Tut 8 Discussion

Let R_1 & R_2 be two rings.

Then we can define their direct sum as $R_1 \oplus R_2 = \{(a,b) \mid a \in R_1 \text{ & } b \in R_2\}$.

$$(a_1, b_1) + (a_2, b_2)$$

$$= (a_1 + a_2,\ b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2)$$

$$= (a_1 a_2, b_1 b_2)$$

$R_1 \oplus R_2$ is a ring wrt the operations defined as above.

$(0_{R_1}, 0_{R_2})$ is the additive identity and $(1_{R_1}, 1_{R_2})$ is the multiplicative identity.

Thm [Chinese Remainder Thm]

Let R be a ring and $I_1, I_2, \ldots, I_n$ be ideals of R such that $I_i + I_j = R$ for $i \neq j$. Then

$$R/\bigcap_{i=1}^{n} I_i \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n.$$

Pf: Let $f : R \longrightarrow R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$

$$f(a) = (a+I_1, a+I_2, \ldots, a+I_n)$$

check that f is a ring homomo.

$$\ker f = \bigcap_{i=1}^{n} I_i.$$

WTS f is a surjective ring homo.

Read from Dummit & Foot.

[Take $n=2$ case].

Tut 8

Q3. $\mathbb{Z}[\sqrt{-2}] = \{a + \sqrt{-2}b \mid a, b \in \mathbb{Z}\}$.

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

$$\frac{a + i\sqrt{2}b}{c + i\sqrt{2}d} = r + i\sqrt{2}s.$$

where $r, s \in \mathbb{R}$.

Follow the steps similar to $\mathbb{Z}[i]$.

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

$$N(a+b\omega) = (a+b\omega)(a+b\omega^2)$$
$$= a^2 - ab + b^2.$$

With the above norm fun^n follow the steps similar to $\mathbb{Z}[i]$.

Q8. $f, g \in \mathbb{Z}[x]$ are relatively prime in $\mathbb{Q}[x]$ iff $(f,g)\mathbb{Z}[x] \cap \mathbb{Z} \neq (0)$.

Pf: Let f & g are relatively prime in $\mathbb{Q}[x]$.

$$\gcd(f,g) = 1 \text{ in } \mathbb{Q}[x].$$

Since $\mathbb{Q}[x]$ is a PID

$$\therefore \quad 1 = fu + gv \quad \text{where } u, v \in \mathbb{Q}[x]$$

Clearing the denominator of u & v from side we get

$$m = fu_1 + gv_1 \quad \left\{ \begin{array}{l} \text{where} \\ m \in \mathbb{Z}, \\ u_1, v_1 \in \mathbb{Z}[x] \end{array} \right.$$

$$\Rightarrow \quad m \in (f,g)\mathbb{Z}[x] \cap \mathbb{Z} \neq (0)$$

Q4. F is a subfield of $\mathbb{C}$.

WTS an irreducible poly in $F[x]$ has no multiple roots!

Let $f(x) \in F[x]$ is irreducible. then its derivative $f'(x) \in F[x]$.

Since f is irreducible over $F[x]$.

$$\gcd(f, f') = 1 \text{ in } F[x].$$

$$\Rightarrow \quad 1 = fu + f'v \text{ for some } u, v \in F[x].$$

$$\Rightarrow \quad 1 = fu + f'v \text{ in } \mathbb{C}[x]$$

$$\Rightarrow \quad 1 = \gcd(f, f') \text{ in } \mathbb{C}[x].$$

If $f(x)$ has a multiple root say $\alpha \in \mathbb{C}$

$$f(x) = (x-\alpha)^2 g(x).$$

$$f'(x) = 2(x-\alpha) g(x) + (x-\alpha)^2 g'(x)$$

$\Rightarrow$ α is a root of $f'(x)$ also.

i.e $(x-\alpha)$ divides both $f(x)$ & $f'(x)$ in $\mathbb{C}[x]$.

i.e $\gcd(f, f') \neq 1$ in $\mathbb{C}[x]$

which is a contradiction.

Thus $f(x)$ can't have multiple roots in $\mathbb{C}$.

Let $n = p_1^4 p_2$.

where $p_1 \equiv 3 \pmod 4$. i.e $N(p_1) = p_1^2$

$p_2 \equiv 1 \pmod 4$.

$p_2 = \pi\bar{\pi}$

$N(p_1 \bar{\pi}) = p_1^2 p_2 = n$

$p_1\bar{\pi} = p_1(a+ib) = \underbrace{p_1 a}_{A} + \underbrace{i p_1 b}_{B}$

$N(p_1^2 \bar{\pi}) = p_1^4 p_2$

$\mathbb{Z}[x]/\mathbb{Z} \cong \mathbb{Z}[x]$ as gp isomorphism ?

$f : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$.

$f(g(x)) = g'(x)$.

$x^2/2 \longleftarrow x$