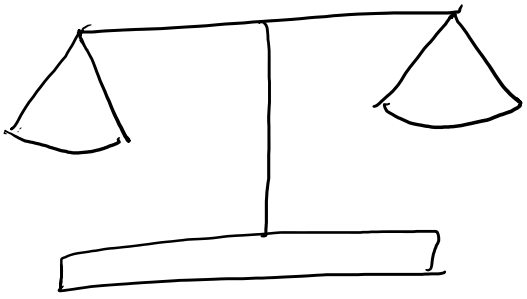
CH1 (13 weights problem.)



13 weights

w_1 w_2 ... w_{13} $\in \mathbb{R}$

s.t. $\forall i$ if we remove the i^{th} weight, we can divide the remaining 12 weights into two groups of 6 each of equal total weight.

Prove: $w_1 = \cdots = w_{13}$.

Def For $f, g \in \mathbb{R}[x]$,

$f \mid g$ if $(\exists$ polynomial $h)(g = f \cdot h)$

f divides g

when does $x \mid g = b_0 + b_1 x + \cdots + b_n x^n$?

$(\forall g)(1 \mid g)$ $\quad g = x \cdot h = x(c_0 + c_1 x + \cdots + c_k x^k)$

$= c_0 x + c_1 x^2 + \cdots + c_k x^{k+1}$

(Ex. 1)

So $x \mid g \iff b_0 = 0$.

$(\forall g)(2 \mid g)$

? $(\forall g)(0 \nmid g)$

what about $0 \mid 0$?

$(\exists h)(0 = h \cdot 0)$?

Ex. $0, 1, x, x^{75} + 530 \ldots$.

So $0 \mid 0$ and

$(\forall g, g \neq 0)(0 \nmid g)$ but

$(\forall c \in \mathbb{R}, c \neq 0)(\forall g)(c \mid g)$

? $(\exists g)(\forall f)(f \mid g)$

yes: $g = 0$

$f \mid 0$ b/c $0 = f \cdot 0$

let $h = 0$.

Degree of a polynomial.

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + \cdots$$

$$\deg(f) = \max \{ i \mid a_i \neq 0 \}$$

Polynomial → infinite sequence of coefficients of which only finitely many are allowed to be nonzero. (Compare these sequences)

Ex. $\deg(1 + x^2) = 2$

$\deg(75) = 0$

$\deg(0) = ?$ (all coefficients are 0...)

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Suppose $g = 0$.

Then $\deg(f \cdot 0) = \deg(f) + \deg(0)$

$\deg(0) = \deg(f) + \deg(0)$ ... ?

Adding any number to deg 0 won't change it? ∞.

$\deg(f+g) = \max\{\deg(f), \deg(g)\}$

$f = 1 + x^2 \qquad g = 1 - x^2$

$f + g = 2 \qquad \deg 0.$

$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}.$

Suppose $g = 0$

$\deg(f+0) \leq \max\{\deg(f), \deg(0)\}$

$\deg(f) \leq \max\{\deg(f), \deg(0)\}$

Seems legit

what about $\deg(f + -f)$?

$\deg(f + -f) \leq \max\{\deg(f), \deg(-f)\}$

$\deg(0) \leq \deg(f) \quad \forall f.$ $\deg f$

$+\infty$ doesn't work... but $-\infty$ does.

Thus

$$\boxed{\deg(0) = -\infty}.$$

and the rules

$$\deg(f \cdot g) = \deg f + \deg g$$

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$

are preserved

Division Theorem for Integers.

$(\forall a, b)$ (if $b \neq 0$ then $\exists q, r)(a = b \cdot q + r$ and $0 \leq r < |b|)$.
$\in \mathbb{Z}$ $\in \mathbb{Z}$

Define a universe - $\mathbb{Z}$ - and seek within it

(q = quotient, r = remainder)

Note that 0 is excluded for a different reason than not being able to divide by 0 - because nothing fits in $0 \leq r < 0$.

(DO) Prove by induction on a for $a \geq 0$...
(and take care of the negatives.)

Division Thm. for $\mathbb{R}[x]$.

($\forall$ polynomials f, g) (if $g \neq 0$ then $\exists$ polynomials q, r)

($f = g \cdot q + r$ and $\deg(r) < \deg(g)$)

This is ok b/c $g \neq 0$ so $\deg g \neq -\infty$.

(DO) Prove by induction on $\deg f$.

(Base case: $-\infty$, else assume all cases less than k)

"strong induction"

A **monic polynomial** if the lead coefficient is 1 (i.e. $a_{\deg(f)} = 1$).

Case: $\underbrace{g = x - \alpha}_{\deg = 1 \text{ monic}}$ $\quad \alpha \in \mathbb{R}$

$$f = (x-\alpha)h + r$$

$$\deg r < 1$$

$$\deg r \leq 0 \Rightarrow r \text{ is a constant } (r \in \mathbb{R})$$

Find r.

$$r = f(\alpha)$$

$$(\forall f \in \mathbb{R}[x])(\forall \alpha \in \mathbb{R})(\exists g \in \mathbb{R}[x])(f(x) = (x-\alpha)g(x) + f(\alpha))$$

i.e

Thm

$$(\forall f \in \mathbb{R}[x])(\forall \alpha \in \mathbb{R})(x-\alpha \mid f(x) - f(\alpha))$$

Thm $\quad x - \alpha \mid f(x) - f(\alpha)$

Proof First we prove this for $f(x) = x^k$.

$x-\alpha \mid x^k - \alpha^k = (x-\alpha)(x^{k-1} + \alpha x^{k-2} + \alpha^2 x^{k-3} + \dots \alpha^{k-1})$

?

DO

$x-\alpha \mid f(x) - f(a)$ is inherited by lin. combs. of x^k.

$\therefore$ true for all polynomials (x^k form a basis).

□

DO

<u>Cor.</u> $f(\alpha) = 0 \iff x-\alpha \mid f$.

<u>Thm.</u> If $f \in \mathbb{R}[x]$ s.t. $\deg f = n \geq 0$, then # of distinct roots of f is $\leq n$.

If $\alpha \neq \beta$ are roots of f,

$f(x) = (x-\alpha)g(x)$ <u>Claim:</u> $g(\beta) = 0$

$0 = f(\beta) = \underbrace{(\beta-\alpha)}_{\neq 0} g(\beta) \Rightarrow g(\beta) = 0$ ✓

$\Downarrow$

$x-\beta \mid g$ so

$g = (x-\beta)h$

$(x-\alpha)(x-\beta) \mid f$ $\Leftarrow$ and $f = (x-\alpha)(x-\beta)h$

Proof of Thm Let $\alpha_1, \ldots, \alpha_k$ be the distinct roots of f. Then

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k) \mid f.$$

(DO) If $g \mid h \neq 0$ then $\deg g \leq \deg h$.

(Follows from $\deg(fg) = \deg f + \deg g$). □

$\therefore k \leq \deg f = n.$

$\gcd(28, 70) = 14$ $\quad a = d \cdot a_1$, $b = d \cdot b_2$

↑ greatest common divisor $\quad \gcd(a,b) = d$

① $d \mid a$ and $d \mid b$ ("d is a common divisor")

② If $e \mid a$ and $e \mid b$ then $d \geq e$... ?

"d is greatest of all common divisors"

$\gcd(28, -70) = 14$

$Div(a)$ = set of divisors of a.

$Div(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$a|b \iff -a|b \iff a|-b \iff -a|-b$.

Def. (In $\mathbb{Z}$)

$a|b$ if $(\exists c)(ac = b)$

Note: $(\forall b)(1|b)$, $(\forall b)(-1|b)$

$(\forall a)(a|0)$

$Div(1) = \{\pm 1\}$

$Div(-a) = Div(a)$

$Div(0) = \mathbb{Z} = \{\text{all integers}\}$

set of common divisors of a, b.

$Div(a,b) = Div(a) \cap Div(b)$.

$gcd(0,0) = \cancel{\max(\mathbb{Z} \cap \mathbb{Z})}$?

$= 0$.

Our definition from before won't work.

(2) If $e|a$ and $e|b$ then $e|d$. ✓

Thus, d is a greatest common divisor of a, b

Def. ~~$\gcd(a,b) =$~~ if

(1) $d|a$ and $d|b$ $(d \in Div(a) \cap Div(b))$

(2) if $e|a$ and $e|b$ then $e|d$.

(DO) If d_1 and d_2 both are gcds of a and b, then $d_2 = \pm d_1$.

Convention: if d is a greatest common divisor of a and b then we write

$$\gcd(a,b) = |d|.$$

$\gcd(a,a) = |a|$.

$\gcd(a,0) = |a|$ $(Div(a) \cap \underbrace{Div(0)}_{\mathbb{Z}} = Div(a))$

How do we know gcd exists?

Thm $(\forall a, b)(\exists \gcd(a,b))$

(DO) d is a greatest common divisor of a and b iff $Div(a,b) = Div(d)$.

Abelian group: $(\mathbb{Z}, +)$ (review from week 2 Day 3)

$H \leq \mathbb{Z}$

$\uparrow$

subgroup: $H \subseteq \mathbb{Z}$ s.t.

- $0 \in H$
- if $a, b \in H \Rightarrow a + b \in H$
- if $a \in H \Rightarrow -a \in H$

Ex. even integers: $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$

$\{0\}$

$k\mathbb{Z} = \{\text{multiples of } k\}$

DO!

Thm There is no other subgroup, i.e. if $H \leq \mathbb{Z}$ then $(\exists k)(H = k\mathbb{Z})$

(Hint: use the Division Theorem.)

Thm. $(\forall a, b)(\exists d)$ (d is a greatest common divisor of a, b and $(\exists x, y)(d = ax + by)$)

(Universe: $\mathbb{Z}$) lin. comb.

Notation: If $A \subseteq \mathbb{Z}$ and $k \in \mathbb{Z}$,

then $kA = \{ka \mid a \in A\}$.

If $A, B \subseteq \mathbb{Z}$ then

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

$|A| = k \quad |B| = \ell \Rightarrow |A + B| \leq k \cdot \ell$

Is it tight? (achievable)

Yes.

$A = \{1, 2, \ldots, 10\}$ $\quad B = \{10, 20, 30, \ldots\}$

(DO) Prove: $(\forall k, \ell)$ (this bound is tight, i.e. $(\exists A, B)(|A| = k, |B| = \ell, |A + B| = k\ell)$).

HW (a) If $|A| = k$, then $|A + A| \leq \binom{k+1}{2} = \frac{k(k+1)}{2}$

(b) $\max |A + A + A| = ?$

(c) $\max |\underbrace{A + A + \cdots + A}_{\ell \text{ times}}| = ?$

$\mathbb{N} = \{0, 1, 2, \dots\}$

$A, B \subseteq \mathbb{N}$

$A \oplus B = \mathbb{N}$

meaning $A + B = \mathbb{N}$ uniquely:

$(\forall n \in \mathbb{N})(\exists! a \in A,\ b \in B)(a + b = n)$

Ex. $A = \{0\}$, $B = \mathbb{N}$.

$A = \{0, 1, 2, \dots, k-1\}$ $B = k\mathbb{N}$.

(Division Thm)

CH Find such A, B both infinite.

Back to Theorem ...

Thm. $(\forall a, b)(\exists d)(d$ is a greatest common divisor of a and b and $(\exists x, y)(d = ax + by))$.

Proof. $K = \{ax + by \mid x, y \in \mathbb{Z}\}$

$= a\mathbb{Z} + b\mathbb{Z}$

Claim: $K \leq \mathbb{Z}$.

$\uparrow$

subgroup.

choose $(x, y) = (0, 0)$

(1) $0 \in K \Leftarrow$

(2) If $k_1, k_2 \in K$, then $k_1 + k_2 \in K$.

$k_1 = ax_1 + by_1$ $\quad k_2 = ax_2 + by_2$ $\quad x_1, y_1, x_2, y_2 \in \mathbb{Z}$.

$k_1 + k_2 = a(x_1 + x_2) + b(y_1 + y_2)$

$x_1 + x_2 \in \mathbb{Z}$, $\quad y_1 + y_2 \in \mathbb{Z}$

so $k_1 + k_2 \in K$.

(3) If $k \in K$, then $-k \in K$.

$k = ax + by$ $\quad x, y \in \mathbb{Z}$

$-k = a(-x) + b(-y)$ $\quad -x, -y \in \mathbb{Z}$

so $-k \in K$.

$x \leftarrow -x$

$y \leftarrow -y$.

$r = 5a + 13b$

$-r = (-5)a + (-13)b$

$\therefore K \leq \mathbb{Z}$.

Since $K \leq \mathbb{Z}$ it follows that

$$(\exists k)(a\mathbb{Z} + b\mathbb{Z} = k\mathbb{Z})$$

Claim: k is a greatest common divisor of a, b.

NTS: (1) k is a common divisor

(2) k is a common multiple of all common divisors.

(1) $k \mid a$, i.e $a \in k\mathbb{Z}$

True b/c $a \in a\mathbb{Z} + b\mathbb{Z}$. $(a = 1 \cdot a + 0 \cdot b)$.

Similarly, $k \mid b$. $(b = 0 \cdot a + 1 \cdot b)$

(2) If $e \mid a$, then $e \mid k$.

$e \mid b$ WTS: $k \in e\mathbb{Z}$

$k = ax + by$ where

$a \in e\mathbb{Z}$

$b \in e\mathbb{Z}$ $a, b \in e\mathbb{Z}$ and $x, y \in \mathbb{Z}$.

$a = e \cdot c_1$

$b = e \cdot c_2$,

$c_1, c_2 \in \mathbb{Z}$

$k = e \cdot c_1 \cdot x + e \cdot c_2 \cdot y$

$= e(c_1 \cdot x + c_2 \cdot y)$

$(c_1 \cdot x + c_2 \cdot y) \in \mathbb{Z}$ so $k \in e\mathbb{Z}$.

$k\mathbb{Z}$ = all multiples of k.

$= \{ka \mid a \in \mathbb{Z}\}$

what about $a\mathbb{Z} + b\mathbb{Z}$?

$a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$ (all linear combinations of a, b)

If $\left.\begin{matrix} e \mid a \\ e \mid b \end{matrix}\right\} \Rightarrow e \mid ax + by \overset{?}{\Rightarrow} e \mid k$

NTS: k is lin. comb. of a, b.

b/c $k \in k\mathbb{Z}$, so $k \in a\mathbb{Z} + b\mathbb{Z}$.

HW (a) $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup.

(b) Given $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup, we know it equals $k\mathbb{Z}$ ... what is the meaning of k?

(no proof required - definition req.)

we can copy this entire process for polynomials:

± 1 in $\mathbb{Z}$ $\Rightarrow$ deg 0 for polynomials

(DO) Redo this process for polynomials

(DO) If $d_1, d_2 \in \mathbb{R}[x]$ are greatest common divisors of f and g $(\in \mathbb{R}[x])$, then

$(\exists\, c \in \mathbb{R},\ c \neq 0)(d_2 = c d_1)$

$I \subseteq \mathbb{R}[x]$

Def I is an ideal of $\mathbb{R}[x]$ if

(1) $0 \in I$

(2) If $f, g \in I$ then $f + g \in I$.

(3) If $f \in I$ and $g \in \mathbb{R}[x]$ then $f \cdot g \in I$.

Integers: $k\mathbb{Z}$ (precisely same as subgroups)

In the polynomials, these are not the same

Ex. $\{0\}$, all multiples of a polynomial.

principal ideal generated by f, denoted (f) —— $(f \cdot \mathbb{R}[x]) = \{f \cdot g \mid g \in \mathbb{R}[x]\}$

HW Prove: every ideal in $\mathbb{R}[x]$ is principal.

DO gcd of polynomials exists and can be written as $d = \gcd(f, g)$

$\exists\, r, s \in \mathbb{R}[x]$

$d = f \cdot r + g \cdot s$

CH Def. f is a prime exponent polynomial if all exponents that actually occur (nonzero coefficients) are prime.

E.g. $10x^3 + 75x^{11} - \sqrt{2} \cdot x^{13}$.

Prove: If $f \in \mathbb{R}[x]$, $f \neq 0$ then f has a nonzero multiple that is a prime-exponent polynomial