Algebra II Reference Sheet

Rings

(Def.) A set R with binary operations $(+, \cdot)$ is a **Ring** if for $a, b, c \in R$:

1. $a + b = b + a$
2. $a + (b + c) = (a + b) + c$
3. R has an additive identity, denoted 0
4. R has additive inverses
5. $a(bc) = (ab)c$
6. $a(b + c) = ab + ac$

Terminology

1. Commutative Rings
2. Unity
3. Units
4. Zero Divisors

Properties

1. $a0 = 0a = 0 \ \forall\, a \in R$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$, $(b - c)a = ba - ca$

Subring

(Def.) A subset of a Ring is a **Subring** if it is itself, a Ring under the same operations.

3-Step Subring Test

$S \subseteq R$ is a Subring of R iff:

1. $S \neq \varnothing$
2. S is closed under subtraction
3. S is closed under multiplication

Integral Domains

(Def.) A Ring R is an **Integral Domain** if:

1. R has unity
2. R is a Commutative Ring
3. R has no Zero Divisors

Theorem: Cancellation

If D is an Integral Domain and $a, b, c \in D$ and $a \neq 0$, with $ab = ac$, then $b = c$.

Fields

(Def.) A **Field** is a Commutative Ring with Unity in which every nonzero element is a Unit.

Theorems:

1. A finite Integral Domain is a Field
2. For every prime p, $\mathbb{Z}_p$ is a Field (Ring of integers modulo p)

Ideals

(Def.) A Subring I of a Ring R is an **Ideal** of R if for every $a \in I$ and $r \in R$, then $ar, ra \in I$.

Ideal Test

$I \subseteq R$ is an Ideal of R iff:

1. $I \neq \varnothing$
2. I is closed under subtraction
3. $\forall a \in I$ and $r \in R$, $ar, ra \in I$

Terminology

1. Principal Ideals , $\langle a \rangle = \{ar | r \in R\}$, with R Commutative
2. Maximal Ideals and Prime Ideals
3. Ideal Lattice

Factor Rings

I is an Ideal of a Ring R iff R/I is a Ring where R/I is the set of Cosets of I in R under $+$.

Theorems

1. R/I is an Integral Domain iff I is Prime
2. R/I is a Field iff I is Maximal

Ring Homomorphisms

(Def.) If R, S are Rings and $\phi : R \to S$, then ϕ is a **Ring Homomorphism** if ϕ preserves operations.

Terminology

1. Kernel of ϕ, $ker\phi$
2. Ring Isomorphism (Bijective Ring Hom.)
3. Field of Quotients

Ring Isomorphism Theorem

Given Rings, R, S and Ring Hom. $\phi : R \to S$, $\psi : R/ker\phi \to \phi(R)$ by $\psi(r + ker\phi) = \phi(r)$ is a Ring Isomorphism

Properties

If $\phi : R \to S$ is a Ring Homomorphism and $r \in R$,

1. If $n \in \mathbb{Z}$, $\phi(nr) = n\phi(r)$, $\phi(r^n) = [\phi(r)]^n$
2. A is a subring of $R \Rightarrow \phi(A)$ is a subring of R
3. ϕ onto and I Ideal of $R \Rightarrow \phi(I)$ Ideal of S
4. J Ideal of S, then $\phi^{-1}(J)$ Ideal of R
5. $ker\phi$ is an Ideal of R

Polynomial Rings

(Def.) Let R be a Commutative Ring. The **Polynomial Ring**, $R[x]$ is:

$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 | a_i \in R, n \in \mathbb{N} \cup \{0\}\}$

Terminology

1. Polynomial Equality
2. Degree of a Polynomial

Theorems

F is a Field, D is an Integral Domain:

1. (Factoring Thrm.) If $f \in F[x], a \in F, f(a) = 0$ then $\exists q \in F[x]$ with $f(x) = (x-a)q(x)$
2. (Division Alg.) If $f, g \in F[x], g \neq 0$ then $\exists! q, r \in F[x]$ with $f = qg + r$, $\deg(r) < \deg(g)$
3. If $f \in D[x]$ is a unit, then $f(x) = a$, $a \in D$
4. If $f \in F[x]$, $\deg(f) = n$, then f has at most n roots.

Principal Ideal Domains

(Def.) A **Principal Ideal Domain**, P is an Integral Domain where every Ideal is a Principal Ideal.

Theorem

1. If F is a Field, then $F[x]$ is a PID.

Factorization of Polynomials

(Def.) Let D be an Integral Domain, then $f \in D[x]$ is **irreducible** if $f = gh \Rightarrow g$ or h is a unit. Otherwise we say f is **reducible**.

Theorems

Let F be a Field.

1. Let $f \in F[x]$, $\deg(f) \geq 2$. If f has a zero, then f is reducible over F. If $\deg(f) = 2, 3$ then the relation is an iff.
2. Let $f \in \mathbb{Z}[x]$. If f is reducible over $\mathbb{Q}$, then f is reducible over $\mathbb{Z}$.
3. (Rational Root Thrm.)
4. (Conjugate Root Thrm.)
5. (Eisensteins's Criterion)
6. Let $p \in F[x]$, then $\langle p \rangle$ is Maximal iff p is irreducible over F.

Factoring in Integral Domains

(Def.) Let D be an Integral Domain. Then $a, b \in D$ are **associates** if $\exists$ a unit $u \in D$ with $a = bu$. Say $c \in D, c \neq 0$, c nonunit, then c is **irreducible** if $c = xy \Rightarrow x$ or y is a unit. Say $p \in D, p \neq 0$, p nonunit, then p is **prime** if $p|st \Rightarrow p|s$ or $p|t$.

Terminology

1. For $d \in \mathbb{Z}, d \neq 1, p^2 \nmid d, p$ prime, define the **Norm**, $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}^+ \cup \{0\}$ by
$$N(a + b\sqrt{d}) = |a^2 - db^2|$$
where:
    1. $N(x) = 0$ iff $x = 0$
    2. $N(xy) = N(x)N(y)$
    3. x is a unit iff $N(x) = 1$
    4. If $N(x)$ prime, then x is irreducible

Theorems

1. In an Integral Domain, prime $\Rightarrow$ irreducible
2. In a PID, prime $\Leftrightarrow$ irreducible

Unique Factorization Domains

(Def.) Let D be an Integral Domain, Then D is a **Unique Factorization Domain** if:

1. Every nonzero, nonunit can be written as a product of irreducibles
2. This factoring is unique up to associates and order.

Ascending Chain Theorem

Let D be a PID and let $I_1, I_2, \dots$ be Ideals of D with $I_1 \subsetneq I_2 \subsetneq \cdots$. Then this chain is finite.

Euclidean Domains

(Def.) Let D be an Integral Domain. Then D is a **Euclidean Domain** if there is a function, $d : D \backslash \{0\} \to \mathbb{Z}^+ \cup \{0\}$ with

1. $d(a) \leq d(ab)\ \forall a, b$
2. $a, b \in D$, $d(b) \leq d(a)$, then $\exists q, r \in D$ with $a = bq + r$, $d(r) < d(b)$ or $r = 0$

Theorems

1. ED $\Rightarrow$ PID $\Rightarrow$ UFD
2. Let D be a PID, $p \in D$. $\langle p \rangle$ is Maximal iff p is irreducible.

Extension Fields and Splitting Fields

(Def.) E is an **Extension Field** of a Field F if $F \subseteq E$ and $F's$ operations are the same as E.

(Def.) Let E be an Extension Field of F and $f \in F[x], deg(f) \geq 1$. We say f **splits** in E if $\exists a \in F$ and $a_1, a_2, \dots, a_n \in E$ with
$$f(x) = a(x - a_1)(x - a_2) \cdots (x - a_n)$$
We call E a **Splitting Field** for f over F if:
$$E = F(a_1, a_2, \dots, a_n)$$

Fundamental Theorem of Field Theory

Let F be a Field and $f \in F[x], deg(f) \geq 1$. Then there is an Extension Field E of F where f has zeros in E.

Theorems

1. Let D be an Integral Domain. Then there exists a Field F that contains a Subring isomorphic to D.
2. Let D be an Integral Domain and F its Field of Quotients. If E is a Field containing D, then E contains a Subfield that is isomorphic to F.