Right board

MAT 312 | Physics? P113

upcoming OHs: Alekseev, today 4-5, in Hall 3-111
Yi, 6-7, in MLC

MAT 312/AMS 351: Applied Algebra

Examples/applications focused

intro to group theory

Recitations: Today: Review of Mathematical Induction

useful reasoning tool

08/27/19

Pick up info handout

Left board

Part I's Main Thm: If $a, b \in \mathbb{Z}^+$ (positive integers)

$\exists$ (there exists) $\alpha, \beta \in \mathbb{Z}$ s.t. $\alpha a + \beta b = \gcd(a,b)$

do not erase

greatest common divisor of a, b

= largest integer that divides a, b

Examples/applications first, proof later

Example 1: $a=3$ $b=5$ $\gcd(3,5)=1$

$\underbrace{2}_{\alpha} \cdot 3 + \underbrace{(-1)}_{\beta} \cdot 5 = 1$ $\quad \underbrace{(-3)}_{\alpha} \cdot 3 + \underbrace{2}_{\beta} \cdot 5 = 1$

$-5 = -b$ $\quad +3 = a$

Example 2: $a=4$ $b=6$ $\gcd(4,6)=2$

$\underbrace{(-1)}_{\alpha} \cdot 4 + \underbrace{1}_{\beta} \cdot 6 = 2$ $\quad \underbrace{2}_{\alpha} \cdot 4 + \underbrace{(-1)}_{\beta} \cdot 6 = 2$

$+3 = 6/2$ $\quad -2 = 4/2$

Crl 1: Let $a, b, c \in \mathbb{Z}^+$ with $\gcd(a,b)=1$ (a relatively prime to b)

(i) If $a \mid bc$ (a divides bc), then $a \mid c$

(ii) If $a \mid c$ and $b \mid c$, then $ab \mid c$

Pf: $\gcd(a,b)=1 \overset{\text{Thm}}{\Rightarrow} \exists \alpha, \beta \in \mathbb{Z}$ s.t.

$\alpha a + \beta b = 1$ (*)

$\Rightarrow \alpha ac + \beta bc = c$ (*)

(i) $a \mid \alpha ac$, $a \mid \beta bc \overset{(*)}{\Rightarrow} a \mid c = \alpha ac + \beta bc$

(ii) $a \mid \alpha ac$, $b \mid c$, $b \mid c$, $a \mid bc$, $b \mid c$, $a \mid c \overset{(*)}{\Rightarrow} ab \mid c = \alpha ac + \beta bc$

Crl 2: 1.16 on HW1

Example of Crl 1: $a=3, b=5 \rightsquigarrow \gcd(3,5)=1$

(i) $c=12$: $3 \mid 5 \cdot 12 \Rightarrow 3 \mid 12$ ✓ condition satisfied

(ii) $c=30$: $3 \mid 30$, $5 \mid 30 \Rightarrow 3 \cdot 5 \mid 30$ ✓

Non-examples of Crl 2: $a=4, b=6 \rightsquigarrow \gcd(4,6)=2 \neq 1$ condition not satisfied

(i) $4 \mid 6c \not\Rightarrow 4 \mid c$

maybe yes, e.g. if $c=4$; maybe not, e.g. if $c=2$

(ii) $4 \mid c$, $6 \mid c \not\Rightarrow 4 \cdot 6 \mid c$; maybe yes, e.g. $c=24$

maybe not, e.g. $c=12$

Lemma To prove Main Thm, need: (do not erase)

(1) Well-Ordering Principle: If $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$ (empty set), then S has a smallest element s_0 ($s_0 \leq s$ $\forall s \in S$)

Lemma 2 (Division w. Remainder): If $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ s.t. $0 \leq r < a$ and $b = qa + r$.

Well-ordering Principle = axiomatic property of $\mathbb{Z}^+$

does not hold for $\mathbb{Z}$, e.g. $S = \mathbb{Z}$ has no smallest element

does not hold for $\mathbb{Q}^+$, e.g. $S = \mathbb{Q}^+$ has no smallest element

Well-ordering Principle $\Rightarrow$ Principle of Mathematical Induction

Lemma 1, Main Thm

Same ↳ also true for $\mathbb{Z}_{\geq 0}$

2 4 10 24 $14 = 1\cdot 10 + 4$, $10 = 2\cdot 4 + 2$, $4 = 2\cdot 2 + 0$ ← gcd

Assume

Pf of Lemma 1: Let $S = \{b - ka : k \in \mathbb{Z}^{\geq 0},\ b - ka \in \mathbb{Z}^{\geq 0}\}$

$S \subset \mathbb{Z}^{\geq 0}$ by dfn; $S \neq \emptyset$ b/c

(i) if $b \geq 0$, $b - 0\cdot a \geq 0 \Rightarrow b \in S$

(ii) if $b < 0$, $b - b\cdot a = b(1-a) \geq 0 \Rightarrow b \in S$

well-ordering principle $\Rightarrow$ S has contains a smallest element r

$0 \leq r = b - qa$ for some $q \in \mathbb{Z}^{\geq 0}$

b/c $r \in S$

Claim: $r < a$ $\Rightarrow$ done with Lemma

Example $a = 24$ $b = 34$

Claim: $r < a$

If by contradiction: Suppose $r \geq a$. Then

$0 \leq r - a = b - qa - a = b - (q+1)a$

$q \in \mathbb{Z}^{\geq 0} \Rightarrow q+1 \in \mathbb{Z}^{\geq 0}$

$\Rightarrow r - a \in S$ b/c

But $r - a < r$ (b/c $a > 0$) and r = smallest element of S

∴ Contradiction $\Rightarrow r < a$ ✓

Pf of Main Thm: Let $S = \{\alpha a + \beta b : \alpha, \beta \in \mathbb{Z},\ \alpha a + \beta b \in \mathbb{Z}^+\}$

$S \subset \mathbb{Z}^+$ by dfn; $S \neq \emptyset$ b/c $a = 1\cdot a + 0\cdot b \in S$

$\Rightarrow S$ contains smallest element s_0

Claim 1: if $c \in \mathbb{Z}^+$ and $c \mid a, b$, then $c \mid s_0$

Claim 2: $s_0 \mid a, b$

Claim 1+2 $\Rightarrow \gcd(a,b) = s_0 \equiv \min\{\alpha a + \beta b : \alpha, \beta \in \mathbb{Z},\ \alpha a + \beta b \in \mathbb{Z}^+\}$

$\Rightarrow$ Main Thm ✓

Pf of Claim 1: $s_0 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$

$c \mid a, b \Rightarrow c \mid \alpha a, \beta b \Rightarrow c \mid s_0$ ✓

Pf of Claim 2 $s_0 \in S \Rightarrow s_0 = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$ and $s_0 \in \mathbb{Z}^+$

Lemma 1 $\Rightarrow \exists q \in \mathbb{Z}^{\geq 0}, r \in \mathbb{Z}^+$ s.t.

$0 \leq r < s_0$, $a = q s_0 + r$

$\Rightarrow r = a - q s_0 = a - q(\alpha a + \beta b) = (1 - q\alpha)a + (-q\beta)b$

∴ $0 \leq r = (1 - q\alpha)a + (-q\beta)b < s_0$

($1 - q\alpha \in \mathbb{Z}$, $-q\beta \in \mathbb{Z}$)

$r < s_0 \Rightarrow r \notin S \Rightarrow r \in \mathbb{Z}^+$ ⇒ $r = 0$

$\Rightarrow a = q s_0 + 0 \Rightarrow s_0 \mid a$

By symmetry, $s_0 \mid b \Rightarrow$ Claim 2 ✓

How to find α, β? $\gcd(a,b)$? Euclid's algorithm

Lemma 2: $\forall\ q \in \mathbb{Z}$ and $a, r, aq + r \in \mathbb{Z}^+$,

$\gcd(a, r) = \gcd(a, aq + r)$ ⊛

Pf: (i) $c \in \mathbb{Z}^+$, $c \mid a, r \Rightarrow c \mid aq + r \Rightarrow \gcd(a, aq+r) \mid c$

$\Rightarrow \gcd(a, aq+r) \mid \gcd(a, r)$

By symmetry (with $-q$) $\gcd(a, r) \mid \gcd(a, aq + r)$

$\Rightarrow$ ⊛ holds.

Euclid's Algorithm: Start with $a, b \in \mathbb{Z}^+$, $a \leq b$

Lemma 1 $\Rightarrow \exists\ q_1, r_1 \in \mathbb{Z}^{\geq 0}$ s.t. $0 \leq r_1 < a$, $b = q_1 a + r_1$

(i) if $r_1 = 0$, $a \mid b \Rightarrow a = \gcd(a,b) = 1\cdot a + 0\cdot b$

o/w Lemma 2 $\Rightarrow \gcd(a,b) = \gcd(a, r_1)$

Lemma 1 $\Rightarrow \exists\ q_2, r_2 \in \mathbb{Z}^{\geq 0}$ s.t. $0 \leq r_2 < r_1$, $a = q_2 r_1 + r_2$

if $r_2 = 0$, $r_1 \mid a \Rightarrow \gcd(a, r_1) = r_1 = (\pm q_1)a + 1\cdot b$

o/w Lemma 2 $\Rightarrow \gcd(a, r_1) = \gcd(r_1, r_2)$. Continue with r_1, r_2

get: $b = q_1 a + r_1$ w. $0 \leq r_1 < a$, $q_1 \geq 0$

$r_0 = a = q_2 r_1 + r_2$ w. $0 \leq r_2 < r_1$, $q_2 \geq 0$

$r_1 = q_3 r_2 + r_3$ w. $0 < r_3 < r_2$, $q_3 \geq 0$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$ w. $0 < r_n < r_{n-1}$, $q_n \geq 0$

$r_{n-1} = q_{n+1} r_n + r_{n+1}$ → eventually 0 b/c $0 \leq r_{n+1} < r_n < \cdots < r_1 < a$

↳ Step: $r_n \mid r_{n-1}$

$\Rightarrow r_n = \gcd(r_{n-1}, r_n) = \gcd(r_{n-1}, r_{n-2}) = \cdots = \gcd(r_1, r_0)$

→ Solve backwards for r_n in terms of a, b $= \gcd(r_2, b)$