03/11

Proposition

Let R be an integral domain, and $f(x) \in R[x]$ be a non-zero polynomial of degree d. Then $f(x)$ has atmost 'd' roots.

(Proof)

We prove the assertion by induction on degree of polynomials.

If $\deg f = 1$, then $f(x) = ax+b$ where $a \neq 0$. Then $f(x)$ has exactly one root, i.e, $x = -b/a$.

Let $\deg f = n$ and suppose the result is true for all polynomials of degree $< n$.

If f has no roots, then we are done.

We may assume that f has a root $a \in R$

Then $f(x) = (x-a)g(x)$ for some $g(x) \in R[x]$ where $\deg(g) = n-1$

$$\begin{aligned}\text{No. of roots of } f &= 1 + \text{No. of roots of } g \\ &\leq 1 + (n-1) \\ &= n\end{aligned}$$

* The result is not true if R is a skew-field. Counterexample is the Quaternions.

(Exercise)

We have classified groups of order pq $(p>q)$ and $q \nmid p-1$. Study about the groups when $q \mid p-1$.

Generators of Ideals

Let R be a ring and $S \subseteq R$.
We say that an ideal I of R is generated by S if every element of I can be written as a finite sum

$a_1 s_1 + \dots + a_m s_m$ for some

$s_1, \dots, s_m \in S$, $a_1, a_2, \dots \in R$.

We write $I = (S)$ (or) $\langle S \rangle$

Definitions

- An ideal I of R is said to be finitely generated if $I = (S)$ for some finite subset $S \subseteq R$.

An ideal I is called a principal ideal if $I = \langle a \rangle$ for some $a \in R$

An Integral Domain in which every ideal is principal is called Principal Ideal Domain.

Examples

$\mathbb{Z}$ is a P.I.D

Proof

Let $I \trianglelefteq R$

If $I = \{0\} \Rightarrow \langle 0 \rangle$

Suppose $I \neq \{0\}$

Then $I_{>0} = \{ a \in I \mid a > 0 \} \neq \emptyset$

Let $m = \min\limits_{a \in I_{>0}} a$

Let $b \in I$. By remainder theorem, there exist $q, r \in \mathbb{Z}$, $0 \leq r < m$ such that

$b = qm + r$

$\Rightarrow r = b - qm$ $(r \in I)$

$\Rightarrow r = 0$ (by minimality)

$\Rightarrow I = m\mathbb{Z}$

$\Rightarrow I = (m)$

- $K[x]$ is a PID (Exercise!)

K → comes from German word Korper

$I \trianglelefteq K[x]$

$I = (0)$

$I_{>0} = \{ f(x) \in I \mid \deg f(x) > 0 \}$

$J = \{ \deg f(x) \mid f(x) \in I_{>0} \}$

$$d = \deg f(x) = \min_{a \in I_{>0}} a$$

$g(x) = f(x)\, q(x) + r(x)$

$\Rightarrow r(x) = g(x) - f(x)\, q(x)$ $\quad 0 \leq \deg(r(x)) < d$

$\Rightarrow r(x) = 0$

- Is $R[x,y]$ a PID?

<u>Example</u>

- $\varphi : \mathbb{R}[x,y] \longrightarrow \mathbb{R}[t]$

$\quad f(x,y) \longmapsto f(t^2, t^3)$

$\ker(\varphi) = ?$

<u>Claim</u> :- $\ker(\varphi) = \langle y^2 - x^3 \rangle$

$(\Leftarrow)$ clearly $\ker(\varphi) \supseteq \langle y^2 - x^3 \rangle$

$g(x,y)(y^2 - x^3) \in \ker(\varphi)$

$(\Rightarrow)$ Let $f(x,y) \in \ker \varphi$

$f(x,y) = p(x,y)(y^2 - x^3) + r(x,y)$

Notice that $\deg_y r(x,y) \leq 1$

$\Rightarrow f(x,y) = p(x,y)(y^2 - x^3) + r(x)\, y + s(x)$

$\Rightarrow \underbrace{r(t^2)\, t^3}_{\text{odd degree terms}} + \underbrace{s(t^2)}_{\text{even degree terms}} = 0$ $\quad \Rightarrow \ker(\varphi) \subseteq \langle y^2 - x^3 \rangle$

$\Rightarrow \boxed{\ker(\varphi) = \langle y^2 - x^3 \rangle}$

$\Rightarrow r(x) = 0$ and $s(x) = 0$

- $ev_{(a,b)} : \mathbb{R}[x,y] \longrightarrow \mathbb{R}$

$$f(x,y) \longmapsto f(a,b)$$

Claim: $\ker(ev_{(a,b)}) = \langle x-a, y-b \rangle$

$$\mathbb{R}[x,y] \to (\mathbb{R}[y])[x]$$

$$f(x,y) = p(xy)(x-a) + r(y) \leftarrow *$$

$$= p(xy)(x-a) + q(y)(y-b) + c$$

$c = 0$ (Trivially!)

$\Rightarrow \ker(ev_{(a,b)}) = \langle x-a, y-b \rangle$

Exercise

Generalize for 'n' variables!

Operations on Ideals

- Intersection

$\{ I_\alpha \mid \alpha \in \Lambda \}$ $\qquad \Lambda \to$ indexing set

$\bigcap_{\alpha \in \Lambda} I_\alpha$ is an ideal

- Sum

$I, J \trianglelefteq R$ $\qquad I+J = \{ a+b \mid a \in I, b \in J \}$

- Product

$I, J \trianglelefteq R$ $\qquad IJ = \{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \}$

Exercise

Compute $m\mathbb{Z} + n\mathbb{Z}$, $m\mathbb{Z} \cap n\mathbb{Z}$

Quotient

Let R be a ring, and $I \trianglelefteq R$

$$R/I := \{ a + I \mid a \in R \}$$

- $a + I = a' + I$

  $\Rightarrow a - a' \in I$

- $(a + I) + (b + I) = (a+b) + I$
- $(a + I)(b + I) = ab + I$

  check $ab + I = a'b' + I$

  $\Rightarrow ab - a'b' \in I$

  $\Rightarrow ab - a'b + a'b - a'b' \in I$

  $\Rightarrow (a - a')b + a'(b - b') \in I$

Analogous to $G \to G/N$, we have $R \to R/I$

$a \mapsto a + I$

First Isomorphism Theorem

Let R, S be rings and $\varphi : R \to S$ be a surjective ring homomorphism.

Then there is a map (ring isomorphism)

$$\tilde{\varphi} : R/\ker(\varphi) \to S$$

(Proof)

$$\begin{tikzcd}
R \arrow[r, "\varphi"] & S \\
R/\ker(\varphi) \arrow[u] \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

$$\tilde{\varphi} : R/\ker(\varphi) \to S$$
$$\bar{r} \mapsto \varphi(r)$$

- Well-defined and one-one

  $\bar{r} = \varphi(r) = \bar{r}' = \varphi(r') \iff \bar{r} - \bar{r}' \in \ker\varphi$

  $\iff \varphi(r - r') = 0$

  $\iff \varphi(r) = \varphi(r')$

- $\tilde{\varphi}(\bar{r} + \bar{r'})$
  $= \tilde{\varphi}(\overline{r + r'})$
  $= \varphi(r + r')$
  $= \varphi(r) + \varphi(r')$
  $= \tilde{\varphi}(\bar{r}) + \tilde{\varphi}(\bar{r'})$

- $K[x] \to K$
  $f(x) \mapsto f(a)$

  $\ker(ev_a) = \langle x - a \rangle$

  $\Rightarrow \quad K[x] / \langle x-a \rangle \cong K$

- $K[x, y] \to K$
  $f(x, y) \mapsto f(a, b)$

  $\ker(ev_{(a,b)}) = \langle x - a, \ y - b \rangle$

  $\Rightarrow \quad K[x,y] / \langle x-a, y-b \rangle \cong K$

  Similarly $\quad K[x_1, \dots, x_n] / \langle x - a_1, \dots, x - a_n \rangle \cong K$

2^{nd} Isomorphism Theorem

Let A be a subring of R and $B \triangleleft R$

then ① $A + B$ is a subring of R
② $A \cap B \triangleleft A$
③ $A+B/_B \cong A/_{A \cap B}$

- $A+B = \{a + b \mid a \in A, b \in B\}$

  $(a_1 + b_1)(a_2 + b_2) = a_1 a_2 + b_1(a_2 + b_2) + b_2(a_1)$
  $\in A + B$

- $A \to A+B/_B$
  $a \mapsto a + B$ (It is a homomorphism)

  $\ker(\varphi) \to B \cap A$ (Trivial!)

Third Isomorphism Theorem

$I, J \trianglelefteq R$, $I \subseteq J$. Then

① $J/I \trianglelefteq R/I$

② $\dfrac{R/I}{J/I} \cong R/J$

- $\dfrac{R/I}{J/I} \cong R/J \Rightarrow \varphi : R/I \to R/J$

$r + I \mapsto r + J$

$r + I \in \ker(\varphi) \Rightarrow r + J = J$

$\Rightarrow r \in J$

$\Rightarrow r \in J/I$

Correspondence Theorem (Exercise!)

Let R be a ring and $I \trianglelefteq R$

Then there is an inclusion preserving bijection

$\{\text{ideals of } R/I\} \longleftrightarrow \{\text{ideals of } R \text{ containing } I\}$

Reading Exercise :- Chapter-1 of Modern number theory by Ireland / Rosen