Theorems

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

Theorem 3.1.3. If R is a ring and char R = n, then

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

Theorem 3.1.5 (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. $s_1 s_2 \in S$ for all $s_1, s_2 \in S$
- **2.** $s_1 s_2 \in S$ for all $s_1, s_2 \in S$
- 3. $1_R \in S$ (if 1_R exists)

Theorem 3.2.1. Let R be a ring. The following are equivalent. That is, either R satisfies all of them or R satisfies none of them.

- **1.** If ab = 0 in R, then a = 0 or b = 0.
- **2.** If ab = ac in R and $a \neq 0$, then b = c.
- 3. If ba = ca in R and $a \neq 0$, then b = c.

Specifically, cancellation holds generally if and only if there are no zero divisors.

Theorem 3.2.2. The characteristic of any domain is either zero or a prime.

Theorem 3.2.3. Every finite integral domain is a field.

Theorem (Wedderburn's Theorem). Every finite division ring is a field.

Theorem 3.3.1. Let I be an ideal of the ring R (with unity). Then the additive group (R/I, +) becomes a ring with multiplication (r + I)(s + I) = rs + I called the factor ring or quotient ring. The unity of R/I is 1 + I and if R is commutative, then R/I is commutative.

Theorem 3.3.2. If I is an ideal of the ring R (that has unity), then the following are equivalent

- **1.** $1 \in I$
- 2. I contains a unit
- 3. I = R

Theorem 3.3.3. If R is a commutative ring, an ideal $P \neq R$ of R is a prime ideal if and only if R/P is an integral domain.

Theorem 3.3.4. Let I be an ideal of the ring R. There is a correspondence

$$\left\{\begin{array}{c} ideals \ of \ R \\ containing \ I \end{array}\right\} \leftrightarrow \left\{ideals \ of \ R/I\right\}.$$

Moreover, this correspondence respects containment.

Theorem 3.3.5. If R is a commutative ring with identity, then R is simple if and only if it is a field.

Theorem 3.3.6. Let M be an ideal of a ring R. Then M is maximal if and only if R/A is simple.

Corollary 1. Let R be a commutative ring, with unity. Let M be an ideal of R. Then M is maximal if and only if R/M is a field.

Corollary 2. Let R be a commutative ring, with unity. If M is a maximal ideal of R, then M is a prime ideal.

Lemma. Lemma 3.3.3 Let R be a ring with unity and $n \ge 1$. Every ideal of $M_n(R)$ has the form $M_n(A)$ for some ideal A of R.

Theorem 3.3.7. If R is a ring with unity then $M_n(R)$ is simple if and only if R is simple.

Corollary 1. If R is a division ring then $M_n(R)$ is simple.

Theorem 3.4.1. Let $\theta: R \to R_1$ be a ring homomorphism and let $r \in R$.

- **1.** $\theta(0) = 0$
- 2. $\theta(-r) = -\theta(r)$ for all $r \in R$
- 3. $\theta(kr) = k\theta(r)$ for all $r \in R$ and $k \in \mathbb{Z}$
- **4.** $\theta(r^n) = \theta(r)^n$ for all $r \in R$ and $n \ge 0$ in \mathbb{Z}
- **5.** If $u \in \mathbb{R}^*$, $\theta(u^k) = \theta(u)^k$ for all $k \in \mathbb{Z}$.

Theorem 3.4.2. Let $R \neq 0$ be a commutative ring with characteristic p, and define

$$\phi: R \to R$$
 by $\phi(r) = r^p$ for all $r \in R$.

Then ϕ is a ring homomorphism.

We call this ϕ the Frobenius Endomorphism. If ϕ is a finite field, we call ϕ the Frobenius Automorphism, which is an isomorphism.

Theorem 3.4.3. Let $\theta \colon R \to S$ be a ring homomorphism. Then

- **1.** $\theta(R)$ is a subring of S
- **2.** $\ker \theta$ is an ideal of R

Theorem 3.4.4 (First Isomorphism Theorem for Rings). Let $\theta: R \to S$ be a ring homomorphism and write $A = \ker \theta$. Then θ induces a ring isomorphism

$$\bar{\theta}: R/A \to \theta(R)$$
 given by $\bar{\theta}(r+A) = \theta(r)$ for all $r \in R$.

Corollary 1. Let A and B be ideals of the rings R and S, respectively. Then $A \times B$ is an ideal of $R \times S$ and

$$\frac{R \times S}{A \times B} \cong \frac{R}{A} \times \frac{S}{B}.$$

Corollary 2. Let A be an ideal of the ring R. Then $M_n(A)$ is an ideal of $M_n(R)$ and

$$\frac{M_n(R)}{M_n(A)} \cong M_n(R/A).$$

Definitions

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.** · is associative (i.e., $r_1(r_2r_3) = (r_1r_2)r_3$)
- **3.** the distributive laws hold:
 - $r_1(r_2+r_3)=r_1r_2+r_1r_3$
 - $(r_1 + r_2)r_3 = r_1r_3 + r_2r_3$

Definition. The direct product $R_1 \times R_2$ of rings R_1 and R_2 is also a ring with component-wise operations:

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

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

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

- **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.

Definition. Given variables i, j, k satisfying $i^2 = j^2 = k^2 = -1$, ij = -ji = k, jk = -kj = i, ki = -ik = j, the set

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

is a ring under under addition and multiplication called the quaternions.

Definition. The *characteristic* of a ring R is the order of 1_R in the additive group (R, +) if the order is finite. Otherwise we say char R = 0. Denote this value by char R.

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

Definition. If R and S are rings with unity, we call a map $\theta: R \to S$ a ring homomorphism if

- **1.** $\theta(r_1 + r_2) = \theta(r_1) + \theta(r_2)$ for all $r_1, r_2 \in R$
- **2.** $\theta(r_1r_2) = \theta(r_1)\theta(r_2)$ for all $r_1, r_2 \in R$
- **3.** $\theta(1_R) = 1_S$

Definition. Let R and S be rings with unity. A ring isomorphism is a bijective ring homomorphism. In this case we say R and S are isomorphic and write $R \cong S$.

Definition. A ring $R \neq \{0\}$ is called a *domain* if ab = 0 implies that either a = 0 or b = 0.

Definition. A commutative domain is called an *integral domain*.

Definition. We say $z \in \mathbb{C}$ is algebraic over \mathbb{Q} if there is some polynomial $p \in \mathbb{Q}[x]$ such that p(z) = 0.

The number field generated by z is the field $\mathbb{Q}(z)$, which is the set of complex numbers of the form $a_0 + a_1 z + a_2 z^2 + \cdots + a_k z^k$ where $k \in \mathbb{N}$ and $a_0, a_1, \ldots, a_k \in \mathbb{Q}$.

Definition. Let $(R, +, \cdot)$ be a ring. An additive subgroup (I, +) of (R, +) is an *ideal of* R if $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$.

Definition. Equivalent definitions of an ideal I of a ring R: (given $(I, +) \leq (R, +)$)

- for all $i \in I$, $iR \subseteq I$ and $Ri \subseteq I$
- for all $i \in I$ and $r \in R$, $ir \in I$ and $ri \in I$.

Definition. If $a \in Z(R)$, then Ra = aR and we call this set the *principal ideal of R generated* by a. Denote this set by (a).

Definition. We call a proper ideal P of a ring R prime if

$$rs \in P \implies r \in P \text{ or } s \in P.$$

Definition. A ring R is a simple ring if $R \neq \{0\}$ and the only ideals of R are $\{0\}$ and R.

Definition. Let R be a ring (not necessarily commutative), and let M be an ideal of R. We call M a maximal ideal of R if

- 1. $M \neq R$, and
- **2.** if I is an ideal of R satisfying $M \subseteq I \subseteq R$, then I = M or I = R.