6. Rings

Rings - Basic Definitions and Examples

Definition: A ring is a set R with *two* binary operations $+$ (addition) and $\times$ (multiplication) such that 1. R is an abelian group under the addition operation. 2. Multiplication is associative. 3. The distributive law holds: $a \times (b + c) = a \times b + a \times c$ and $(b + c) \times a = b \times a + c \times a$. 4. If multiplication is commutative, then R is called a commutative ring. 5. If there is an identity element 1 for multiplication, then R is said to be a ring with identity or with unity.

The properties of arithmetic you expect hold. For example, if $-a$ is the additive inverse of a, then $(-a)(-b) = ab$. The identity element, if it exists, is unique. See DF, Proposition 1 on page 226.

Definitions: Let R be a ring with unity and assume $1 \neq 0$.

1. A *unit* x in R is an element with a multiplicative inverse, so that there is y such that $xy = yx = 1$. The set R^* of units in a ring form a group.
2. A *zero-divisor* in R is a non-zero element x such that there is $y \in R$ with $xy = 0$ or $yx = 0$.
3. If every non-zero element in R is a unit, then R is called a *skew-field* or a *division ring.*
4. A commutative skew-field is called a *field.*
5. A commutative ring with no zero divisors is called a *domain* or an *integral domain.*

Examples:

1. The rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ are all examples of fields.
2. The integers $\mathbb{Z}$ are a commutative ring with unity. It is also an integral domain, but not a field.
3. For each $n \geq 2$, the groups $\mathbb{Z}/n\mathbb{Z}$ are actually commutative rings with unity.
4. If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.
5. If n is composite, then $\mathbb{Z}/n\mathbb{Z}$ is not a domain. Its units $(\mathbb{Z}/n\mathbb{Z})^*$ are the multiplicative group of elements relatively prime to n.
6. Let $R = C([0, 1], \mathbb{R})$ be the space of continuous real-valued functions on

$[0,1]$. R is a commutative ring with unity; its units are the non-vanishing functions. If f vanishes at a point, then f is not a unit, but it is also not a zero divisor.

7. The Gaussian integers $\mathbb{Z}[i]$ are an integral domain. So is $\mathbb{Z}[\sqrt{2}]$.
8. If R is a ring, then the $n \times n$ matrices over R are a ring $M_n(R)$. If R has a unit element, so does $M_n(R)$.
9. If R is a commutative ring with unity, then $R[x]$, the polynomials over R, are a commutative ring with unity.
10. If R is any commutative ring with unity and G is a finite group, then the group ring $R[G]$ consists of functions on G with multiplication by "convolution"
$$(a * b)(g) = \sum_h a(h)b(gh^{-1})$$
11. The real quaternion ring $\mathbb{H}$ consists of sums $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with multiplication using the usual quaternion rules. $\mathbb{H}$ is a division ring.

Proposition: A finite integral domain is a field.

Ring homomorphisms, ideals, and quotients

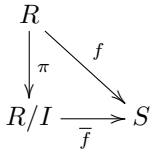
Definition: An subset I of a ring R is a *left ideal* if it is a subring of R (meaning it is closed under addition and multiplication) such that, for all $a \in R$, $aI = \{ax : x \in I\}$ is contained in I. It is a *right ideal* if $Ia \subset I$ for all $a \in R$. It is an *ideal* if it is both a left and right ideal.

Definition: A map $\phi : R \to S$ of rings is a homomorphism if $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.

Lemma: The kernel of a ring homomorphism (the elements that map to zero) form an ideal of R. The image is a subring (i.e. closed under addition and multiplication).

Definition: If R is a ring and I is an ideal, then the quotient R/I consists of elements of the quotient group R/I with multiplication defined by $(a+I)(b+I) = (ab + I)$. This is well defined because I is an ideal. The map $R \to R/I$ given by $a \mapsto a + I$ is a ring homomorphism with kernel I called the *canonical projection.*

Theorem: Let $f : R \to S$ be a homomorphism of rings, let I be the kernel of f, and let $\pi : R \to R/I$ be the canonical projection. Then there is a unique *injective* homomorphism $\overline{f} : R/I \to S$ such that $\overline{f} \circ \pi = f$.



Properties of ideals (in rings with unity)

Assume that R has an identity element for these definitions and theorems.

Definition: If $A \subset R$ is a subset, then RA is the smallest left ideal containing A, AR is the smallest right ideal containing A, and RAR is the smallest ideal containing A.

a. If I is generated by finitely many elements, it is called *finitely generated.*

b. If it is generated by one element, it is called *principal.* If R is commutative, a principal ideal is the multiples aR of a given element $a \in R$.

c. I is called *maximal* if the only ideals of R containing I are I and R.

d. If R is commutative, then an ideal P is called *prime* if $P \neq R$ and $ab \in P$ implies either $a \in P$ or $b \in P$.

Lemma: Suppose R is commutative.

- P is prime if and only if R/P is a domain.
- P is maximal if and only if R/P is a field.

Theorem: Every ideal $I \subset R$ is contained in a maximal ideal.