MATH H113: Honors Introduction to Abstract Algebra

2016-01-27

- $\mathbb{Z}/n\mathbb{Z}$
- Groups

$\mathbb{Z}/n\mathbb{Z}$

Let n be a fixed positive integer.
Define a relation "$\equiv \pmod{n}$" on $\mathbb{Z}$ by $a \equiv b \pmod{n}$ if $n \mid (b-a)$.
So $a \equiv b \pmod{n}$ iff $qn = b - a$ for some $q \in \mathbb{Z}$.
$b = qn + a$ for some $q \in \mathbb{Z}$
This relation is:

i. reflexive (take $q = 0$)
ii. symmetric (check it yourself, or see book)
iii. transitive:
$a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
$\implies b = qn + a$ and $c = rn + b$ for some $q, r \in \mathbb{Z}$
$\implies c = (q+r)n + a$ for some $q, r \in \mathbb{Z}$
$\implies a \equiv c \pmod{n}$.

Therefore "$\equiv \pmod{n}$" is an equivalence relation. Define $\mathbb{Z}/n\mathbb{Z}$ to be the set of equivalence classes for "$\equiv \pmod{n}$".
By the division algorithm, for all $b \in \mathbb{Z}$ there are $q, r \in \mathbb{Z}$ such that $b = qn + r$ and $0 \le r < n$, $\therefore b \equiv$ one of $0, 1, 2, \ldots, n-1 \pmod{n}$. Also all of these are different if $0 \le i, j < n$ and $i \neq j$ then $i \not\equiv j \pmod{n}$ because $j = qn + i$ would contradict uniqueness in the division algorithm, since also $j = 0 \times n + j$.

Example:
$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ where $\bar{0} =$ set of even integers and $\bar{1} =$ set of odd integers.
$\mathbb{Z}/10\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{9}\}$ where $\bar{3} = \{$positive integers whose last digit is 3$\} \cup \{$negative integers n for which $-n$ has last digit 7$\}$.

Definition:
We can define addition, multiplication and unary minus on $\mathbb{Z}/n\mathbb{Z}$ by $\bar{a} + \bar{b} = \overline{a+b}, \bar{a} \times \bar{b} = \overline{ab}$, and $-\bar{a} = \overline{-a}$, respectively. These are well defined. For example, if $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, then $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$ so $a_2 = qn + a_1$ and $b_2 = rn + b_1$ for some $q, r \in \mathbb{Z}$. $\therefore a_2 b_2 = (qrn + a_1 r + b_1 q)n + a_1 b_1 \implies a_2 b_2 = a_1 b_1$.

One other thing (useful on homeworks):
if $a \equiv b \pmod{n}$ then $\gcd(a, n) = \gcd(b, n)$ because $b = qn + a$ for some $q \in \mathbb{Z}$, and we showed that $\gcd(qn + a, n) = \gcd(a, n)$

Definition:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \text{there exists a } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{a}\bar{c} = \bar{1}\}$.
Example:
$(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$ $(\bar{1} \times \bar{1} = \bar{1}, \bar{5} \times \bar{5} = \bar{1})$
Proposition:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} : a \in \mathbb{Z} \text{ and } \gcd(a, n) = 1\}$.
Proved in your homework.

One other thing: integers a and b are *relatively prime* if $\gcd(a, b) = 1$.
(This is equivalent to: a and b have no prime factor in common).

Groups

Definition:
A *binary operation* on a set G is a function $\star : G \times G \to G$, usually written $(a, b) \mapsto a \star b$ or (often) $(a, b) = ab$.
Such a binary operation is:

- *associative* (if $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$).
- *commutative* if $a \star b = b \star a$.

Examples:
$+, -, \times$ are binary operations on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
$\div$ is not a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, (can't divide by 0).
But $\div$ is a binary operation on $\mathbb{Q}^* = \{r \in \mathbb{Z} : r \neq 0\}$, similarly for $\mathbb{R}^*$ and $\mathbb{C}^*$. (need to check: if $a, b \neq 0$ then $a \div b \neq 0$ in each case). $+$ and $\times$ are binary operations on $\mathbb{Z}/n\mathbb{Z}$.
All of these so far are commutative and associative (except division and subtraction).
Subtraction (on $\mathbb{Z}$) is neither commutative nor associative.
$a \star b = z(a + b)$ on $\mathbb{Z}$ is commutative but not associative.
Let G be the set of function from $\mathbb{R}$ to $\mathbb{R}$. Then composition of functions $(f \circ g = (x \mapsto f(g(x))))$ is associative $(f \circ g) \circ h = f \circ (g \circ h) = x \mapsto f(g(h(x)))$ but not commutative $f(x) = |x|, g(x) = \cos x, |\cos x| \neq \cos |x|$ when $x = \pi$.

Definition:
A *group* is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G, such that

i. $\star$ is associative
ii. there is an element $e \in G$, called the *identity element*, such that $a \star e = e \star a = a$ for all $a \in G$.
iii. for each $a \in G$, there is "an inverse element" a^{-1} that satisfies $a \star a^{-1} = a^{-1} \star a = e$.

Often we'll say "G is a group under $\star$" instead of "$(G, \star)$ is a group", or just "G is a group" if $\star$ is understood.

Note:
A group G has only one element e that satisifies condition (ii), because if e' also satisfies (ii), then $e = e \star e' = e'$ (since both satisify (ii)). Therefore (iii) is well defined.

Examples:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under addition
- $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ are groups under multiplication
- $\mathbb{Z}/n\mathbb{Z}$ is a group under addition
- $\mathbb{Z}/n\mathbb{Z}$ is *not* a group under multiplication (since $\bar{0}$ does not have an inverse).
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are not groups under multiplication (since 0 does not have an inverse).
- $(\mathbb{Z}/n\mathbb{Z})^\times$ *is* a group under multiplication
  Need to check that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ then $\bar{a}\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ($(\mathbb{Z}/n\mathbb{Z})^\times$ is closed under multiplication). This is true because there are $\bar{c}, \bar{d} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a}\bar{c} = \bar{b}\bar{d} = \bar{1}$. Then $(\bar{a}\bar{b})(\bar{c}\bar{d}) = \overline{abcd} = (\bar{a}\bar{c})(\bar{b}\bar{d}) = \bar{1} \times \bar{1} = \bar{1}$ so $\bar{a}\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.
  (We only require $\bar{c}, \bar{d} \in \mathbb{Z}/n\mathbb{Z}$, but in fact they're in $(\mathbb{Z}/n\mathbb{Z})^\times$ because $\bar{a}\bar{c} = \bar{1}$ and $\bar{d}\bar{b} = \bar{1}$.)
  In fact, $\bar{1}$ satisfies condition (ii), multiplication is associative (easy to check) and for all $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\bar{c}$ (as in the def.) satisfies condition (iii). for $\bar{a}^{-1}$. $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under multiplication.
  {bijective functions from $\mathbb{R}$ to $\mathbb{R}$} is a group under compostion, but composition is *not* commutative.
  $(x \mapsto x + 1) \circ (x \mapsto 2x) \neq (x \mapsto 2x) \circ (x \mapsto x + 1)$.