Chapter 15 Ring Homomorphisms

Definitions Let R_1, R_2 be rings. A function $\phi : R_1 \to R_2$ is a ring homomorphism if $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R_1$. If in addition that ϕ is bijective, then ϕ is a ring isomorphism.

This works for negative integers if r^{-1}, $\phi(r)^{-1}$ exists

Theorem 15.1-2 let $\phi : R_1 \to R_2$ be a ring homomoprhism.

$r + r + \cdots + r$

(1) For any $r \in R$ and positive integer n, $\phi(nr) = n\phi(r)$ and $\boxed{\phi(r^n) = \phi(r)^n}$.

$\phi(nr) = \cancel{n\phi(r)}\ n\phi(r)$ also holds for negative integer n,

(2) If A is a subring of R_1, then $\phi(A)$ is a subring of R_2.

(3) If A is an ideal of R_1, then $\phi(A)$ is an ideal of $\phi(R_1)$.

(4) If B is a subring/ideal of R_2, then $\phi^{-1}(B)$ is a subring/ideal of R_1. In particular, $Ker(\phi)$ is an ideal.

(5) If A is a commutative subring of R, then $\phi(A)$ is commutative.

(6) If R_1 has a unity, then $\phi(1)$ is a unity of $\phi(R_1)$.

(7) The map ϕ is injective if and only if $Ker(\phi) = \{0\}$.

Theorem 15.3 Let $\phi : R_1 \to R_2$ be a ring homomorphism. Then $x + Ker(\phi) \mapsto \phi(x)$ is an isomorphism from $R_1/Ker(\phi)$ to $\phi(R_1)$.

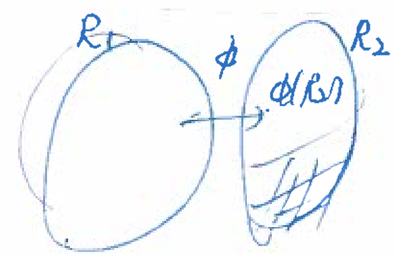
$Ker(\phi) = \{ x \in R_1 : \phi(x) = 0_2 \}$ is an ideal of R_1

By group theory, $Ker(\phi)$ is a subgroup of R_1 under $+$

$x \in Ker(\phi)$, $y \in R_1 \Rightarrow \phi(xy) = \phi(x)\phi(y) = 0_2 y = 0$.

$\phi(yx) = \phi(y)\phi(x) = y\, 0_2 = 0$

$\therefore xy, yx \in Ker(\phi)$



$R_1/Ker(\phi)$ is a ring.

$\Phi : R_1/Ker(\phi) \to \phi(R_1)$

defined by $\Phi(r + Ker(\phi)) = \phi(r) \in \phi(R_1)$

is an ring isomorphism

1° well-defined of Φ By group Theory

2° $\Phi : R_1/Ker(\phi) \to \phi(R_1)$ is injective by group theory

3° Surjective: By definition, every $\phi(r) \in \phi(R_1)$

$\Phi(r + Ker(\phi)) = \phi(r)$.

4° $\Phi((x + Ker\,\phi)(y + Ker(\phi))) = \Phi(xy + Ker(\phi)) = \phi(xy)$

Theorem 15.4 Every ideal A of a ring R is the kernel of the ring homomorphism $\phi : \cancel{A}R \mapsto R/A$ defined by $\phi(a) = a + A$.

$A \subseteq R$, an ideal

$R/A = \{ r + A : r \in R \}$.

Then $\cancel{\phi : A \to}$ $\phi : R \to R/A$.

defined by $\phi(r) = r + A$.

Then $\phi(r) = 0 + A \iff r \in A$.

$\therefore \ \mathrm{Ker}(\phi) = A$. $\square$

To illustrate how to extend properties of $\mathbb{Z}$ to $\mathbb{F}[x]$.

integral domain

Chapter 16 Polynomial Rings

Notation Let R be a commutative ring. The ring of polynomials over R in the indeterminate x is the set

$$R[x] = \{a_0 + \cdots + a_n x^n : n \in \mathbb{N},\ a_0, \ldots, a_n \in R\}.$$

We can consider equality, addition, multiplication and degree of a polynomial $f(x) \in R[x]$.

Theorem 16.1 If $\mathbb{D}$ is an integral domain, then $\mathbb{D}[x]$ is an integral domain.

In $\mathbb{Z}_4[x]$. $2x, 2x \in \mathbb{Z}_4[x]$ nonzero $(2x)(2x) = 4x = 0$.

Proof: $\mathbb{D}[x]$ is a commutative ring with unity $f(x) = 1$.

No zero divisor because $f(x), g(x) \in \mathbb{D}[x]$ are non-zero. Then consider two cases.

① $f(x) = f_0$, $g(x) = g$, are constant polynomials. not equal to zero. Then $f(x)g(x) = fg \neq 0$ in $\mathbb{D}$.

② $f(x) = f_0 + \cdots + f_n x^n$, $g(x) = g_0 + \cdots + g_m x^m$. n or $m > 0$.

Then $f(x)g(x) = f_n g_m x^{n+m} + \cdots + f_0 g_0$ has degree > 0 as $f_n g_m \neq 0$.

Theorem 16.2 If $\mathbb{F}$ is a field, and $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, then there exist unique polynomials $q(x), r(x)$ such that $f(x) = g(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(g(x))$.

By induction on m. $\deg f(x) = m$, $\deg g(x) = n$

① If $m < n$, then $f(x) = g(x) \cdot 0 + r(x)$, $r(x) = f(x)$ has degree $< n$.

② $f(x) = f_0 + f_1 x + \cdots + f_m x^m$
$g(x) = g_0 + \cdots + g_n x^n$. $m \geq n$

$a \overline{)\, b}$ and r

Anything: {

Recall

A field $\mathbb{F}$ is always an integral domain.

$\mathbb{F}$ is commutative with unity.

If $a \neq 0$ is a zero divisor, then $\exists b \neq 0$ s.t. $ab = 0$

[illegible] is not [illegible]

Recall. $\deg f(x)$

~~Define~~ Let $f(x) = f_0 + \cdots + f_n x^n$,

$$\begin{cases} f_n \neq 0,\ n > 0 & ① \\ f_0 \neq 0 & ② \\ 0 & ③ \end{cases}$$

Then $\deg(f(x)) = \begin{cases} n \\ 0 \\ -\infty . \end{cases}$

Fact: $\deg(f(x)\,g(x)) = \deg(f(x)) + \deg(g(x))$

(Cont'd Proof of Theorem 16.2)

$$\begin{array}{r|l} & g_n^{-1} f_m \cdot x^{m-n} \\ \hline g_n x^n + \cdots + g_0 & f_m x^m + \cdots + f_0 \\ & f_m x^m + c_{m-1} x^{m-1} + \cdots + 1 \end{array}$$

$$\begin{array}{r|l} & \tfrac{3}{4} x \\ \hline 4x^2 + 1 & 3x^3 + 2x + 1 \end{array}$$

$\therefore$ $f_m x^m + \cdots + f_0 = (g_n^{-1} f_m x^{m-n})(g(x)) + R(x)$ ~~with~~ where $R(x)$ has degree at most $m-1$

Then $R(x) = q_1(x)\,g(x) + r(x)$ by induction degree $r(x) < n$

So $f(x) = g_n^{-1} f_m x^{m-n} g(x) + q_1(x)\,g(x) + r(x)$

$q(x)\,g(x) + r(x)$.

Theorem If $\mathbb{F}$ is a finite field, then the nonzero elements in $\mathbb{F}$ is a cyclic group under multiplication.

$(\mathbb{F}^*, \cdot)$ is isomorphic to

$$\mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$$

by the F.T. of F.G.A group

If $p_1, \ldots, p_k$ are distinct primes

then $(1, \ldots, 1)$ has order

$p_1^{r_1} \cdots p_r^{r_k}$ and

$(1, \ldots, 1)$ will be a generator of the group.

Assume $p_1, \ldots, p_k$ are not distinct,

then ~~the max or~~ $x^m = 1$.

for $m = \operatorname{lcm}(p_1^{r_1}, \ldots, p_k^{r_k}) < p_1^{r_1} \cdots p_k^{r_k}$.

However, for $f(x) = x^m - 1$.

$f(a) = 0 \quad \forall a \in \mathbb{F}^*$

So $f(x)$ has $p_1^{r_1} \cdots p_k^{r_k}$ zero !!!

$\mathbb{Z}_3[x] / \langle x^2+1 \rangle \leftarrow A$

has 9 elements

8 non-zero element

$= \{ax+b+A : \cancel{ax+b}\ a, b \in \mathbb{Z}_3\}$

$\{\cancel{0+A}, 1+A, 2+A$

$x+A \quad 2x+A$

$1+x+A \quad 2+x+A$

$1+2x+A \quad 2+2x+A\}$

A field

$\mathbb{Z}_5[x] / \langle x^2+2 \rangle$

with 25 elements

$\cancel{(x^2+c) = (x+a)(x+b)}$

$\{ax+b+A \mid a, b \in \mathbb{Z}_5\}$

Corollary Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, $a \in \mathbb{F}$. Then the following holds.

(a) $f(x) = (x-a)q(x) + f(a)$, i.e., $f(a)$ is the remainder.

(b) $(x-a)$ is a factor of $f(x)$ if and only if $f(a) = 0$.

(c) If $\deg(f(x)) = n$, then $f(x)$ has at most n zeros, counting multiplicities.

$$x-a \overline{\big)\, f(x)}^{\,g(x)}$$
$$-(x-a)g(x)$$
$$r = f(a)$$

a is a zero of $f(x)$.

Proof:

(a) If $f(x) = (x-a)g(x) + r$.
then $f(a) = (a-a)g(a) + r$ $\therefore r = f(a)$

(b) $\therefore f(x) = (x-a)g(x) \iff f(a) = 0$.

(c) Proof by induction on n.

If $n=1$, i.e., $f(x) = ax - b$, $a \neq 0$
then $a^{-1}b$ is a zero.

Suppose the statement holds for polynomials of degree at most k
& $f(x) = f_0 + \cdots + f_{k+1}x^{k+1}$ has degree $k+1$.

Case 1 If $f(x)$ has no zero, we are done.

Case 2 If $f(x)$ has a zero "a". then
$f(x) = (x-a)\hat{f}(x)$ where $\deg \hat{f}(x) = k$.

By induction. $\hat{f}(x)$ has at most k zeros
Note that $f(b)=0 \iff b=a$ or b is a zero of $\hat{f}(x)$.

Construction of solution to polynomials in a larger field

Suppose $f(x) \in \mathbb{F}[x]$.

Decompose $f(x) = \underline{f_1(x)} \cdots \underline{f_k(x)}$ as irreducible polynomials.

Then construct $\mathbb{F}[x] / \langle f_1(x) \rangle \leftarrow A$ $\quad f_1(x)$ has degree m.

is a field $\mathbb{E} = \{ a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + A :$

$a_0, a_1, \cdots, a_{m-1} \in \mathbb{F} \}$

Suppose $f_1(x) = b_0 + b_1 x + \cdots + b_m x^m$, $m > 2$

Then

① $\mathbb{F}$ is isomorphic to the subfield

$$\{ \varphi + A : \varphi \in \mathbb{F} \}.$$

② The element $x + A$ in $\mathbb{E}$ satisfies.

$$f_1(y) = \underbrace{b_0}_{} + \overset{\in \mathbb{E}}{b_1} \cdot y + \cdots + b_m y^m$$

$$f_1(x+A) = (b_0 + A) + (b_1 + A)(x+A) + (b_2 + A)(x+A)^2 + \cdots + (b_m + A)(x+A)$$

$$= (b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m) + A$$

$$= f_1(x) + A = \underline{\underline{0 + A}}$$