Previously.

- Kernels
- The first isomorphism theorem

This Section.

- Rings
- Commutative Rings
- Fields
- Subrings
- Ring Isomorphisms

Definition. Suppose R is a set and it has two binary operations on it (written as $+$ and $\cdot$), then the set R is a `ring` if

1. $(R,+)$ is an abelian group

2. $\cdot$ is associative (i.e., $r_1(r_2r_3) = (r_1r_2)r_3$)

3. the distributive laws hold:

- $r_1(r_2+r_3) = r_1r_2 + r_1r_3$
- $(r_1+r_2)r_3 = r_1r_3 + r_2r_3$

Example. Some rings we know and love.

1. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

2. $(2\mathbb{Z},+,\cdot)$

3. $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$

4. $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ $\leftarrow$ The book calls this $\mathbb{Z}(i)$

5. $(\mathbb{Z}_n,+,\cdot)$

6. $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$

Example. The `direct product` $R_1 \times R_2$ of rings R_1 and R_2 is also a ring with componentwise operations:

- $(a, b) + (c, d) = (a + c, b + d)$
- $(a, b) \cdot (c, d) = (ac, bd)$

Definition. Given a ring $(R, +, \cdot)$,

1. If $\cdot$ is commutative, then we call R a `commutative ring`.

2. The `additive identity` element in R is denoted 0 or 0_R.

3. If there exists a `multiplicative identity` element in R, it is denoted 1 or 1_R. A ring that has a 1_R is called a `ring with unity`.

4. A non-zero element $a \in R$ is called a `zero-divisor` if there is some non-zero $b \in R$ such that $ab = 0$ or $ba = 0$.

5. An element $a \in R$ is called `nilpotent` if there is some $n \in \mathbb{Z}^+$ such that $a^n = 0$.

6. Suppose R is a rings with unity. Then an element $a \in R$ is called a `unit` if there is some $b \in R$ such that $ab = ba = 1$.

7. The `center` $Z(R)$ of a ring R is defined to be

$$Z(R) = \{x \in R \mid xr = rx \ \forall r \in R\}.$$

Question 1. Why don't we care about all the $x \in R$ such that $x + r = r + x$ for all $r \in R$?

8. A ring $R \neq \{0\}$ is called a `division ring` if every non-zero element in R is a unit.

9. A `field` is a commutative division ring.

Exercise 2. Examine these definitions for $(\mathbb{Z}_6, +, \cdot)$?

1. commutative

2. additive identity

3. multiplicative identity

4. zero-divisors

5. nilpotent elements

6. units

7. trivial ring

8. center

9. division ring

10. field

Example. A non-commutative ring called the the quaternions $\mathbb{H}$. Is defined similar to a vector space, or $\mathbb{R}^4$, with a twist:

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

with multiplication working as follows:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Example (Some popular commutative division rings.)**.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ where p is prime

Theorem 3.1.1. If 0 is the zero of a ring R, then $0r = 0 = r0$ for every $r \in R$.

Theorem 3.1.2. Let r and s be arbitrary elements of a ring R.

1. $(-r)s = r(-s) = -rs$

2. $(-r)(-s) = rs$

3. $(mr)(ns) = (mn)(rs)$ for all integers m and n

Definition. A subset S of a ring $(R, +, \cdot)$ is called a `subring` if $(S, +, \cdot)$ is also a ring.

Example. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

The Subring Test. Let $(R, +, \cdot)$ be a ring and S a non-empty subset of R. Then S is a subring of R if

1. $r_1 - r_2 \in S$ for all $r_1, r_2 \in S$

2. $r_1 r_2 \in S$ for all $r_1, r_2 \in S$

3. $1_R \in S$

Example. Prove $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Example. Prove $T_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$.

Definition. Let R and S be rings. A `ring isomorphism` is a bijective map $\phi : R \to S$ such that for all $r_1, r_2 \in R$,

1. $\phi(r_1 + r_2) =$

2. $\phi(r_1 r_2) =$

3. $\phi(1_R) = 1_S$

In this case we say R and S are `isomorphic` and write $R \cong S$.

Some Observations. Let $\phi : R \to S$ be a ring isomorphism.

1. $\phi(0_R) = 0_S$
2. $\phi(-r) = -\phi(r)$
3. $\phi(kr) = k\phi(r)$ for all $k \in \mathbb{Z}$
4. If R and S are rings with unity, then $\phi(1_R) = 1_S$.
5. If ϕ is an isomorphism, then it preserves the addition and multiplication tables of both rings.

Example. Prove that $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are isomorphic as rings.

Definition. If there is some finite n for which

$$n(1_R) = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}}$$

then we say the characteristic of a ring R is the smallest such n (aka, the order of 1_R in the additive group $(R, +)$.) Otherwise we say the characteristic of R is 0. Denote this value by $\operatorname{char} R$.

Exercise 3. (a) $\operatorname{char} \mathbb{Z}_3 =$

(b) $\operatorname{char} \mathbb{R} =$

(c) $\operatorname{char} \mathbb{Z}_4 \times \mathbb{Z}_6 =$

Theorem 3.1.3. If R is a ring and $\operatorname{char} R = n$, then

1. If $\operatorname{char} R = n > 0$, then $kR = \{0\}$ if and only if n divides k.

2. If $\operatorname{char} R = 0$, then $kR = 0$ if and only if $k = 0$.

Fun Fact. If $r \in R$ is nilpotent, then $1 - r$ is a unit.