = \gcd_R(x^2, x^3)$

By $1 = x^2 f(x) + x^3 g(x)$

By deg $f(x) = 0$, or ≥ 2 $\quad f'(x) = -f(x)$

$x^3 g(x) = x^2 f'(x) + 1$

$\Rightarrow x^3 \mid x^2 f'(x) + 1$ Contradict

$\Rightarrow 1 \neq x^2 f(x) + x^3 g(x)$

e) Prove that x^5 and x^6 do not have a greatest common divisor

$x^3 \mid x^5$, $x^3 \mid x^6$

$x^2 \mid x^5$, $x^2 \mid x^6$

But $x^2 \nmid x^3$

---

44. Let R be an integral domain. Suppose that a,b,c and d are elements of R and $abc=d$. Prove that $e \in R$ is a $\gcd(a,b)$ iff $e = \gcd(b,d)$

$abc=d$

$e = \gcd(a,b)$

$e \mid a$, $e \mid b$

$\Rightarrow e \mid d$

If $e \neq \gcd(b,d)$

Let $k = \gcd(b,d)$ i.e. e, k are not associate

$\Rightarrow e \mid k$, $k \nmid e$

And $k \mid a$ by $a = d - bc$

$\Rightarrow e$ is not $\gcd(a,b)$ contradict.

---

46. Prove that $(x, y+1)$ and $(x-1, y, 1)$ are prime ideals of $\mathbb{Z}[x,y]$. Which, if any, are maximal.

$\mathbb{Z}[x,y]/(x, y+1) \cong \mathbb{Z}$

$\varphi(f(x,y)) = f(0,-1)$

$\mathbb{Z}$ is an integral domain, but not a field $\Rightarrow$ $(x, y+1)$ is prime but not maximal

$\mathbb{Z}[x,y]/(x-1, y, 1)$

$= \mathbb{Z}_3[x,y]/(x-1, y) \cong \mathbb{Z}/3\mathbb{Z}$

$\varphi(f(x,y)) = f(1,0)$

This is onto by $\mathbb{Z}/2\mathbb{Z}$ is a field $\Rightarrow$ prime by field is maximal domain.

---

47. Prove that $(x, y+1)$ is not a principal ideal of $\mathbb{Q}[x,y]$

If $(x, y+1) = (d)$

Then $d \mid x \Rightarrow d = x, d = 1$

$d \mid y+1 \Rightarrow d = y+1, d = 1$

$\Rightarrow d = 1$

But $(x, y+1) \neq \mathbb{Q}[x,y]$

By $\mathbb{Q}[x,y]/(x, y+1) \cong \mathbb{Q}$

$\Rightarrow (x, y+1)$ is maximal

$\Rightarrow (x, y+1) \neq \mathbb{Q}[x,y]$

$\Rightarrow$ ……

$\Rightarrow (x, y+1)$ is not principal

---

49. Let F be a field. Prove that $F[x,y]/(y^2-x)$ and $F[x,y]/(y^2-x^2)$ are not isomorphic.
[Hint: It may be useful to show that if R is a commutative ring with 1 and $r \in R$ then $R[t]/(t-r)$ is isomorphic to R.

pf: $F[x,y]/(y^2-x) = F[y][x]/(y^2-x) \cong F[y]$

$\varphi(f(x)) = f(y^2)$

$F[x,y]/(y^2-x^2) = F[y][x]/(y^2-x^2)$

y^2-x^2 is reducible in $F[y][x]$

$\Rightarrow F[y][x]/(y^2-x^2)$ is not integral domain

By $F[y][x]$ is U.F.D

$\Rightarrow y^2-x^2$ is not prime

$\Rightarrow F[y][x]/(y^2-x^2)$ is not integral domain

But $F[y]$ is integral domain

$\Rightarrow$ They are not isomorphic.

---

50. Prove that if F is a field, then $F[x]$ has infinitely many irreducible elements. (Hint: How do you prove that $\mathbb{Z}$ has infinitely many primes.)

pf: Suppose $F[x]$ has finitely many irreducible element

$f_1(x), \ldots, f_n(x)$

Then consider $f_1(x) f_2(x) \cdots f_n(x) + 1$

Since $F[x]$ is P.I.D $\Rightarrow$ U.F.D $\Rightarrow$ $f_i(x) \mid \cdots$

$\Rightarrow f_i(x) \mid 1$

Contradict

---

51. Let $F_2 = \mathbb{Z}/2\mathbb{Z}$

a) Prove that $x^5 - x^2 + 1$ is irreducible in $F_2[x]$

By $x \nmid x^5 - x^2 + 1$

F_2 is a field

$\Rightarrow$ Unique $q(x), r(x)$

s.t. $x^5 - x^2 + 1 = x q(x) + r(x)$

$(x+1) \nmid x^5 - x^2 + 1$

- $x^2 + x + 1$ irreducible No root.
- $x^2 + 1$ reducible
- x^2 reducible

$x^5 - x^2 + 1$ is irreducible in $F_2[x]$

$\Rightarrow$ prime in $F_2[x]$

$\Rightarrow$ maximal in $F_2[x]$ by $F_2[x]$ is a P.I.D

$x^5 - x^2 + 1$ is the minimal polynomial

$\Rightarrow F_2[x]/(x^5 - x^2 + 1) \cong \text{span}_{F_2}\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$

Suppose α is a root, we know it exists in $\mathbb{C}$

$\varphi(f(x)) = f(\alpha)$ $\quad$ Im $F_2(\alpha)$

$\Rightarrow$ kernel is $(x^5 - x^2 + 1)$ $\quad$ not $F_2[x]$

5 X 2 = 10

52. In each case below, prove or disprove the polynomial $f(x)$ is irreducible in the ring $R[x]$

(a) $x^5+7x^2+1 = x^5-x^2+1$ in $F_3[x]$
is irreducible in $F_2[x] \Rightarrow$ irreducible in $\mathbb{Z}[x]$. $\Rightarrow$ irreducible $\mathbb{Q}[x]$

(b) $f(x) = x^4 - (17i/5)x^3 + (5-3i)x^2 + ((1+(8i/15))x + (9-2i)$, $R = \mathbb{Q}[i]$
$= \{a+bi \mid a,b \in \mathbb{Q}\}$

(c) $f(x) = 2x^4+5$, $R = F_{13}$

(b) $f(x) = x^4 - \frac{17}{5}x^3 + (5-3i)x^2 + (1+\frac{8i}{15})x + 9-2i$

$\mathbb{Q}[i]$ is a field, it is principle

$f(x) = x^4 - \frac{17}{5}x^3 + (5-3i)x^2 + (1+\frac{8i}{15})x + (9-2i)$

Consider $R[i]$

$f(x)$ has solution in $\mathbb{Q}[i]$

$\Rightarrow \frac{a}{b} + \frac{c}{d}i$

$15f(x)$

$15x^4 - 51x^3 + (75-45i)x^2 + (15+8i)x + (135-30i) =$

$2 \mid 51$ $N(2) \mid 3^2 \times 17^2$

$2 \mid 75-45i$ $N(2) \mid 75^2+45^2 = 15^2(5^2+3^2) = 15^2 \cdot 34 = 15^2 \cdot 2 \cdot 17$

$2 \mid 15+8i$ $N(2) \mid 15^2+8^2 = 225+64 = 289 = 17^2$

$2 \mid 135-30i$ $N(2) \mid 135^2+30^2 = 15^2(9^2+2^2)$
$= 15^2 \cdot 85$
$= 15^2 \cdot 17 \cdot 5$
$\Rightarrow N(2) \mid 17$

$N(15)$

$N(2) = 1$
$N(2) = 17$

$a^2+b^2 = 17$
$4+i, 4-i$

Use $(4+i) \Rightarrow$

$15f(x)$ is irreducible in $\mathbb{Z}[i][x]$

And $15f(x)$ is primitive

By $N(a_5) = N(15) = 15^2$

$\Rightarrow \gcd(a_5, \dots, a_1) = 1$

$\Rightarrow 15f(x)$ is irreducible in $\mathbb{Q}[i][x]$

$\Rightarrow f(x)$ is irreducible in $\mathbb{Q}[i][x]$

$\frac{51}{4+i} = \frac{51(4-i)}{17} = 3(4-i)$

$\frac{15+8i}{4+i} = \frac{(15+8i)(4-i)}{17} = \frac{60+8+32i-15i}{17} = \frac{17(4+i)}{17} = 4+i$

$\frac{75-45i}{4+i} = \frac{15(5-3i)(4-i)}{17} = \frac{15(20-5i-12i-3)}{17} = \frac{15(17-17i)}{17} = 15(1-i)$

$\frac{135-30i}{4+i} = \frac{15(9-2i)(4-i)}{17} = \frac{15(36-2-17i)}{17} = \frac{15(34-17i)}{17} = \frac{15 \cdot 17(2-i)}{17} = 15(2-i)$

$\frac{15(2-i)}{4+i} =$

c) $(ax^2+b)(cx^2+d)$

$(ax^2+bx+c)(dx^2+ex+f)$

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

$2x^4+5 \equiv 0$
$2x^4 \equiv 8$
$x^4 \equiv 4 \pmod{13}$
$x^4 \equiv 4 \pmod{13}$
$x^2 \equiv \pm 2 \pmod{13}$

$\left(\frac{2}{13}\right)$, $\left(\frac{-2}{13}\right)$
$= -1$ $= \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right)$
$= -(1) \cdot 1$
$= -1$

---

54. Prof that $f(x) = x^6+26x^5+12x^4-40x^3+48x^2+32$ is irreducible in $\mathbb{Q}[x]$.

Consider $R[x]$

$f(\frac{2}{x}) = \frac{64}{x^6} + 26 \cdot \frac{32}{x^5} + \frac{12 \cdot 16}{x^4} - 40 \cdot \frac{8}{x^3} + 48 \cdot \frac{4}{x^2} + 32$

$x^6 f(\frac{2}{x}) = 64 + 26 \cdot 32x + 12 \cdot 16x^2 - 40 \cdot 8x^3 + 48 \cdot 4x^4 + 32x^6$

$= 32(2 + 26x + 6x^2 - 10x^3 + 6x^4 + x^6)$

irreducible
is irreducible by Eisenstein Criterion

$\Rightarrow x^6 f(\frac{2}{x})$

$f(x) = g(x)h(x)$

$f(\frac{2}{x}) = g(\frac{2}{x})h(\frac{2}{x})$

$\Rightarrow x^6 g(\frac{2}{x})h(\frac{2}{x}) = g(x)h(x)$ s.t. $g(x), h(x)$ are non-constant polynomial $\Rightarrow g'(x), h'(x)$ are non-constant

By above we show at least one of them has 0 constant polynomial

Contradict.

---

56. Let $\alpha \in \mathbb{C}$ be the root of x^3-3x+3. Show that α^4+1 and express α^{-1}, $(\alpha+1)^{-1}$, and $(\alpha^2+1)^{-1}$ in the form of $a+b\alpha+c\alpha^2$ with $a,b,c \in \mathbb{Q}$.

$\alpha^4 - 1 = 0$

$x^4 - 3x^2 + 3x = 0$

$1 \pm 3 + 3x = 0$
$\Rightarrow 3x = -4$ or 2
$\Rightarrow x = -\frac{4}{3}$ or $\frac{2}{3}$

$\alpha^3 - 3\alpha + 3 = 0$ $\quad -3 = \alpha^3 - 3\alpha$
$\alpha^{-1} = -\frac{1}{3}\alpha^2 + 1$ $\quad 1 = -\frac{1}{3}\alpha^3 + 3$

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

$(\alpha+1)^3 - 3(\alpha+1) + 3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 - 3\alpha - 3 + 3$
$= \alpha^3 - 3\alpha + 3 + 3\alpha^2 + 3\alpha - 2$
$= 3\alpha^2 + 3\alpha - 2$

$(\alpha+1)^3 - 3(\alpha+1) + 5 = 3\alpha(\alpha+1)$
$5 = -(\alpha+1)^3 + 3(\alpha+1) + 3\alpha(\alpha+1)$
$(\alpha+1)^{-1} = -\frac{1}{5}(\alpha+1)^2 + \frac{3}{5} + \frac{3}{5}\alpha = -\frac{1}{5}(\alpha+1)^2 + \frac{3}{5}(\alpha+1)$

$\alpha^3 - 3\alpha + 3 = 0$

$\frac{15(2-i)(4-i)}{17}$

$\frac{15(7-6i)}{17}$

$x = \sqrt[7]{1+\sqrt[3]{5}} \Rightarrow x^7 - \sqrt{1+\sqrt[3]{5}} = 0$

$x^7 = \sqrt{1+\sqrt[3]{5}}$

$x^{14} = 1+\sqrt[3]{5}$

$x^{14} - 1 = \sqrt[3]{5}$

$(x^{14}-1)^3 = 5$

$f(x) = (x^{14}-1)^3 - 5$

$= x^{42} - 3x^{28} + 3x^{14} - 6$

$6 \in (3)$

$6 \notin (3)^2 = (9)$

$\Rightarrow$ By Eisenstein $f(x)$ is irreducible on $\mathbb{Z}[x]$

$\Rightarrow$ $f(x)$ is irreducible on $\mathbb{Q}[x]$ by primitive then Gauss's Lemma.