Rings

Definition. A ring \( \langle R; +, \cdot \rangle \) is a set \( R \), given with binary operations \(+\) ("addition") and \( \cdot \) ("multiplication"), that satisfies:

- \( R_1 \): \( \langle R; + \rangle \) is an abelian group, written additively (so we have 0 and \( -a \) and \( a - b \))
- \( R_2 \): multiplication is associative
- \( R_3 \): the distributive laws hold for all \( a, b, c \in R \):
  \[
  a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc .
  \]

(We typically omit \( \cdot \), and use the usual rules that multiplication is done before addition and subtraction. As above.)

Definition. A ring is commutative if its multiplication operation is commutative.

Theorem 18.8. In any ring \( R \),

1. \( 0a = a0 = 0 \) for all \( a \in R \)
2. \( a(-b) = (-a)b = -ab \) for all \( a, b \in R \)
3. \( (-a)(-b) = ab \) for all \( a, b \in R \).

Proof. (1) \( 0a + 0a = (0 + 0)a = 0a = 0a + 0 \); now cancel \( 0a \).

2. \( ab + a(-b) = a(b - b) = a0 = 0 = ab + (-ab) \); cancel \( ab \) to get \( a(-b) = -ab \).

\( ab + (-a)b = (a - a)b = 0b = 0 = ab + (-ab) \); cancel \( ab \) to get \( (-a)b = -ab \).

3. Apply (2) twice to get \( (-a)(-b) = -(ab) = ab \). \( \square \)

Examples of Rings

- \( \mathbb{Z} \), \( \mathbb{Q} \), \( \mathbb{R} \), and \( \mathbb{C} \). These always have the usual addition and multiplication operations
- \( \langle \mathbb{Z}_n; +, \cdot \rangle \) for all \( n \in \mathbb{Z}^+ \) (\( a \cdot n \) \( b \) is the remainder you get when you divide \( ab \in \mathbb{Z} \) by \( n \))
- \( M_n(\mathbb{R}) \) for all \( n \in \mathbb{Z}^+ \): this is the ring of \( n \times n \) matrices with entries in \( \mathbb{R} \), under matrix addition and matrix multiplication. It is not commutative.
- the (trivial) ring \( \langle \{0\}, +, \cdot \rangle \) (the same as \( \mathbb{Z}_1 \))
- If \( R_1, \ldots, R_n \) are rings, then so is \( R_1 \times \cdots \times R_n \), with \( + \) and \( \cdot \) defined componentwise. If \( R_1, \ldots, R_n \) are commutative, then so is \( R_1 \times \cdots \times R_n \).

Unity Elements

Definition. A unity element of a ring \( R \) is an identity element for its multiplication operation. It is customarily denoted \( 1 \). (\( \langle R; \cdot \rangle \) is not (usually) a group, but it is a binary algebraic structure, so \( 1 \) is unique if it exists: \( 1 = 1' = 1'' \).)

"\( R \) is a ring with unity" means what it says

1
“R is a ring with unity 1” is the same as above, and it also says that the unity element is called “1”.
“R is a ring with unity 1 ≠ 0” is the same as above, and it also requires that R ≠ (0).

Homomorphisms

Definition. A homomorphism from a ring $R$ to a ring $R'$ is a function $\phi: R \to R'$ such that
(a). $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$ and
(b). $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

An isomorphism is a bijective homomorphism.

Definition. The kernel of a ring homomorphism $\phi: R \to R'$ is the subset
$$\ker \phi = \{a \in R : \phi(a) = 0\}.$$  

As is the case for groups, a ring homomorphism is injective if and only if its kernel is trivial.

Examples of Ring Homomorphisms

- The inclusion maps $(0) \to Z \to Q \to R \to C$ are homomorphisms.
- For all $n \in Z^+$ the “reduction modulo $n$” map $\gamma: Z \to Z_n$ is a ring homomorphism (18.11).
- The map $(n \mapsto 2n): Z \to 2Z$ is a group homomorphism but not a ring homomorphism.
- For any ring $R$ the identity map id$_R: R \to R$ is a ring homomorphism.
- If $\phi: R \to R'$ and $\psi: R' \to R''$ are ring homomorphisms then so is their composition $\psi \circ \phi: R \to R''$.

Units, etc.

Definition. Let $R$ be a ring with unity 1 (we will not assume 1 ≠ 0 here). Then a unit in $R$ is an element with a multiplicative inverse.

Examples

- 0 is a unit in the trivial ring (≠ the book).
- The sets of units in $Q$, $R$, and $C$ are $Q^*$, $R^*$, and $C^*$, respectively.
- The units in $Z$ are $±1$.
- What are the units in $Z_n$?

For any ring $R$ with unity, its units form a group under multiplication. This is denoted $R^*$ and called the group of units of $R$. 
**Division Rings and Fields**

**Definition.** A **division ring** or **skew field** is a ring $R$ with $1 \neq 0$ such that all nonzero elements are units (i.e., $\langle R \setminus \{0\}, \cdot \rangle$ is a group).

**Definition.** A **field** is a commutative division ring.

Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ (but not $\mathbb{Z}$).

**Definition.** A **strictly skew field** is a noncommutative division ring.

**Zero Divisors**

**Definition.** A **zero divisor** in a ring $R$ is a nonzero element $a \in R$ such that $ab = 0$ or $ba = 0$ for some nonzero $b \in R$.

Let $R$ be a ring with 1. If $a \in R$ is a zero divisor then $a$ is not a unit.

**Proof.** If $a \in R$ is a unit and $ab = 0$, then
$$b = ab^{-1} = a^{-1}0 = 0,$$

and similarly if $ba = 0$ then $b = 0$. Therefore $a$ is not a zero divisor. \hfill $\Box$

**Units and Zero Divisors in $\mathbb{Z}_n$**

Let $n \in \mathbb{Z}^+$, let $a$ be a nonzero element of $\mathbb{Z}_n$, and let $g = \gcd(a, n)$. Since then $0 < a < n$, we have $0 < g < n$.

Now if $g = 1$ then there are $x, y \in \mathbb{Z}$ such that $xa + yn = 1$, so $xa \equiv 1 \pmod{n}$, and therefore $x \mod n$ (the remainder you get when you divide $x$ by $n$) is a multiplicative inverse for $a$ in $\mathbb{Z}_n$.

If $g > 1$ then $0 < n/g < n$, so $n/g \in \mathbb{Z}_n$, and $a \cdot (n/g) = (a/g)n$ is a multiple of $n$, so $a \cdot (n/g) = 0$ in $\mathbb{Z}_n$. Therefore $a$ is a zero divisor in $\mathbb{Z}_n$, so it is not a unit.

Therefore, we have proved:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

We also showed that the set of zero divisors in $\mathbb{Z}_n$ is

$$\{a \in \mathbb{Z}_n : a \neq 0 \text{ and } \gcd(a, n) \neq 1\}.$$