ABSTRACT ALGEBRA

Congruences

$a \equiv b \pmod m$

means

$m \mid a-b$

Ex $1 \equiv 23 \pmod 7$

DEF divisibility $\mathbb{Z}$

$a \mid b$ if $(\exists x)(ax = b)$

divides

$0 \mid 0$

Fix m congruence mod m is an equivalence relation on $\mathbb{Z}$

" classes: residue classes mod m

Example: mod 2 residue classes

$m \in \mathbb{Z}$

$\ldots, -4, -2, 0, 2, 4, 6, \ldots$ even

$-5, -3, -1, 1, 3, 5, 7$ odd

---

mod m there are $|m|$ residue classes

except if $m = 0$

mod 0 residue classes is ∞

$a \equiv b \mod m$

$\Updownarrow$

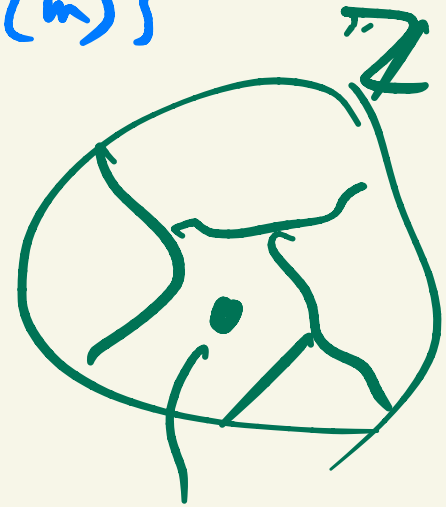
$a \equiv b \mod (-m)$

$a \equiv b \ (m)$

$a \equiv b \ (0) \iff a = b$

fix m $\quad [a]$: residue class of m

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \ (m)\}$$



representative of its equivalence class

DEF $\quad [a] + [b] := [a+b]$

if $\quad [a] = [a']$
$\quad\quad [b] = [b']$

need $\quad [a+b] = [a'+b']$

i.e. if $\quad a \equiv a' \ (m)$
$\quad\quad b \equiv b' \ (m)$
$\quad$ then $\quad a+b \equiv a'+b' \ (m)$

Do

$$\left.\begin{array}{l} a \equiv a' \ (m) \\ b \equiv b' \ (m) \end{array}\right] \Rightarrow a \cdot b \equiv a' \cdot b' \ (m)$$

DO

$\therefore \quad [a] \cdot [b] := [ab]$ def **Sound**

---

mod 5

+	0	1	2	3	4
0					
1			3		
2					1
3					
4					

2+4

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	.	.	.
4	0	4	.	.	.

$\mathbb{Z}/(m)$ $\mathbb{Z}_m$

GROUP $(G, *)$

$*: G \times G \to G$

$(a, b) \mapsto a * b$

① associative

$(\forall a, b, c)\ (a*(b*c) = (a*b)*c)$

② $\exists$ neutral element e

$(\forall a)\ (e*a = a*e = a)$

③ $\exists$ inverses

$(\forall a)(\exists a')(a*a' = a'*a = e)$

Commutative group (Abelian grp)

④ $a*b = b*a$

Examples: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^\times, \cdot)$

$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

Nonexamples: $(\mathbb{N}_0, +)$, $(\mathbb{R}, \cdot)$

$|G|$: order of G

DEF permutation of a set A

bijection $\varphi : A \to A$

if $|A| = n$ then there are $n!$ permutations

$a \mapsto a^{\varphi}$

composition $\varphi\psi$

$A \xrightarrow{\varphi} A \xrightarrow{\psi} A$

$a \mapsto a^{\varphi} \mapsto (a^{\varphi})^{\psi}$

$a^{\varphi\psi} := (a^{\varphi})^{\psi}$

$(\varphi\psi)\vartheta = \varphi(\psi\vartheta)$

$|A| = n$ $\quad S_n \leftarrow$ degree $\quad |S_n| = n!$

Symmetric group acting on A

$\mathrm{Sym}(A)$

RING $(R, +, \times)$

$(R, +)$ Abelian group

$\times$ associative

distributive over $+$

$a(b+c) = ab + ac$

$(b+c)a = ba + ca$

Additive neutral element: zero 0

DO $(\forall a)(0 \cdot a = a \cdot 0 = 0)$

Example: $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{Z}, +, \times)$, $(\mathbb{Z}_n, +, \times)$

noncommutative ring: $M_n(\mathbb{R})$ $n \times n$ matrices over $\mathbb{R}$

Ring R

DEF a is a zero-divisor if

$a \neq 0$ and $\exists b \neq 0$ s.t. $ab = 0$

Ex $\mathbb{Z}_m$ has no zero-divisors $\iff$ m prime

Obs for $n \geq 2$ $M_n(R)$ has zero-div.

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$A^2 = \underline{0}$$

FIELDS $\mathbb{F}$

commutative ring

s.t. $(\mathbb{F}^\times, \times)$ group

$\therefore$ field has no zero-divisors

Ex $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ p prime

Not $\mathbb{Z}$

Thm If R is a finite comm. ring with identity and without zero-divisors then R is a field

∞ counterexample: $\mathbb{Z}$

DEF $a \in \mathbb{Z}$ has the prime property

if $(\forall x,y)(a \mid xy \Rightarrow (a \mid x \vee a \mid y))$

$a \neq \pm 1$

THM If a is a prime number then a has the prime property

Euclid's lemma

$\therefore \mathbb{Z}_p$ is a field: $\mathbb{F}_p$

other finite fields

EX $\mathbb{F}_p[i] = \{a + bi \mid a, b \in \mathbb{F}_p\}$ $\quad i^2 = -1$

For what primes is this a field ?

$$|\mathbb{F}_p[i]| = p^2$$

Theorem (Galois +)

① If $\mathbb{F}$ is a finite field then $|\mathbb{F}| = p^k$

② $\forall p^k$ $\exists!$ finite field of order p^k

$GF(p^k)$ Galois field

also denoted $\mathbb{F}_{p^k}$

DEF

$\mathbb{F}$ field

characteristic of $\mathbb{F}$:

smallest $k \in \mathbb{N}$ s.t. $\underbrace{1+1+\dots+1}_{k} = 0$

if no such k exists: $\mathrm{char}(\mathbb{F}) := 0$

Ex.

$\mathrm{char}(\mathbb{R}) = 0$

$\mathrm{char}(\mathbb{F}_p) = p$

$\mathrm{char}(\mathbb{F}_p[i]) = p$

Thm $\mathrm{char}(\mathbb{F})$ is always $<$ prime, $<$ zero

"finite char." means nonzero char.

polynomials over $\mathbb{F}_p$ → infinite field of char p → $\left\{ \frac{p(x)}{q(x)} \mid p,q \text{ poly. over } \mathbb{F}_p \right\}$

$\mathbb{F}$ field

$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{F}^n$ vector space: $v_1 \dots v_k \in \mathbb{F}^n$

$a_i \in \mathbb{F}$ linear combination: $\sum_{i=1}^{k} a_i v_i$

$a_i \in \mathbb{F}$

Application area

Theory of error-correcting codes
based on vector spaces
polynomials
} over finite fields

$W \subseteq \mathbb{F}^n$

W is a subspace if

- $(W \neq \emptyset)$
- closed under lin. combinations

$k=0$ empty sum $=0$

$v_1 \dots v_k$ linearly indep. if

$$(\forall a_1 \dots a_k \in \mathbb{F})\left(\sum a_i v_i = 0 \Rightarrow a_1 = \dots = a_k = 0\right)$$

$S \subseteq V$ $\quad \text{span}(S) = \{\text{all finite lin comb.}\}$

$v_1 \dots v_k$ is a basis of subspace W if lin indep + span $= W$

Thm. All maximal lin indep sets in W same size

$:= \dim W$

DEF dot product: $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ $w = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$

$$v \cdot w = \sum a_i b_i$$

$$v \cdot (w_1 + w_2) = v \cdot w_1 + v \cdot w_2$$

def $v \cdot (aw) = a \cdot (vw)$

DO $a \cdot \underline{v} = \underline{0} \iff a = 0$ or $\underline{v} = \underline{0}$

DEF $v \perp w$ if $v \cdot w = 0$

perpendicular

$v^\perp = \{ w \mid v \perp w \}$

$S \subseteq F^n$ $\quad S^\perp = \bigcap_{v \in S} v^\perp = \{ w \mid (\forall v \in S)(v \perp w) \}$

Do $(\forall S)(S^\perp$ is a subspace)

Do $S \subseteq S^{\perp\perp}$

if W is a subspace $W \leq \mathbb{F}^n$

EX Thm If $U \leq \mathbb{F}^n$

then $\dim U + \dim U^\perp = n$

DEF $v \in \mathbb{F}^n$ is <u>isotropic</u> if $v \neq 0$, $v \perp v$

Do $\exists$ is over $\mathbb{R}$

EX in $\mathbb{F}^2$: find isotropic vectors if $\mathbb{F} = \mathbb{C}$

$\mathbb{F} = \mathbb{F}_5, \mathbb{F}_2$

Q For what primes p $\exists$ isoth vectors in $\mathbb{F}_p^2$

COROLLARY $U^{\perp\perp} = U$

DEF. U is totally isotropic if $U \subseteq U^{\perp}$

i.e. $(\forall a, b \in U)(a \perp b)$

COR If U tot isotr then $\dim U \leq \lfloor \frac{n}{2} \rfloor$.

If $\mathbb{F}_q$ and $W \leq \mathbb{F}_q^n$ $\dim W = d$

prime power then $|W| = q^d$

Put these all together

to prove Eventowa Thm