Reference

Friday, April 19, 2024 12:05 PM

Reference: http://abstract.ups.edu/aata/aata.html chapter 10, 16 and 17

Factor groups and normal subgroups

Tuesday, April 30, 2024 12:07 PM

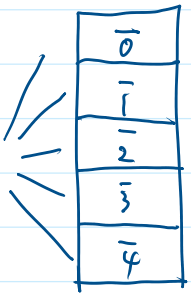
Motivation:

$\mathbb{Z} \longrightarrow \mod n$

mod 2	mod 3	mod 4
mod 5	...	....

$\mathbb{Z}/5\mathbb{Z}$

5 congrence class



remainder = 0

remainder = 1

remainder = 4

If a, b are in the same congruence class:

$a \equiv b \mod n$

Group $(\mathbb{Z}, +)$

Subgroups $2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, \cdots$

Caution:

- nZ is subgroup of Z
- Z/nZ is not subgroup of Z

$\mathbb{Z}$

$0+5\mathbb{Z}$	$\{\cdots, -10, -5, 0, 5, 10, \cdots\}$
$1+5\mathbb{Z}$	$\{\cdots, -9, -4, 1, 6, 11, \cdots\}$
$2+5\mathbb{Z}$	$\{\cdots, -8, -3, 2, 7, 12, \cdots\}$
$3+5\mathbb{Z}$	$\{\cdots -7, -2, 3, 8, 13, \cdots\}$
$4+5\mathbb{Z}$	$\{\cdots, -6, -1, 4, 9, 14, \cdots\}$

"Cosets partition the group"

Here we use a subgroup $5\mathbb{Z}$ and all its left cosets to represent $\mathbb{Z}$. Other subgroups can do the same.

Def: $H < G$ is **normal** in G if $gH = Hg \ \forall g \in G$. That is, a normal subgroup of a group G is one in which the left and right cosets are precisely the same. Denote normal subgroup as $H \trianglelefteq G$.

Example: G abelian, then $H \trianglelefteq G \ \forall H < G$.

$gh = hg \ \forall g \in G$ and $h \in H$

$\Rightarrow gH = Hg \ \forall g \in G$

abelian $\Rightarrow$ normal

The reverse is not true

Theorem: $N < G$, the following are equivalent:

1. $N \trianglelefteq G$
2. $gNg^{-1} \subset N \ \forall g \in G$
3. $gNg^{-1} = N \ \forall g \in G$

↑ because $gN = Ng$

Def: If $N \trianglelefteq G$, then cosets of N in G form a group G/N under the operation $(aN)(bN) = abN$. This group is called the factor or quotient group of G and N.

$G \rightarrow G/N$ factor group or quotient group

G: group; N: normal subgroup

Theorem: $N \trianglelefteq G$. The cosets of N in G form a group G/N of order $[G:N]$

Proof: Group operation on G/N is $(aN)(bN) = abN$.

1. operator is associative and closed
2. identity exists → N, since $(N)(aN) = aN$
3. every element has inverse: $gN \rightarrow g^{-1}N$ $\quad (g^{-1}N)(gN) = N$ ↑ identity

- It is very important to remember that the elements in a factor group are sets

of elements in the original group.

Example: $3\mathbb{Z} \leq \mathbb{Z}$. Cosets are:

$0+3\mathbb{Z} = \{\cdots, -3, 0, 3, 6, \cdots\}$
$1+3\mathbb{Z} = \{\cdots -2, 1, 4, 7, \cdots\}$
$2+3\mathbb{Z} = \{\cdots, -1, 2, 5, 8, \cdots\}$

$\Big\}$ = elements of $\mathbb{Z}/3\mathbb{Z}$ (cosets of $3\mathbb{Z} \leq \mathbb{Z}$)

$\mathbb{Z}/3\mathbb{Z}$:

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

We said $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, but in fact $\mathbb{Z}/3\mathbb{Z} = \{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$.

In general, $n\mathbb{Z} \leq \mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, \cdots, (n-1)+n\mathbb{Z}\}$

Rings

Wednesday, May 1, 2024 12:28 AM

Def: Ring → $+$ and $\cdot$ $(R,+)$, $(R,\cdot)$

1) $+$: abelian group
2) $\cdot$: monoid (associativity + identity)
3) $+$ and $\cdot$; $\cdot$ is distributive

$$a\cdot(b+c) = ab+ac$$
$$(b+c)\cdot a = ba+bc$$

Ring without identity is called "rng"
If ab = ba, it is a commutative ring

$\mathbb{Z}$ is integral domain, but not a field

Def: A commutative ring is called **integral domain** if $\forall a,b\in R$ s.t. $ab=0$, either $a=0$ or $b=0$.

zero divisors

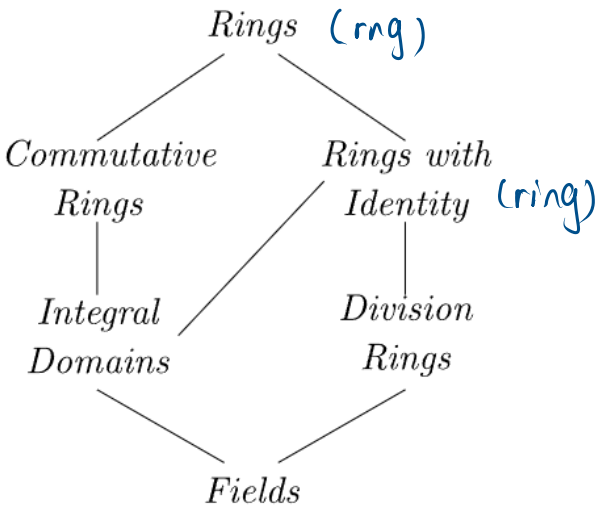
if $a\neq 0$, $b\neq 0$ but $a\cdot b = 0$, then not integral domain
for example, $2\cdot 3 = 6 = 0$ in $(\mathbb{Z}/6\mathbb{Z},\cdot)$

Def: A **division ring** is a ring R in which every nonzero element in R is a unit.

↑ $\forall a\neq 0\in R$, $\exists$ unique a^{-1} s.t $aa^{-1} = a^{-1}a = 1$.

Def: A commutative division ring is a **field**.

$\Leftrightarrow$ A field is a commutative ring where every nonzero element has inverse.



Example: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields

Integral domains and fields

Wednesday, May 1, 2024 12:29 AM

Example: Gaussian Integers

$\mathbb{Z}[i] = \{ m+ni : m,n \in \mathbb{Z} \}$ is a ring
is a subring of $\mathbb{C}$
but not a field

Proof: Let $\alpha = a+bi$ be a unit in $\mathbb{Z}[i]$. Then $\bar{\alpha} = a-bi$ is also a unit since if $\alpha\beta = 1$ then $\bar{\alpha}\bar{\beta} = 1$. If $\beta = c+di$, then:

$$1 = \alpha\beta\,\bar{\alpha}\bar{\beta} = \underbrace{(a^2+b^2)(c^2+d^2)}_{=\pm 1}$$

$\Rightarrow a^2+b^2 = \pm 1$

$(a+bi)(a-bi) = \pm 1$

$a+bi = \pm 1$ or $\pm i$

$\Rightarrow$ units are ± 1 and $\pm i$

$\Rightarrow$ not every element has inverse

$\Rightarrow$ not a field.

"extend" $\mathbb{Q}$ to handle $\sqrt{2}$

Example: The set $\mathbb{Q}(\sqrt{2}) = \{ a+b\sqrt{2} : a,b \in \mathbb{Q} \}$ is a field.

The inverse of every element $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is:

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

Proposition (cancellation law)

Let D be a commutative ring. Then D is integral domain iff $\forall a \neq 0 \in D$ with $ab = ac$, we have $b = c$.

Proof: ($\Rightarrow$) Suppose D integral domain. Then D has no zero divisor.
Let $ab = ac$ with $a \neq 0$.

$ab = ac$

$ab - ac = 0$

$a(b-c) = 0$

$a = 0$ or $b = c$ ✓

impossible

$(ab = ac \Rightarrow b = c)$

($\Leftarrow$) Suppose cancellation is possible. Pick any $a \neq 0 \in D$. then:

(whenever) $ab = 0$

$ab = a \cdot 0$

$b = 0 \rightarrow$ a is not zero divisor

Theorem: Every finite integral domain is field.

proof: Let D be finite integral domain.

$D^* = D \setminus \{0\}$

he show every element in D^* has inverse $\rightarrow$ D^* is field.

Pick any $a \in D^*$, define a map $\lambda_a : D^* \rightarrow D^*$

$\lambda_a(d) = ad \quad a \neq 0 \quad d \neq 0$

property: if $a \neq 0$ and $d \neq 0$, then $ad \neq 0$

Injective: $d_1, d_2 \in D^*$, $\lambda_a(d_1) = \lambda_a(d_2)$

$ad_1 = ad_2$

$d_1 = d_2$ (by cancellation law)

Surjective: D^* is finite set

Def: For any $n \in \mathbb{Z}^+$ and any $r \in R$, write $\underbrace{r + r + \cdots + r}_{n \text{ times}} = nr$.

Define characteristic of a ring R to be the least positive integer n s.t. $nr = 0 \ \forall r \in R$. If n does not exist, characteristic $= 0$.

$$\text{char}(R) = n \quad / \quad \text{char}(R) = 0$$

Example: p prime, $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

is a field, since every element in $(\mathbb{Z}/p\mathbb{Z})^*$ has inverse.

Pick $a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$, then $pa = 0$ since the order of any nonzero element in $\mathbb{Z}/p\mathbb{Z}$ is p.

↖ Corollary of Lagrange:

> **Corollary 6.11.** *Suppose that G is a finite group and $g \in G$. Then the order of g must divide the number of elements in G.*

Lemma: R ring. If 1 has order n, then $\text{char}(R) = n$.

Proof: 1 has order $n \Rightarrow n$ is the smallest integer s.t. $n1 = 0$

$\Rightarrow \forall r \in R: \ nr = n(1r) = (n1)r = 0r = 0$

→ alternative definition of $\text{char}(R)$:

$$n1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0 \Rightarrow \text{char}(R) = n$$

Theorem: char(integral domain) $= p$ or 0

Proof: Let D be integral domain. Suppose $\text{char}(D) = n \neq 0$.

For the sake of contradiction, suppose n is not prime. Then $n = ab$ where $1 < a < n$ and $1 < b < a$. Then:

$(a < n, \ b < n)$

$$n1 = 0$$

where $1 < a < n$ and $1 < b < n$. Then: $(a<n, b<n)$

$n1 = 0$

$(ab)1 = 0$

$(a1)(b1) = 0$

$a1 = 0$ or $b1 = 0$ (since D is integral domain)

↑ ↑

$\text{Char}(D) = \min(a,b)$, Contradiction

$\Rightarrow$ n must be prime.

→ char(field) = p or 0

↑ ↑

$GF(p^n)$ subfields of $\mathbb{C}$

Polynomial rings

Thursday, May 2, 2024 1:00 PM

Def: Polynomial ring. R commutative ring

$$f(x) = \sum_{i=0}^{n} a_i x^i$$ Polynomial over R with indeterminate x

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \qquad a_i \in R, \quad a_n \neq 0$$

a_i: Coefficients

a_n: leading coefficient

if $a_n = 1$, polynomial is monic

n: degree $\rightarrow \deg f(x) = n$

We will denote the set of all polynomials with coefficients in a ring R by R[x].

Equal: $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ $\quad [a_0, a_1, \cdots, a_n, 0]$

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$ $\quad [b_0, b_1, \cdots, b_n, 0]$

Then $p(x) = q(x)$ iff $a_i = b_i \ \forall i \geq 0$

Sum: $p(x) + q(x) = c_0 + c_1 x + \cdots + c_k x^k$

$$c_i = a_i + b_i$$

Product: $p(x)q(x) = c_0 + c_1 x + \cdots + c_k x^k$

$$c_i = \sum_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$$

Example: $p(x) = 3 + 3x^3$ in $\mathbb{Z}/12\mathbb{Z}[x]$

$q(x) = 4 + 4x^2 + 4x^4$

Sum: $p(x) + q(x) = 7 + 0x + 4x^2 + 3x^3 + 4x^4$

Product: $p(x)\,q(x) = (3 + 3x^3)(4 + 4x^2 + 4x^4)$

product: $p(x)\,q(x) = (3+3x^3)(4+4x^2+4x^4)$

$= 12 + 12x^2 + 12x^4 + 12x^3 + 12x^5 + 12x^7$

$\equiv 0 \bmod 12$

→ If R is not integral domain, do not expect $R[x]$ to be integral domain.

Theorem: R commutative ring, then $R[x]$ is commutative ring.

Proposition: $p(x), q(x) \in R[x]$, R integral domain. Then

$$\deg p(x) + \deg q(x) = \deg(p(x)q(x))$$

And $R[x]$ is integral domain.

Proof: $p(x) = a_m x^m + \cdots + a_1 x + a_0$ $\quad a_m \neq 0$

$q(x) = b_n x^n + \cdots + b_1 x + b_0$ $\quad b_n \neq 0$

$p(x)\,q(x) = a_m b_n x^{m+n} + \cdots\cdots$

$a_m b_n \neq 0$ "lower terms"

Since R is integral domain, so x^{m+n} term must exist

$\Rightarrow p(x)q(x) \neq 0$

$p(x) \neq 0$ and $q(x) \neq 0$ implies $p(x)q(x) \neq 0$ $\Rightarrow$ $R[x]$ is integral domain.

Def: $R[x,y]$: ring of polynomials in two indeterminates x and y with coefficients in R

(e.g. $x^2 - 3xy + 2y^3$)

(e.g. $x^2 - 3xy + 2y^3$)

In general, $R[x_1, x_2, \cdots, x_n]$.

Theorem: R commutative ring, $\alpha \in R$. Then $\phi_\alpha : R[x] \to R$ is a ring homomorphism:

$$\phi_\alpha(p(x)) = p(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0$$

where $p(x) = a_n x^n + \cdots + a_1 x + a_0$. ϕ_α is the evaluation homomorphism at α.

Ring homomorphism: $\phi : R \to S$

$$\phi(a+b) = \phi(a) + \phi(b) \qquad \forall a, b \in R.$$
$$\phi(ab) = \phi(a)\phi(b)$$

If ϕ is bijection then ϕ is isomorphism.

The division algorithm

Thursday, May 2, 2024 2:52 PM

Theorem: Division Algorithm:

$f(x), g(x) \in \bar{F}(x)$, $\bar{F}$ field, $g(x) \neq 0$.
Then $\exists$ unique polynomials $q(x), r(x) \in \bar{F}[x]$ s.t.:

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

where $\deg r(x) < \deg g(x)$ or $r(x) = 0$.

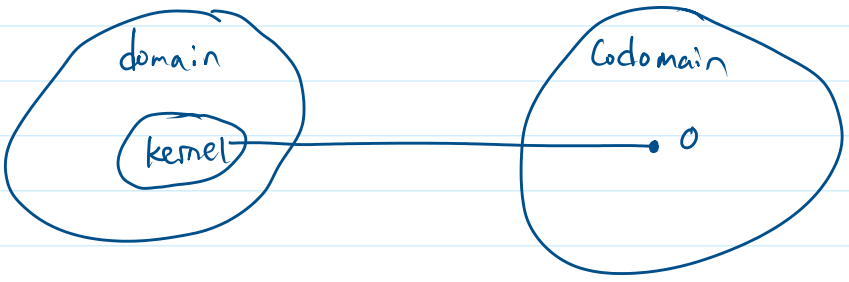
Example: Long division

$$\begin{array}{r|l} & x^2+x+4 \\ \hline x-2 & x^3-x^2+2x-3 \\ & x^3-2x^2 \\ \hline & \quad x^2+2x-3 \\ & \quad x^2-2x \\ \hline & \qquad 4x-3 \\ & \qquad 4x-8 \\ \hline & \qquad\quad 5 \end{array}$$

$$\Rightarrow \quad x^3-x^2+2x-3 = (x-2)(x^2+x+4)+5$$

Def: $p(x) \in \bar{F}[x]$ and $\alpha \in \bar{F}$. We say α is zero or root of $p(x)$ if $p(x)$ is in the kernel of the evaluation homomorphism ϕ_α ($p(\alpha) = 0$).

$$\ker \phi = \{ r \in R : \phi(r) = 0 \}$$



Corollary: $\bar{F}$ field. $\alpha \in \bar{F}$ is a zero of $p(x) \in F[x]$ iff $x - \alpha$ is a factor of $p(x)$ in $F[x]$.

$$p(x) = (x-\alpha)(x-\beta)$$

α, β are zeros / roots

Corollary: $\bar{F}$ field. $p(x) \neq 0 \in F[x]$ with degree n can have at most n distinct zeros in $\bar{F}$.

Def: Monic polynomial $d(x)$ is a gcd of $p(x), q(x) \in F[x]$ if $d(x)$ evenly divides both $p(x)$ and $q(x)$ and if for any other polynomial $d'(x)$ dividing both $p(x)$ and $q(x)$, $d'(x) \mid d(x)$. We write

$$d(x) = \gcd(p(x), q(x))$$

Two polynomials $p(x)$ and $q(x)$ are relatively prime if $\gcd(p(x), q(x)) = 1$.

Irreducible polynomials

Thursday, May 2, 2024 2:52 PM

- Irreducible means we can't factor f(x) into f(x) = g(x) * h(x).

- Irreducible polynomials function as the "prime numbers" of polynomial rings.

Example: ① $x^2-2 \in \mathbb{Q}[x]$ is irreducible

$(x+\sqrt{2})(x-\sqrt{2})$

② $x^2+1 \in \mathbb{R}[x]$ is irreducible

$(x+i)(x-i)$

Both have zeros in $\mathbb{C}[x]$.

Fundamental theorem of algebra: $p(x)$ has ≥ 1 complex root.

Theorem 17.14. Gauss's Lemma. *Let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $p(x)$ factors into a product of two polynomials $\alpha(x)$ and $\beta(x)$ in $\mathbb{Q}[x]$, where the degrees of both $\alpha(x)$ and $\beta(x)$ are less than the degree of $p(x)$. Then $p(x) = a(x)b(x)$, where $a(x)$ and $b(x)$ are monic polynomials in $\mathbb{Z}[x]$ with $\deg \alpha(x) = \deg a(x)$ and $\deg \beta(x) = \deg b(x)$.*

Proof.

???

Corollary 17.15. *Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$ and $a_0 \neq 0$. If $p(x)$ has a zero in $\mathbb{Q}$, then $p(x)$ also has a zero α in $\mathbb{Z}$. Furthermore, α divides a_0.*

Proof.

Look at an example.

$p(x) = x^4 - 2x^3 + x + 1$ determine if it is irreducible over $\mathbb{Q}[x]$

Suppose $p(x)$ is reducible over $\mathbb{Q}[x]$, then:

1. $p(x) = (x-\alpha)\,q(x)$

or 2. $p(x) = (x^2+ax+b)(x^2+cx+d)$

X case 1: By corollary 17.15, $\alpha \mid 1 \Rightarrow \alpha = \pm 1$.

But $p(1) = 1$ X

$p(-1) = 3$ X

case 2: $p(x) = (x^2+ax+b)(x^2+cx+b)$

$$p(x) = x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$$

By Gauss's Lemma, each factor is in $\mathbb{Z}[x]$, so:

$a+c = -2$

$ac+b+d = 0$

$ad+bc = 1 \Rightarrow b=d$ so $b(a+c) = 1 = -2b = 1 \Rightarrow b = -\frac{1}{2}$

$bd = 1 \Rightarrow b = d = 1$ or $b = d = -1$

Contradiction

Theorem: Eisenstein's Criterion

p prime, and suppose $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$

If $p \mid a_i$ for $i = 0, 1, \cdots, n-1$ but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Example: $f(x) = \underset{a_n}{16}x^5 - 9x^4 + 3x^2 + 6x \underset{a_0}{-21}$

$p = 3$ $\quad 3 \mid -21$ $\quad 3 \mid 6$ $\quad 3 \mid 3$ $\quad 3 \mid -9$

$3 \nmid 16$

$9 \nmid -21$

$\Rightarrow$ $f(x)$ is irreducible over $\mathbb{Q}$

Eisenstein's Criterion is more useful in constructing irreducible polynomials of a certain degree over Q than determining the irreducibility of an arbitrary polynomial in Q[x].

Homework

Tuesday, April 30, 2024 10:48 AM

- Read http://abstract.ups.edu/aata/aata.html chapter 16, 18, 21, 22, 23
- Read https://www.rareskills.io/zk-book