8/29/2022
Mon

Last time Proved: • there are infinitely many primes 4.1
• any integer ≥ 2 can be uniquely factored into primes
• Sketched an argument for any set $X (\neq \emptyset)$ there is a bijection:
equivalence relations on X $\longleftrightarrow$ partitions of X

"Example" Let $X = \mathbb{Z}$. Fix $n \in \mathbb{N}$, $n > 1$. Define a relation $\sim_n$ on $\mathbb{Z}$ by $a \sim_n b \iff n \mid (a-b)$

Then $\sim_n$ is an equivalence relation: (i) $\forall a$, $n \mid (a-a)$ so $a \sim_n a$

(ii) $a \sim_n b \Rightarrow n \mid a-b \Rightarrow n \mid -(a-b) = b-a \Rightarrow b \sim_n a$

(iii) $a \sim_n b$, $b \sim_n c \Rightarrow a-b = kn$, $b-c = \ell n$ for some $k, \ell \in \mathbb{Z}$

$\Rightarrow a-c = (a-b)+(b-c) = a-c = (k+\ell)n. \Rightarrow a \sim_n c.$

We get a partition $\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a]$

where $[a] = \{b \in \mathbb{Z} \mid n \mid (b-a)\} = \{b \in \mathbb{Z} \mid b-a = kn \text{ for some } k\}$

$= \{a+kn \mid k \in \mathbb{Z}\} \equiv a + n\mathbb{Z}$

Claim $\{[a]\}_{a \in \mathbb{Z}} = \{[0], [1], \dots [n-1]\}$

Reason $\forall a \in \mathbb{Z}$ $\exists!$ $q, r \in \mathbb{Z}$ s.t. $a = qn + r$, $0 \leq r < n$.

Hence $a \sim_n r \Rightarrow [a] = [r]$ □

Notation If $\sim$ is an equivalence relation on a set X then

$X/\sim$ = set of equiv classes of $\sim$ $= \{[x] \mid x \in X\}$.

Ex $\sim = \sim_n$ on $\mathbb{Z}$. $\mathbb{Z}/\sim_n \equiv \mathbb{Z}_n = \{[a] \mid a \in \mathbb{Z}\} = \{[0], \dots [n-1]\}$

Remark If $0 \leq k < \ell < n$, then $0 < \ell - k < n$. Hence $n \nmid (\ell - k)$

$\Rightarrow [\ell] \neq [k]$.

$\Rightarrow [0], [1], \dots [n-1]$ are all distinct.

Remark One usually writes $a \equiv b \bmod n$ whenever $n \mid (a-b)$.

Theorem 4.1 Fix $n \in \mathbb{N}$, $n > 1$. Suppose $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ with
$a_1 \equiv a_2 \bmod n$, $b_1 \equiv b_2 \bmod n$.
Then (1) $a_1 b_1 \equiv a_2 b_2 \bmod n$ and (2) $a_1 + b_1 \equiv a_2 + b_2 \bmod n$.

Proof $a_1 \equiv a_2 \bmod n \Rightarrow a_1 - a_2 = kn$ for some $k \in \mathbb{Z}$
$b_1 \equiv b_2 \bmod n \Rightarrow b_1 - b_2 = \ell n$ for some $\ell \in \mathbb{Z}$.

Then
$(a_1+b_1) - (a_2+b_2) = (a_1 - a_2) + (b_1 - b_2) = kn + \ell n = (k+\ell)n$.
$\Rightarrow a_1 + b_1 \equiv a_2 + b_2 \bmod n$.

$a_1 b_1 - a_2 b_2 = (a_2 + kn)(b_2 + \ell n) - a_2 b_2 =$
$a_2 b_2 + kn b_2 + \ell n a_2 + kn\ell n - a_2 b_2 = n(kb_2 + \ell a_2 + kn\ell)$.
$\therefore a_1 b_1 \equiv a_2 b_2 \bmod n$.

Corollary 4.2 We have two well-defined maps
$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, $([a],[b]) \mapsto [a+b]$
$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ $([a],[b]) \mapsto [a \cdot b]$.

Proof If $[a] = [a']$, $[b] = [b']$ then
$[a+b] = [a'+b']$ and $[a \cdot b] = [a'b']$ by 4.1. □

Notation We define $[a] + [b] := +([a],[b])$
$[a] \cdot [b] := \cdot([a],[b])$

Definition A ring is a set R together with two maps
$+, \cdot : R \times R \to R$ and two distinguished elements $0, 1 \in R$
[usually $0 \neq 1$] so that

1) $+$ is commutative and associative: $a+b = b+a \quad \forall a,b \in R$
$(a+b)+c = a+(b+c) \quad \forall a,b,c \in R$

2) $0+a = a = a+0 \quad \forall a \in R$

3) For each $a \in R \quad \exists\, b \in R$ s.t. $a+b = 0$
(ie. There are additive inverses)

4) $\cdot$ is associative: $(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall a,b,c \in R$
(we may write ab for $a\cdot b$)

5) $a\cdot 1 = a = 1\cdot a \quad \forall a \in R$

6) $a\cdot(b+c) = (a\cdot b)+(a\cdot c) \quad \forall a,b,c \in R$
$(b+c)\cdot a = (b\cdot a)+(c\cdot a)$

Examples $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ are rings

$M_n(\mathbb{R})$ = $n\times n$ matrices with real entries
$+$ = matrix addition, $\cdot$ = matrix multiplication
0 = $n\times n$ zero matrix, $1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, identity matrix
is a ring $\forall\, n \geq 1$.

Note in $M_n(\mathbb{R})$ $A\cdot B \neq B\cdot A$, in general.

Definition A ring R is commutative if $ab = ba$ $\forall a,b \in R$.

Ex $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$
is a commutative ring.

$M_2(\mathbb{R})$ is not a commutative ring.

Remark Strictly speaking we haven't checked that $\mathbb{Z}_n$ is a (commutative) ring. But it's easy.

Lemma 4.3 Let R be a rng. Then

1) 0 is unique: if $\exists\, 0' \in R$ s.t. $a + 0' = a = 0' + a$, then $0 = 0'$.

2) 1 is unique: if $\exists\, 1' \in R$ s.t. $a \cdot 1' = a = 1' \cdot a$, then $1 = 1'$.

3) additive inverses are unique: $\forall\, a \in R$ if $\exists\, b, b' \in R$ s.t.

$$a + b = 0 = a + b' \text{, then } b = b'.$$

Proof 1) $0' = 0 + 0' = 0$

2) $1' = 1' \cdot 1 = 1$

3) $b = 0 + b = (b' + a) + b = b' + (a + b) = b' + 0 = b'$.

Notation $\forall\, a \in R$, $-a$ = the unique element of R s.t. $(-a) + a = 0$, the additive inverse of a.

Next time we'll start studying groups (we'll come back to rings in mid October)