

M is one of $\mathbb{N} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$

operations: $+$ and \cdot both $M^2 \rightarrow M$

Properties: (1) Assoc



$\{x_1, x_2, \dots, x_n\} \subset M$ we write $x_1 + x_2 + \dots + x_n$ b.c. induction

$P(n) := x_1 + x_2 + \dots + x_n$ is well-defined regardless of association.

$P(n)$ holds $\forall n \in \mathbb{N}$.

Proof: $P(1), P(2), P(3)$ all true obviously.

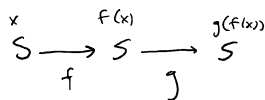
If $P(k)$ then $x_1 + x_2 + \dots + x_k + x_{k+1}$ in any grouping we have

two groups w/ less than n parentheses, both of which are well defined, so the whole sum is well defined. \square

(2) commutativity:

Can do the same thing w/ commutativity.

$g, f: S \rightarrow S$



$$(g \circ f)(x) = g(f(x))$$

comp. not comm but assoc.

(3) Neutral / identity element: 0 for $+$, 1 for \cdot . $0 + x = x + 0 = x$

Uniqueness: $0' + 0 = 0' = 0$

(4) Inverses: $-x$ when $x \in \mathbb{Z}$ or anything bigger and x^{-1} when $0 \neq x \in \mathbb{Q}$ or anything bigger

$$(-x) + x = x + (-x) = 0$$

Uniqueness: $\hat{x} = \hat{x} + x + (-x) = -x$

(5) Distributivity: $x(y+z) = xy + xz$.

\mathbb{Z} satisfies everything except mult. inverse. It is ^{Commutative} Ring.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. \mathbb{Q}, \mathbb{R} are ordered, \mathbb{R}, \mathbb{C} are complete.

$x, y \in \mathbb{Z}$. $x \equiv y \pmod{m}$ if $x - y = nm$ for some $n \in \mathbb{Z}$.

\equiv is an equivalence relation.

$x \in \mathbb{Z} \Rightarrow [x]$ is the equivalence class, $\{y \in \mathbb{Z} \mid y \equiv x \pmod{m}\}$

$\mathbb{Z}/(\equiv \pmod{m})$ means all equivalence classes in \mathbb{Z} .

$$\mathbb{Z}/(\equiv \pmod{m}) = \{[0], [1], \dots, [m-1]\}$$

$$[x] + [y] = [x + y]$$

$$[x][y] = [xy]$$

Other notations:

$$\mathbb{Z}/_m\mathbb{Z} = \mathbb{Z}_m = \mathbb{Z}/(\equiv \pmod{m}) = \mathbb{F}_p$$

when $m=p$ prime

\mathbb{Z}_m a ring. when m is prime \mathbb{Z}_m is a field.

When m not prime, $m = n_1 n_2$ so $[0] = [m] = [n_1][n_2]$

When $m=p$ prime, $\overset{\text{for some } k \in \mathbb{Z}}{[k]} \{[1], \dots, [p-1]\} = \{[1], \dots, [p-1]\}$ when $k \neq 0$

When $m=p$ prime, $[k] \{ [1], \dots, [p-1] \} = \{ [1], \dots, [p-1] \}$ ^{when $k \neq 0$} (prove this)

(multiplication by $[k]$ is bijective (injective) (prove this))

so one element gets mapped to 1. this is $[k]^{-1}$.

Proof multiplication by $[k]$ injective.

If $[k][x] = [k][y]$ then $[kx] = [ky]$ so $kx - ky = np \Rightarrow k(x-y) = np$ for some n
 p not divisible by k , so n divisible by k meaning $x-y = mp$ for some m
so $[x] = [y]$.