Basic Definitions and Theorems on Rings

Definition T1 (Identity): Let S be a set with a binary operation $\circledast$. If for some $e \in S$, $a \circledast e = e \circledast a = a$ for all $a \in S$ then e is called an identity under $\circledast$.

Theorem T2 (Uniqueness of identity): Let S be a set with a binary operation $\circledast$. If $a \circledast e = e \circledast a = a$ and $a \circledast f = f \circledast a = a$ for all $a \in S$, then $e = f$.

Theorem T3 (Uniqueness of inverses): Let S be a set with an identity e and an associative binary operation $\circledast$. Let $a \in S$ and assume $a \circledast b = b \circledast a = e$ as well as $a \circledast c = c \circledast a = e$. Then $b = c$.

Definition D4 (Ring): A ring is a set of elements with two binary operations, called addition and multiplication, such that:

- $+$ is closed
- $+$ is commutative
- $+$ is associative
- $+$ has an additive identity, we'll call it 0_R.
- Everything in S has an inverse under $+$, we call them negatives and use the − symbol.
- $\times$ is closed
- $\times$ is associative
- $\times$ is distributive over $+$

Theorem T5 (Uniqueness+ of Identity): Let $e \in R$. If $a + e = a$ for some $a \in R$, then $e = 0_R$.

Theorem T6 (Double Negation): Let $a \in R$. Then $-(-a) = a$.

Theorem T7 (Additive Cancellation): Let $a, b, c \in R$. If $a + b = a + c$, then $b = c$.

Theorem T8 (Zero Multiplication): Let $a, b \in R$. Then $a0_R = 0_R a = 0_R$

Theorem T9 (Moving Negatives): Let $a, b \in R$. Then $a(-b) = (-a)b = -(ab)$.

Theorem T10 (Negative Cancellation): Let $a, b \in R$. Then $(-a)(-b) = ab$.

Theorem T11 (Addition Equation): Let $a, b \in R$. Then $a + x = b$ always has a unique solution.

Definition and Theorems on Subrings

Definition D12: Let R be a ring and $S \subseteq R$. S is said to be a subring of R if S is itself a ring with the same operations as R.

Theorem T13 (Subring criterion): Let R be a ring, and S a subset of R. S is a subring if and only if all of the following are satisfied for all elements $a, b \in S$:

1. $S \neq \emptyset$
2. $a, b \in S \Rightarrow a + b \in S$ (Closed under addition)
3. $a, b \in S \Rightarrow a \cdot b \in S$ (Closed under multiplication)
4. $a \in S \Rightarrow -a \in S$ (Closed under additive inverses)

Theorem T14 (Subring criterion, quick): Let R be a ring, and S a subset of R. S is a subring if and only if all of the following are satisfied for all elements $a, b \in S$:

1. $S \neq \emptyset$
2. $a, b \in S \Rightarrow a - b \in S$ (Closed under subtraction)
3. $a, b \in S \Rightarrow a \cdot b \in S$ (Closed under multiplication)

Theorem T15 (Subring criterion, finite): Let R be a ring, and S a finite subset of R. S is a subring if and only if all of the following are satisfied for all elements $a, b \in S$:

1. $S \neq \emptyset$
2. $a, b \in S \Rightarrow a + b \in S$ (Closed under addition)
3. $a, b \in S \Rightarrow a \cdot b \in S$ (Closed under multiplication)

Theorem T16 (Zero in subring): Let R be a ring and S a subring of R. Then $0_S = 0_R$.

Future Theorem That Appears Later:
Let R be a ring and S a subring of R. If $1_R \in S$, then S has unity and $1_S = 1_R$.

Definition and Theorems involving $\mathbf{1_R}$

Definition D17 (Unity): Let R be a ring. If R contains a multiplicative identity, we call R a ring with unity. We write 1_R to denote the identity.

Definition D18 (Multiplicative Inverses): Let R be a ring with unity and $a \in R$ be nonzero. If there is some $b \in R$ such that $ab = 1_R$ and $ba = 1_R$, then a is called invertible or a unit.
Because of the uniqueness theorem, we may denote such a b as a^{-1}.

Theorem T19 (Left and right inverses): Let R be a ring with unity and let $a, b_1, b_2 \in R$. If both $b_1 a = 1_R$ and $ab_2 = 1_R$ then $b_1 = b_2$.
(As a corollary a is invertible and $b_1 = b_2 = a^{-1}$)

Theorem T20 (one sided inverse is an inverse): Let R be a ring with unity and let $a \in R$ be a unit. If $ab = 1_R$ for some $b \in R$, then $b = a^{-1}$.
Similarly if $ca = 1_R$ for some $c \in R$, then $c = a^{-1}$.

Theorem T21 (Inverse of a product): Let R be a ring with unity and let $a, b \in R$ both be units. The product ab is also a unit and $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem T22 (Identity in a subring): Let R be a ring and S a subring of R. If $1_R \in S$, then S has unity and $1_S = 1_R$.

Theorem T23 (0≠1): Let R be a ring with unity that is not $\{0_R\}$. Then $0_R \neq 1_R$.

Definition D24 (Zero divisor): Let R be a ring and $a \in R$ be nonzero. If there is some other nonzero $b \in R$ such that $ab = 0$ then a and b are called zero divisors.

Theorem T25 (Cancellation) Let R be a ring and assume $a \in R$ is not a zero divisor. Let $b, c \in R$.

- If $ab = ac$, then $b = c$.
- If $ba = ca$, then $b = c$.

Theorem T26 (Units and zero divisors): Let R be a ring with unity and let $a \in R$.

- If a is a unit, it is not a zero divisor.
- If a is a zero divisor, it is not a unit.

Definition D27 (Nilpotent): Let R be a ring and $a \in R$. If there is some positive integer n such that

$$\underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{n \text{ times}} = 0$$

then a is called nilpotent.

Theorem T28 (Nilpotent and zero divisors) Let R be a ring and $a \in R$ be nonzero. If a is nilpotent, then a is a zero divisor.

Definition and Theorems involving Integral Domains

Definition D29 (Commutative): Let R be a ring. If multiplication is commutative, then the ring is called a commutative ring.

Definition D30 (Integral Domain): Let R be a nontrivial ring. If R is commutative and has no zero divisors, then R is called an integral domain.

Theorem T31 (Cancellation): Let R be an integral domain. The cancellation laws apply to R:
If $ab = ac$, then $b = c$

Theorem T32 (Integral Domain Criterion): Let R be ring. If the following are satisfied, then R is an integral domain.

1. R is commutative
2. $R \neq \{0_R\}$
3. $ab = ac \Rightarrow b = c$ for all $a, b, c \in R,\ a \neq 0_R$.

Definition D33 (Divides): Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$. If there is some $k \in R$ such that $bk = a$, then we say b divides a, that a is a multiple of b, and write $b|a$.

Theorem T34 (Properties of divides): Let R be a commutative ring. As a relation, "divides" is reflexive and transitive in that for all $a, b, c \in R$:

1. $a|a$ (If R has unity)
2. If $a|b$ and $b|c$, then $a|c$.

Definition D35 (Associates): Let R be an integral domain with unity. Let $a, b \in R$. If $a = bu$ for some $u \in R^*$, then a and b are called associates.

Theorem T36 (Properties of associates): Let R be an integral domain with unity. "Being associates" is an equivalence relation. In particular for all $a, b, c \in R$:

1. a is an associate with a
2. If a is an associate with b, then b is an associate with a.
3. If a is an associate with b and b is an associate with c, then a is an associate with c.

Theorem T37 (Divides & Associates): Let R be an integral domain with unity and let $a, b \in R$. Then a and b are associates iff both $a|b$ and $b|a$.

Definition D38 (prime): Let R be an integral domain and let $a \in R - R^*$ be nonzero. We say that a is prime if for all $b, c \in R$:
If $a|bc$, then $a|b$ or $a|c$

Definition D39 (Irreducible): Let R be an integral domain with unity and let $a \in R - R^*$ be nonzero. We say that a is irreducible if for all $b, c \in R$: If $a = bc$, then either $b \in R^*$ or $c \in R^*$

Theorem T40 (Prime implies Irreducible): Let R be an integral domain with unity and let $a \in R$ be prime. Then a is also irreducible.

Definition and Theorems involving Ideals

Definition D41 (Ideal): Let R be a ring and S a subring of R. We call S an ideal if the following are satisfied:

- $rs \in S$ for all $s \in S$ and $r \in R$
- $sr \in S$ for all $s \in S$ and $r \in R$

Theorem T42 (Ideals are subrings): Let R be a ring and I an ideal of R. Then I is a subring.

Theorem T43 (What is $\langle 1_R \rangle$?): Let R be a commutative ring with unity. $\langle 1_R \rangle = R$

Definition D44 (Prime Ideal): Let R be a commutative ring. An ideal P of R is called a prime ideal if both:

- $P \neq R$
- If $ab \in P$, then either $a \in P$ or $b \in P$ for all $a, b \in R$.

Definition D45 (Maximal Ideal): Let R be a ring with unity. An ideal M of R is called a maximal ideal if both:

- $M \neq R$
- If $I \supseteq M$ is an ideal of I, then either $I = M$, or $I = R$.

Theorem T46 (Ideals are contained in a maximal ideal): Let R be a ring with unity and I an ideal. Then there is some maximal ideal M such that $I \subseteq M$.

Theorem T47 (Maximal ⇒ Prime): Let R be a commutative ring with unity. Every maximal ideal of R is a prime ideal.

Definition D48 (Finitely Generated): Let R be a commutative ring and I an ideal of R. We call I finitely generated if everything in I can be written sums and products of things in R with things in some finite set $\{a_1, \dots, a_n\}$:

$$I = \langle a_1, \ \dots, a_n \rangle \coloneqq \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n | r_1, \dots, r_n \in R\}$$

Definition D49 (Principal): Let R be a commutative ring and I an ideal of R. We call I principal and use the notation below, if everything in I can be written as a multiple of some single element:

$$I = \langle a \rangle \coloneqq \{ar | r \in R\}$$

Definition D50 (PID): Let R be an integral domain. If every ideal of R is principal, we call R a principal ideal domain.

Theorem T51 (Connection between principal ideals and divisibility): Let R be a commutative ring with unity. Fix two elements $a, b \in R$.

(a) If $\langle a \rangle \subseteq \langle b \rangle$, then $a = bt$ for some $t \in R$.
(b) If $a = bt$ for some $t \in R$, then $\langle a \rangle \subseteq \langle b \rangle$.

Theorem T52 (Connection between principal ideals and the whole ring): Let R be a commutative ring with unity and $r \in R$.

(a) If $\langle r \rangle = R$, then r is a unit.
(b) If r is a unit, then $\langle r \rangle = R$.

Theorem T53 (Connection between principal ideals and associates): Let R be an integral domain with unity and let $r, s \in R$.

(a) If $\langle r \rangle = \langle s \rangle$, then r and s are associates.
(b) If r and s are associates, then $\langle r \rangle = \langle s \rangle$.

Definition and Theorems involving ideals and quotient rings

Definition D54 (Coset): Let R be a ring, S a subring of R, and $a \in R$. The set "$S + a$" is called the "a^th^ coset of S in R"

$$S + a \coloneqq \{s + a | s \in S\}$$

Definition D55 (R mod I): Let R be a commutative right with identity and I an ideal. The quotient ring of R mod I is the collection of cosets of I as below, and addition and multiplication are defined as follows.

$$R/I \coloneqq \{I + r | r \in R\}$$
$$(I + r_1) + (I + r_2) \coloneqq I + (r_1 + r_2)$$
$$(I + r_1)(I + r_2) \coloneqq I + (r_1 r_2)$$

Theorem T56 (Basic properties of R/I): Let R be a commutative right with unity and I an ideal.

1. $I + a = I + b$ iff $a - b \in I$
2. Addition of cosets is well defined.
3. Multiplication of cosets is well defined.
4. R/I is a ring.

Theorem T57 (Relating quotient rings to prime ideals): Let R be a commutative ring with unity and I an ideal of R. The quotient ring R/I is an integral domain if and only if I is prime.

Future Theorems That Appears Later:

Let R be a commutative ring with unity. and I an ideal of R. The quotient ring R/I is a field if and only if I is maximal.
Let R be a commutative ring with unity. R is a field if and only if its only ideals are $\{0\}$ and R itself.

Definition and Theorems involving Unique Factorization Domains

Definition D58 (Irreducible): Let R be an integral domain with unity and let $a \in R - R^*$ be nonzero. We say that a is irreducible if for all $b, c \in R$: If $a = bc$, then either $b \in R^*$ or $c \in R^*$

Definition D59 (Irreducible Factorization): Let R be an integral domain with unity and let $a \in R$. If we can write $a = p_1 p_2 \cdots p_n$ for some $n \in \mathbb{N}$ where each p_k is irreducible, then we say that a has an irreducible factorization.

Definition D60 (Uniqueness): Let R be an integral domain with unity and let $a \in R$ have an irreducible factorization. Suppose we can write

$$a = p_1 p_2 \cdots p_n$$
$$a = q_1 q_2 \cdots q_n$$

for some $n, m \in \mathbb{N}$ where each p_i and q_j are irreducible. We say that the factorization is unique up to associates if $n = m$ and there is some re-numbering of the factors so that $p_k = q_k$ for each k.

Definition D61 (UFD): Let R be an integral domain with unity. If every nonzero nonunit element of R has a unique factorization, we call R a Unique Factorization Domain.

Theorem T62 (Irreducible ⇒ Prime): Let R be a unique factorization domain. Then any element of R is prime iff it is irreducible.

Theorem T63 (GCD from factorization): Let R be a unique factorization domain. Then $\gcd(a, b)$ may be computed by taking their prime factorizations and looking at what is in common.

Theorem T64 (PID ⇒ UFD): Let R be a principal ideal domain. Then R is a unique factorization domain.

Definition and Theorems involving Euclidean Domains

Definition D65 (Norm): Let R be an integral domain with unity. A function $N: R \to \mathbb{N}$ with $N(0_R) = 0$ is called a norm.
Remark: This is very different from the notion of a norm in other subjects such as advanced calculus.

Definition D66 (ED): Let R be an integral domain with unity. We call R a Euclidean Domain if there is a norm N on R such that for any two elements $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that:

$$a = qb + r$$

$r = 0_R$ or $N(r) < N(b)$

Theorem T67 (EA, EEA): Let R be a Euclidean Domain. Both the Euclidean Algorithm and Extended Euclidean Algorithm can be used in R.

Theorem T68 (ED⇒PID): Let R be a Euclidean Domain. Then R is a principal ideal domain.

Definition and Theorems involving Fields

Definition D69 (Field): Let R be an integral domain with unity. If every nonzero element of R is invertible, R is called a field.

Theorem T70 ($\mathbb{Z}_n$ vs $\mathbb{Z}_p$): The ring $\mathbb{Z}_n$ is a field if and only if n is prime, in which case we typically use p instead of n.

Theorem T71 (No zero divisors): Let R be a field. Then R does not have any zero divisors, irreducibles, or primes.

Theorem T72 (Finite ID): Let R be a finite integral domain. Then R is a field.
Note: This applies even if we don't assume R has unity, but the proof is a bit more involved than our proof that assumed unity.

Theorem T73 (Fields and Quotient Rings): Let R be a commutative ring with unity and I an ideal of R. The quotient ring R/I is a field if and only if I is maximal.

Theorem T74 (Ideals in Fields): Let R be a commutative ring with unity. R is a field if and only if its only ideals are $\{0\}$ and R itself.

Theorem T75 (Field ⇒ ED): Let F be a field. Then F is also a Euclidean Domain.

Definition and Theorems specific to polynomial rings, $R[x]$, not covered in the abstract theory

Let R be a commutative ring and F a field in all of the following.

Definition D76: Let R be a ring and $f \in R[x]$. Write $f = a_0 + a_1x + \cdots + a_nx^n$ where $a_n \neq 0$.

- f is called a polynomial.
- n is called the degree of f.
  - Unless $f = 0$ in which case $\deg(f) \coloneqq -\infty$
- Each a_i is called a coefficient.
- Each a_ix^i is called a term.

Definition D77: Let $f = \sum_{i=0}^{n} a_ix^i$ and $g = \sum_{j=0}^{m} b_jx^j$ denote some arbitrary $f, g \in R[x]$. Then:

- $f + g \coloneqq \sum_{k=0}^{\max(n,m)} (a_k + b_k)x^k$
- $fg \coloneqq \left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{j=0}^{m} b_jx^j\right)$

Theorem T78: Conditions as above.

- $fg = \sum_{i=0}^{n} \sum_{j=0}^{m} a_ib_j\, x^{i+j}$
- $fg = \sum_{d=0}^{n+m} \sum_{k=0}^{d} a_kb_{d-k}\, x^d$

Definition D79: Let $f \in R[x]$. If $f \in R$, we call f a constant polynomial.

Theorem T80: Let $a, f \in F[x]$ such that a is a constant polynomial. Then $a|f$.

Definition D81: Let $f \in R[x]$ and $a \in R$. If $f(a) = 0$ then a is called a root of f.

Theorem T82: Let $f \in F[x]$ and $a \in F$. Then $(x - a)|f$ if and only if a is a root of f.

Theorem T83: Let $0 \neq f \in F[x]$ have degree n. Then f has at most n roots

Theorem T84 (Gauss's Lemma): Let $f \in \mathbb{Z}[x]$. If f is reducible in $\mathbb{Q}[x]$, then f is reducible in $\mathbb{Z}[x]$.

Theorem T85 (Rational Root Theorem): Let $f \in \mathbb{Z}[x]$, and write $f = a_0 + a_1x + \cdots + a_nx^n$. If $p,$ and q are coprime integers such that $f\left(\frac{p}{q}\right) = 0$, then $q|a_n$ and $p|a_0$.

Theorem T86 (Eisenstein's Criterion): Let $f \in \mathbb{Z}[x]$, and write $f = a_0 + a_1x + \cdots + a_nx^n$. Let p be a prime number such that:

- $p|a_k$ for $k = 0,\ 1,\ 2,\ \ldots, n-1$.
- $p \nmid a_n$.
- $p^2 \nmid a_0$

Then f is irreducible

Theorem T87: Let $f \in \mathbb{Q}[x]$ or $f \in \mathbb{Z}[x]$ be a polynomial of degree at most 3. Then f is reducible if and only if f has a root in $\mathbb{Q}$.

Definition and Theorems specific to power series rings, $R[\![x]\!]$, not covered in the abstract theory

Let R be a commutative ring and F a field in all of the following.

Definition D88: Let R be a ring and $f \in R[x]$. Write $f = a_0 + a_1x + a_2x^2 \cdots$.

- f is called a power series.
- Each a_i is called a coefficient.
- Each a_ix^i is called a term.

Definition D89: Let $f = \sum_{i=0}^{\infty} a_ix^i$ and $g = \sum_{j=0}^{\infty} b_jx^j$ denote some arbitrary $f, g \in R[\![x]\!]$. Then:

- $f + g \coloneqq \sum_{k=0}^{\infty}(a_k + b_k)x^k$
- $fg \coloneqq \left(\sum_{i=0}^{\infty} a_ix^i\right)\left(\sum_{j=0}^{\infty} b_jx^j\right)$

Theorem T90: Conditions as above.

- $fg = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_ib_j\, x^{i+j}$
- $fg = \sum_{d=0}^{\infty}\sum_{k=0}^{d} a_kb_{d-k}\, x^d$

Theorem T91: Let $f \in R[\![x]\!]$ be denoted as above. Then $f \in (R[\![x]\!])^*$ iff $a_0 \in R^*$.

Definition and Theorems specific to modular arithmetic rings, $\mathbb{Z}/\langle n\rangle$, not covered in the abstract theory

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ in all of the following.

Definition D92: Define $a \equiv b$ mod n via: $a \equiv b$ if and only if $n|a-b$

Theorem T93: The relation $\equiv$ defined above is an equivalence relation.

Definition D94: Write $[c]_n$ to denote the equivalence class of c.

Theorem T95: $[c]_n = \{c + nk | k \in \mathbb{Z}\}$

Theorem T96: $a \equiv_n b$ if and only if $\langle n\rangle + a = \langle n\rangle + b$.

Definition D97: Let $f(x) \equiv a$ be an equation mod n. To solve the equation via brute force means to plug in every value of $x \in \mathbb{Z}_n$ and take note of which are solutions.

Theorem T98: Let $a \in \mathbb{Z}_n$. Then $a \in (\mathbb{Z}_n)^*$ iff $\gcd(a, n) = 1$.