MATH H113: Honors Introduction to Abstract Algebra

2016-01-22

- Well-defined functions
- Properties of $\mathbb{Z}$

Homework due Fri. 2016-01-29:

- 0.1: 5, 7
- 0.2: 1d
- 0.3: 2, 12, 13, 14

Error in Proposition 1 (0.1)

$f : A \to B$ is injective if and only if it has a left inverse. If $A = \emptyset$, $B = 1$ then $f : A \to B$ is one-to-one but there's no left inverse $g : B \to A$ because there's no function $g : B \to A$. Attempted proof that f is one-to-one $\implies$ there's a left inverse: Define $g : B \to A$ by $g(b) = a$ if $b \in f(A)$ and $a \in A$ satisfies $f(a) = b$ (there's only one such a because f is one-to-one $\therefore$ g is well defined) If $b \notin f(A)$ then let $g(b) =$ any element of A (assumes that $A \neq \emptyset$ (where things went wrong)).

Note: Part 3 is still true. The above proof works if f is bijective (includes $f : \emptyset \to \emptyset$), because the 2nd part never comes up. (3. f is bijective $\iff$ f has a two-sided inverse g.)

Well-Defined

Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \begin{cases} |x| & x \geq 0 \\ x & x \leq 1 \end{cases}$ is well-defined (sets not disjoint, but this is OK becuase $|x| = x$ where they overlap. On the other hand, $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \begin{cases} |x| & x \geq 0 \\ 2x & x \leq 1 \end{cases}$ is not well-defined since $g(\frac{1}{2}) = \frac{1}{2}$ if you use the first part, but $g(\frac{1}{2}) = 1$ if you use the second part.

More typical example: $f : [-1, 1] \to \mathbb{R}$ defined by $f(x) = \sin(\theta)$, where θ is such that $\cos(\theta) = x$ is not well-defined: $f(\frac{1}{2})$ if $\theta = \frac{\pi}{3}$ then $f(x)$ would be $\frac{\sqrt{3}}{2}$ if $\theta = \frac{\pi}{3}$ then $f(x)$ would be $\frac{-\sqrt{3}}{2}$ (this is not really $f(x) = \sin(\cos^{-1}(x))$)

Is well-defined: $f(x) = |\sin(\theta)|$, if θ is such that $\cos(\theta) = x$.

Properties of the Integers

Well-Ordering Property of $\mathbb{N}$

Any *non-empty* subset A of $\mathbb{N}$ has a smallest element (*smallest element* means an element $m \in A$ such that $m \leq a$ for all $a \in A$).

Definition: let $a, b \in \mathbb{Z}$. We say that $a \mid b$ (a divides b) iff there is an integer q such that $aq = b$ (I do not require $a \neq 0$).
If a does not divide b, we write $a \nmid b$.

Examples: $-7 \mid 21$, $0 \mid 0$ (any q will work), $3 \mid 0$, $0 \nmid 3$, $2 \nmid 7$

Theorem (Division Algorithm): For all $a, b \in \mathbb{Z}$ with $b \neq 0$ there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < |b|$.

Proof:

- Case 1: $b > 0$
  - Uniqueness: Suppose $q, r, q', r' \in \mathbb{Z}$ satisfy $a = qb + r = q'b + r'$, $0 \leq r < b$, $0 \leq r' < b$
    Then $qb - q'b = r' - r$
    $q - q' = \frac{r'-r}{b}$, $r' - r < b$, similarly $r' - r > -b$
    So $1 < \frac{r-r'}{b} < 1$, $-1 < q - q' < 1$ (where $q - q' \in \mathbb{Z}$) so $q - q' = 0$, $r' - r = 0$.
  - Existence: Let $A = \{a - qb : q \in \mathbb{Z}\} \cap \mathbb{N}$
    Then A is a subset of $\mathbb{N}$.
    Want to check that $A \neq \emptyset$.
    If $a \geq 0$ then $a \in A$ (take $q = 0$, note that $a \in \mathbb{N}$)
    If $a < 0$ then take $q = a$.
    Then $a - ab \in A$ because you can take $q = a$ and $a - ab = (-a)(b-1) \geq 0$ it it's in $\mathbb{N}$.
    By the well-ordering property of $\mathbb{N}$, the set A has a smallest element r. Since $r \in A$,

    i. $r = a - qb$ for some $q \in \mathbb{Z}$, so $a = qb + r$
    ii. $r \geq 0$ because $r \in A \subseteq \mathbb{N}$
    iii. $r < b$, because if $r \geq b$ then $r - b \geq 0$ and $r = a - (q+1)b$, so $r - b \in A$ so r is not the smallest element of A ($r - b < r$).
- Case 2: $b < 0$ By case I, $a = q(-b) + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < -b = |b|$. Then $a = (-q)b + r$. QED

Definition: If $a, b \in \mathbb{Z}$ and $a \mid b$ then we say that a is a *divisor* of b, and the b is a *multiple* of a.
Definition: If $a, b \in \mathbb{Z}$ then a *common divisor* of a and b is an integer d such that $d \mid a$ and $d \mid b$.

Definition: If $a, b \in \mathbb{Z}$, not both zero. The *greatest common divisor* of a and b is a positive integer d such that

i. d is a common divisor of a and b
ii. $d' \mid d$ whenever d' is a common divisor of a and b

We write $d = \gcd(a, b)$
(Note: $\gcd(0, 0)$ is not defined.)
Also: $\gcd(a, b) = \gcd(b, a)$

Theorem: For all $a, b \in \mathbb{Z}$, not both zero, there is a unique gcd of a and b
Proof:

- *Uniqueness*: Suppose d_1 and d_2 both satisfy the definitionfor $gcd(a, b)$. Then $d_1 \mid d_2$ because d_1 is a common divisor and d_2 satisfies (ii). $d_1 \leq d_2$ because $d_2 > 0$. If $d_1 > d_2$ and $d_1 r = d_2$ then $r = \frac{d_1}{d_2} < 1$ so $f \notin \mathbb{Z}$ or $r \leq 0 \implies d \leq 0$ not true Similarly $d_2 \mid d_1$ so $d_2 \leq d_1 \therefore d_1 = d_2$
- *Existence*: Euclidean algorithm (next time).