Intro Ring and Field Theory Cheat Sheet

Ring and Field Axioms

A ring R is a set with two binary operations $+$ and $\times$ satisfying the following axioms:
i. $(R,+)$ is an abelian group.
ii. Multiplicative associativity: $(a\times b)\times c = a\times(b\times c)\ \forall a,b,c\in R$.
iii. Left and right distributivity:
$(a+b)\times c=(a\times c)+(b\times c)$ and $a\times(b+c)=(a\times b)+(a\times c)$.
In addition to these rings may also have the following optional properties.
a. Multiplicative commutativity: $a\times b=b\times a,\ \forall\, a,b\in R$.
b. Multiplicative Identity: $\exists\, 1\in R$ s.t. $\forall a\neq 0\in R, 1\times a=a\times 1=a$.
c. Multiplicative Inverse: $\forall\, a\neq 0\in R\ \exists\, a^{-1}\in R$ s.t. $a\times a^{-1}=a^{-1}\times a=1$.

FOR THE PURPOSE OF THIS SHEET WE LOOK AT RINGS WITH MULTIPLICATIVE COMMUTATIVITY AND 1≠0.

A field F is a set with two binary operations $+$ and $\times$ satisfying the following axioms:
i. $(F,+)$ is an abelian group with identity 0.
ii. The non-zero elements of F form a abelian group under multiplication with identity 1.
iii. Left and right distributivity.

Polynomial Rings

For a ring R, $R[x]$ denotes the polynomial ring of a single variable x s.t.the elements of $R[x]$ are of the form
$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ with $n\geq 0$ and $a_i\in R$
Polynomial rings can be generalized for multiple variables.

Zero Divisors, Units and Integral Domains

i. Zero Divisor: $a\neq 0\in R$ is called a zero divisor of R if $\exists\, b\neq 0\in\ R$ s.t. either $ab=0$ or $ba=0$.
ii. Unit: For a ring R with identity $1\neq 0$, $u\in R$ is called a unit in R if $\exists v\in R$ s.t. $uv=vu=1$.
iii. Integral Domain: A commutative ring with identity $1\neq 0$ is called an integral domain if it has no zero divisors.

- Any finite integral domain is a field.
- If R is an integral domain than the polynomial ring of one variable over R, i.e. $R[x]$, is also a integral domain.

Subrings

A subring of the ring R is defined as a subgroup of R that is closed under multiplication.

Ring Homomorphisms, Isomorphisms and Kernels

For rings R and S.
i. Ring Homomorphism is a map $\varphi:R\to S$ satisfying:

- $\varphi(a+b)=\varphi(a)+\varphi(b)\ \forall\, a,b\in R$
- $\varphi(ab)=\varphi(a)\varphi(b)\ \forall\, a,b\in R$

ii. Isomorphism is a bijective ring homomorphism.
iii. Kernel of the ring homomorphism φ is the set of elements of R that map to 0 in S.

- The image of φ is a subring of S.
- The kernel of φ is a subring of S. *(For Rings without 1)*

Ideals

Ideal: A subset I of ring R is called an ideal of R if

- It is a subring of R.
- It is closed under both left and right multiplication with elements from R.

Ideals are to rings what normal subgroups are to groups.

Quotient Rings

Let R be a ring with ideal I. R/I is called a quotient ring if
i. $(r+I)+(s+I)=(r+s)+I$
ii. $(r+I)\times(s+I)=(rs)+I$

First Isomorphism and Correspondence Theorem

i. First Isomorphism Theorem: Let $\varphi:R\to S$ be a ring homomorphism from ring R to S then:

- Kernel of φ is an ideal of R,
- Image of φ is a subring of S and,
- $R/\ker\varphi\cong\varphi(R)$.

ii. Correspondence Theorem: Let R be a ring, and I be an ideal of R. The correspondence $A\leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I.
or
There exists an inclusion preserving biijection between ideals in R containing $\ker(\varphi)$ and ideals in $\varphi(R)$.

Principal, Prime and Maximal Ideals

i. Principal Ideals: An ideal generated by a single element is called a principal ideal.
ii. Prime Ideals: If $P\neq R$, then an ideal P is called a prime ideal if $ab\in P$, when $a,b\in R$ then at least one of a and b in an element of P. *This is analogous to the definition of prime numbers in number theory*
iii. Maximal Ideals: If $M\neq R$, then an ideal M is called a maximal ideal if the only ideals containing M are M and R itself.
• *Every maximal ideal of R is a prime ideal.*
• *The ideal P is a prime ideal in R iff R/P is an integral domain.*

Zorn's Lemma

If S is any nonempty partially ordered set in which every chain has an upper bound, then S has a maximal element.

Ring of Fractions of an Integral Domain

Let R be an integral domain. Let K be the ring of fractions of R s.t. $K=\{\frac{a}{b}|a,b\ \in\ R, b\neq 0\}$. K is also called a field of fractions since it always forms a field for any ring R.

- $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $b,d\ \neq 0$
- $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$, $b,d\ \neq 0$

Chinese Remainder Theorem

The ideals I and J of a ring R are said to be **comaximal** if $I+J=R$.
Chinese Remainder Theorem: $\forall\, a,b\ \in R$, $\exists\, x\ \in\ R$ s.t.
$x\equiv a(\text{mod } I)$ and $x\equiv b(\text{mod } J)$

Noetherian Rings

A commutative ring R is called **Noetherian** if there is no infinite increasing chain of ideals in R, i.e. when $I_1\subseteq I_2\subseteq I_3\ldots$ is an ascending chain of ideals $\exists\, k\in\mathbb{Z}^+$ s.t. $I_k=I_m\ \forall k\geq m$.
It is equivalent to say that R is Noetherian if every ideal of R is finitely generated.

Hilbert Basis Theorem

If R is a noetherian ring then so is the polynomial ring $R[x]$.
$R[x_1,x_2,x_3,\ldots,x_n]$ for finite n is also noetherian.

Irreducible and Prime Elements

i. Irreducible Element An element a of ring R is called **irreducible** if it is non-zero, not a unit and, *only has trivial divisors (i.e. units and products of units).*
ii. Prime Element An element a of ring R is called **prime** if it is non-zero, not a unit and, if $a\mid bc$ then either $a\mid b$ or $a\mid c$ for some $b,c\ \in\ R$.
The concept of primes and irreducible is the same in integers, but they are distinct in general.
In an integral domain, every prime element is irreducible, but the converse holds only in UFDs.

Norm and Euclidean Domain

i. Norm: For a integral domain R, any function $N:R\to\mathbb{Z}^+\cup 0$ with $N(0)=0$ is called a *norm* on R.
ii. Euclidean Domain: An integral domain R is called an **Euclidean Domain** if there is a norm N on R s.t. for any two elements $a,b\ \in\ R$, where $b\neq 0\ \exists\, q,r\ \in\ R$ s.t. $\mathbf{a=qb+r}$ **where** $\mathbf{r=0}$ **or** $\mathbf{N(r)<N(b)}$.
• Any field F is a trivial example of a Euclidean Domain.

Principal Ideal Domains (PIDs)

A **Principal Ideal Domain (PID)** is an integral domain in which every ideal is principal.
Every Euclidean Domain is a PID.
Examples:
•$\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not.
•$F[x]$ if F is a field, •$Z[i]$

Unique Factorisation Domains (UFDs)

Two elements $a,b\ \in\ R$ are said to be **associates** in R if they differ by a unit, i.e. $a=ub$ for some unit $u\ \in\ R$. A **Unique Factorisation Domain (UFD)** is an integral domain R in which every nonzero element $r\ \in\ R$ which is not a unit follows the properties:
i. r can we written as a finite product of irreducibles p_i of R.
ii. This decomposition is unique up to associates, i.e. if $r=p_1p_2\ldots p_n$ and $r=q_1q_2\ldots q_n$ then $m=n$ and for some renumbering of factors there is p_i associate to q_i
The above definition can be equivalently stated as:
A UID is any integral domain in which every non-zero, non-invertible element has a unique factorisation.
•**Every PID is a UID.**
• $Z[x]$ is a UID, but not a PID.
•In a UID every non-zero element is a prime iff it is irreducible.
• Fields $\subset$ Euclidean Domains $\subset$ PIDs $\subset$ UFDs $\subset$ Integral Domains.

Primitive Polynomials and Gauss' Lemma

A polynomial $f(x) \in \mathbb{Z}[x]$ is called **primitive** if $n = deg(f) > 0$, $a_n > 0$ and, $gcd(a_0, a_1, \ldots, a_n) = 1$ for $a_i \in \mathbb{Z}$
Gauss' Lemma: If $f(x), g(x) \in \mathbb{Z}$ are primitive $\implies$ fg is also primitive.

Eisenstein's Criterion

The Eisenstein's Criterion is a test for irreducibility of polynomials.
Let P be a prime ideal of the integral domain R amd, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$.
Eisenstein's Criterion states that $f(x)$ is irreducible in R[x] if
• $a_{n-1}, \ldots a_1, a_0$ are elements of P and,
• a_0 is **not** an element of P^2.
If Eisenstein's Criterion doesn't directly apply to f(x) try on f(x+1), if f(x+1) is irreducible it implies f(x) is also irreducible.

Characteristics of Fields

Let 1_F denote the identity of F.
The **characteristic** of a field F, denoted as $ch(F)$ is defined as the smallest integer p such that $p \cdot 1_f = 0$ if such a p exists and is defined as 0 otherwise.
• $ch(F)$ is either 0 or a prime p, • $\mathbb{Q}$ and $\mathbb{R}$ have characteristic 0
• $F_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p,

Field Extensions and Degree

If K is a field containing the subfield F, then K is said to be an **extension field** of F. It is denoted as K/F.
The **degree** of a field extension K/F denoted by $[K : F]$ is the dimension of K as a vector space over F.

Irreducible Polynomials in Fields

• For a irreducible polynomial $p(x) \in F$, there exists a field K containing a isomorphic copy of F in which $p(x)$ has a root, i.e. there exists a field extension K of F in which $p(x)$ has a root. A simple way to find this extension is to consider the quotient $K = F[x]/(p(x))$.
• For the above case, let $\theta = x \mod (p(x)) \in K$. Then the elements $1, \theta, \theta^2 \ldots \theta^{n-1}$ are a basis for K as a vector space over F, with $[K : F] = n$.
• For the above case, let α be the root of $p(x)$ s.t. $p(\alpha) = 0$. Then, $F(\alpha) \cong F[x]/(p(x))$.

Algebraic and Transcendental Elements

i. Algebraic Element: If K is a field extension over F, then $\alpha \in K$ is called **algebraic** over F, if there exists some non-zero polynomial $f(x)$ with coefficients, in F, s.t. $f(\alpha) = 0$.
ii. Transcendental Element: Elements $\alpha \in K$ which are not algebraic over F are called **transcendental**.
• If α is algebraic over F, then $F[\alpha] = F(\alpha)$, if α is transcendental over F, then $F[\alpha] \neq F(\alpha)$.

Algebraic Extensions

• Let α be algebraic over F. There there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root.
• If L/F is an extension of fields and α is algebraic over both F and L then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.
• If $F(\alpha)$ is the field generated by α over F then, $F(\alpha) \cong F[x]/(m_\alpha(x))$.
• Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$ • Similarly, $[K : F]$ divides $[L : F]$.
• Let K_1, K_2 be two finite extensions of field F contained in K. Then, $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$, but if $[K_1 : F] = n, [K_2 : F] = m$ and if gcd $(m, n) = 1$. Then, $[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$.

Splitting Fields

Splitting Fields: The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ but not over any proper subfield of K containing F.
• For any field F, if $f(x) \in F[x]$. Then, there exists an extension K of F which is a splitting field for $f(x)$.
• A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.
• Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic. • The polynomial $x^n - 1$ over $\mathbb{Q}$ has in general a splitting field contained in $\mathbb{C}$.
• Let $\mathbb{Q}(\zeta_n)$ be the cyclotomic field of n^{th} roots of unity. $[\mathbb{Q}\zeta_n : \mathbb{Q}] = \varphi(n)$ where $\varphi(n)$ is Euler's totient function.

Algebraic Closure of Fields

• The field $\bar{F}$ is called an **algebraic closure** of F if $\bar{F}$ is algebraic over F and, if every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$.
• A field K is said to be **algebraically closed** if every polynomial with coefficients in K has a root n K. $\bar{F}$ as defined above is algebraically closed.
• For every field F there exists an algebraically closed field K containing F.

Fundamental Theorem of Algebra

The field $\mathbb{C}$ is algebraically closed.

Finite Fields

• For every prime $p \in \mathbb{N}$ there exists a field $\mathbb{F}_p$ of order p, e.g.$\mathbb{Z}/p\mathbb{Z}$.
• For any finite field F, the order of F is $q = p^r$ for some prime p and positive integer r.

Structure Theorem for Finite Fields

Let p be a prime integer and let $q = p^r$ for some positive integer r. Then the following statements hold.

- There exists a field of order q.
- Any two fields of order q are isomorphic.
- Let K be a field of order q. The multiplicative group K^x of non-zero elements of K is a cyclic group of order $q - 1$.
- Let K be a field of order q. The elements of K are the roots of $x^q - x \in \mathbb{F}_p[x]$.
- A field of order p^r contains a field of order $p^k \iff k|r$
- The irreducible factors of $x^q - x$ over $\mathbb{F}$ are the irreducible polynomials in $\mathbb{F}[x]$ whose degree divides r.