Make it Ob algebra

correct url & course website:
math.ucsd.edu/~hwen261/log.html

Integers:

important axiom:

Well Ordering Principle (WOP)

Any nonempty subset S of the integers has a smallest member
Divisibility

\[ t, s \text{ integers} \]
\[ t \text{ is a divisor of } s \text{, (notation: } t \mid s) \]
if we can find an integer \( u \) s.t.
\[ s = tu \]

Notation: if \( t \) is not a divisor of \( s \): \( t \nmid s \)
Division Algorithm

\[ a, b \text{ integers, } b > 0 \]

⇒ There exist unique numbers \( q \) and \( r \) such that
\[ a = bq + r \]
where \( 0 \leq r < b \)

Proof @ Existence

use \( \text{WOP} \)

Consider set \( S = \{ a - bh, \ \text{h integer s.t.} \ a - bh \geq 0 \} \)

\begin{align*}
\text{case 1: } & 0 \in S \Rightarrow \exists \text{ integer, say } q, \text{ s.t.} \\
& a - bq = 0 \Rightarrow a = bq + 0 \\text{ can take } r = 0 \text{ and giving} \checkmark
\end{align*}
case 2  \(0 \in S\)

can use WOP

\[\exists q \text{ s.t. } a - qb \text{ is smallest element in } S\]

enough to show: \(a - qb < b\)

( because then \(a = qb + (a - qb)\)

positive, \(\leq b\)

can take as \(r\)

proof by contradiction:

assume \(a - qb \geq b\)

\[\Rightarrow a - qb - b \geq 0\]

\[\Rightarrow a - (a+b)b \leq a - qb\]

\(\Rightarrow\) to \(a - qb\) smallest element in \(S\)
\[ r = a - q_0 b \] does the job

(b) uniqueness.

Assume \( a = b q + r \)

and \( a = b q' + r' \)

where \( q, q', r, r' \) integers

will \( 0 \leq r, r' < b \)

\[ bq + r = b q' + r' \]

Assume \( r' \geq r \)

\[ b(q - q') = b q - b q' = r' - r \geq 0 \]

\[ \Rightarrow 0 \leq b(a - q') = r' - r < b \]

Observe: \( 0 \leq r' - r \leq r' < b \)

\[ \uparrow \text{multiple of } b \]

\[ \uparrow \leq b \]

\[ \Rightarrow b(q - q') = 0 = r' - r. \]
\[ r' = r \quad \text{and} \quad q' = q. \]

**Example:**

\[
\begin{align*}
  a &= -27 \\
  b &= 6 \\
  \Rightarrow \quad -27 &= (-6)6 + 3 \\
  &= -36 + 3 \\
  q &= -5 \\
  r &= 2
\end{align*}
\]
Def. \( a, b \) integers

\[ \gcd(a, b) = \text{greatest common divisor of } a \text{ and } b \]

Ex. \( \gcd(12, 18) = 6 \)

Theorem \( (\gcd(a, b) \text{ as a linear comb. of } a \text{ and } b) \)

\( a, b \) integers \( \Rightarrow \) \( \exists \) integers \( s \) and \( t \) s.t.

\[ \gcd(a, b) = as + bt \]

(e.g. \( 6 = (-1) \cdot 12 + 1 \cdot 18 \))
Proof. Let \( S = \{ am + bn, \quad m,n \text{ integers such that } am + bn > 0 \} \)

can use WOP

Let \( d = as + bt \)

be the smallest element in \( S \)

claim: \( d \mid a \)

division algorithm: \( a = qd + r \) with \( 0 \leq r < d \)

\[
0 \leq r = a - qd
\]
\[
= a - q(as + bt)
\]
\[
= a(1 - qs) - b tq
\]
\[
= a(1 - qs) + b(-tq) < d
\]
\[
\Rightarrow r = 0 \quad (otherwise \quad r \in S \text{ contradicting our choice of } d)
\]
\[ \Rightarrow \quad d \mid a \]

same way one shows: \[ d \mid b \]

\[ \Rightarrow \quad d \text{ is a common divisor of } a \text{ and } b. \]

Let \( d' \) be another common divisor of \( a \) and \( b \)

\[ \Rightarrow \quad a = d'h \]
\[ b = d'k \]

\[ a = d'hs + d'kt \]
\[ = d'(hs + kt) \quad \Rightarrow \quad d' \mid d \]

\[ \Rightarrow \quad d \text{ greatest common divisor} \]