12 Rings and Fields

12.1 Definition Groups and Abelian Groups
Let $R$ be a non-empty set. Let $+$ and $\cdot$ (multiplication) be two binary (must be “closed”) operations satisfying:

1. $a + b = b + a$ ($\forall a, b \in R$)
2. $(a + b) + c = a + (b + c)$ ($\forall a, b, c \in R$)
3. There exists $0 \in R$ such that $a + 0 = a$ ($\forall a \in R$)
4. To each $a \in R$, there exists $" - a " \in R$ so that $a + ( - a ) = 0$

Just rules 2, 3, 4 make $R$ a group. $(R, +)$ is an Abelian group.

12.2 Definition Rings

5. $(ab)c = a(bc)$ ($\forall a, b, c \in R$)
6. $a \cdot (b + c) = ab + ac$ ($\forall a, b, c \in R$)
7. $(a + b)c = ac + bc$ ($\forall a, b, c \in R$)

12.3 Definition Commutative Rings
If $ab = ba$ for all $a, b \in R$, we call $R$ a commutative ring.

12.4 Definition Unity
A non-zero element of a ring $R$, 1, is called a unity if it is an identity element in multiplication. Unity, if exists, is unique.

12.4 Theorem
1. In a ring $(R, +, \cdot)$, to each $a \in R$, “$ - a $” is unique, and $0 \in R$ is also unique.
2. $a \cdot 0 = 0 \cdot a = 0$ for all $a \in R$
3. $a(-b) = (-a)b = -(ab)$
4. $(-a)(-b) = ab$
5. $a(b - c) = ab - ac$
   $(a - b)c = ac - bc$

12.5 Definition Direct Sum

Construction of new rings from known ones. Let $R_1, R_2, \cdots, R_n$ be rings. Their direct sum $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ is the set $\{(r_1, r_2, \ldots, r_n) \mid r_i \in R_i\}$ with the operations:

$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$

$(r_1, \ldots, r_n)(s_1, \ldots, s_n) = (r_1 s_1, \ldots, r_n s_n)$

The Cartesian product with the above 2 operation is indeed a ring. It is called the direct sum of $R_1, \ldots, R_n$.

12.6 Definition Ring Isomorphisms

Let $R$ and $S$ be 2 rings. An isomorphism $\phi$ from $R$ to $S$ is a bijective mapping (also known as a one-to-one correspondence) which preserves the algebraic (ring operations). Long form: if $r_1 + r_2 = r_3$ in $R$, then $\phi(r_1) + \phi(r_2) = \phi(r_3)$ in $S$ and if $r_1 r_2 = r_3$ in $R$, then $\phi(r_1)\phi(r_2) = \phi(r_3)$ in $S$.

In shorter form, $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ for all $r_1, r_2 \in R$.

We say that $R$ and $S$ are isomorphic if an isomorphism exists from $R$ to $S$, i.e. $R \cong S$.

12.7 Theorem Chinese Remainder Theorem

If $m, n$ are coprime (positive integers), then $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

12.8 Proposition

For rings $R_1, R_2, R_3$:

1. $R_1 \oplus R_2 \simeq R_2 \oplus R_1$
2. $(R_1 \oplus R_2) \oplus R_3 \simeq R_1 \oplus (R_2 \oplus R_3)$

That is $\oplus$ is commutative and associative.

12.9 Theorem

$R \oplus S$ is a ring with unity if and only if both $R$ and $S$ are rings with unity. In fact, if $1 \in R$ and $\bar{1} \in S$ are the unities of $R$ and $S$ respectively, then $(1, \bar{1})$ is the unity of $R \oplus S$, and vice versa.

12.10 Definition Unit

Let $R$ be a ring with unity $1$. An element $a \in R$ is called a unit if it has a multiplicative inverse, i.e. there exists a $b$ in $R$ so that $ab = ba = 1$. All units of $R$ is denoted by $U(R)$.

12.11 Definition Subrings

Let $R$ be a ring, a subset $S$ of $R$ is a subring if it is by itself a ring under the operations of $R$.

12.12 Theorem Subring Test

A non-empty subset $S$ of a ring $R$ is a subring iff it is closed under subtraction and multiplication.

12.13 Theorem

2
If $R$ is a ring and $\mathcal{F}$ is a family of subrings of $R$, then the intersection of $\mathcal{F} = \{x \in R \mid x \in S \text{ for every } S \in \mathcal{F}\}$ is a subring of $R$.

12.14 Theorem Generated Subrings

There exists a smallest subring of $R$ which contains $A$ (over all the subrings which contain $A$). We call it the subring generated by $A$, denoted by $\langle A \rangle$. 
13 Integral Domains

13.1 Definition Zero Divisor
A zero divisor is a non-zero element of a commutative ring for which there exists a non-zero \( b \in R \) so that \( ab = 0 \).

When \( a, b \) are both non-zero and \( ab = 0 \) in a commutative ring, then both \( a \) and \( b \) are zero divisors.

13.2 Definition Integral Domains
An integral domain is a commutative ring, with unity, without zero divisors. Thus, in an integral domain, if \( ab = 0 \), then either \( a = 0 \) or \( b = 0 \).

13.3 Proposition Cancellation Law
In an integral domain, we have the cancellation law: if \( a \neq 0 \), and \( ab = ac \) (where \( b, c \in R \)) as well, then \( b = c \).

13.4 Terminology Injective Maps
A map \( f \) from set \( X \) to set \( Y \) is injective if \( f(b) = f(c) \Rightarrow b = c \).

13.5 Theorem
In an integral domain, left (or right) multiplication by \( a \neq 0 \) is an injective function of \( R \) to \( R \): \( f(x) = ax \) for all \( x \in R \).

13.6 Corollary
If \( R \) is a finite integral domain, then (left) multiplication by \( a \neq 0 \) is surjective (in addition to being injective).

Thus, every non-zero \( a \) in \( R \) (finite \( R \)) is a unit.

13.7 Definition Fields
A field is a commutative ring with unity where every non-zero element is a unit.

13.8 Corollary
Every finite integral domain is a field.

13.9 Proposition
\( \mathbb{Z}_m \) is an integral domain (field) iff \( m \) is prime.

13.10 Theorem
Every field is an integral domain.

13.11 Definition Embeddings of Rings
A ring \( R \) is said to be embedded in a ring \( S \) if there is an injective map \( f : R \to S \) preserving the operations:

1. \( f(r_1 + r_2) = f(r_1) + f(r_2) \)
2. \[ f(r_1r_2) = f(r_1) + f(r_2) \]
for all \( r_1, r_2 \in R \).

In terms of isomorphisms, \( f \) is an isomorphism between \( R \) and the image of \( R \) in \( S \). The image is a subring of \( S \).

13.12 Proposition
If \( R_1 \) can be embedded in \( R_2 \), and that \( R_2 \) can be embedded in \( R_3 \), then \( R_1 \) can be embedded in \( R_3 \).

13.13 Question
If \( R_1 \) can be embedded in \( R_2 \) and \( R_2 \) can be embedded in \( R_1 \), does it imply that \( R_1 \) and \( R_2 \) are isomorphic?

13.14 Proposition
1. If \( F \) is a field, and \( S \subset F \) is a subring, then \( S \) is commutative. Further, if \( S \) has unity, then \( S \) is an integral domain.
2. If \( R \) can be embedded in a field \( F \), and \( R \) has unity, then \( R \) is an integral domain.
3. A ring \( R \) is an integral domain iff it can be embedded in a field and \( R \) has a unity matching the unity of \( F \).

13.15 Definition Ring Characteristics
Let \( R \) be a ring. The least positive integer \( n \) such that
\[ a + \cdots + a \text{ (n-fold)} = 0 \]
for all \( a \in R \) is called the characteristic of \( R \). If no positive integer \( n \) gives such a line, we say that the characteristic of \( R \) is 0.

13.16 Proposition
If \( R \) has a unity, then its characteristic is equal to the first (least) positive \( n \) so that \( 1 + \cdots + 1 \text{ (n-fold)} = 0 \). If there is no such \( n \), the characteristic will be 0.

13.17 Proposition
For an integral domain, the characteristic is either 0 or a prime.
14 Ideals and Factor Rings

14.1 Definition Ideals
Let $R$ be a ring. An ideal $I$ is a subring which is closed under left and right multiplications by elements of $R$, i.e. $a \in I \Rightarrow ra \in I$ and $ar \in I$

14.2 Theorem
Consider $\mathbb{R}[x]$. Let $I = \{p(x) \in \mathbb{R}[x] \mid p(\sqrt{2}) = 0\}$. Then it is an ideal.

14.3 Theorem
Let $R$ be a ring and let $a \subset R$ be a subset. Then there exists a smallest ideal of $R$ which contains $A$.

14.4 Definition Generated Ideals
We call $\cap \mathcal{F}$ the ideal generated by the subset $A$.

14.5 Definition Quotient Rings
Let $R$ be a ring and $I$ be an ideal of $R$. Let $R/I$ denote the partition of the set $R$ by the cosets of $I$, i.e. by $\{r + I \mid r \in R\}$ (needs to be justified). The set is called the quotient set.

On the quotient set, we define $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$. $R/I$ under the above operation is a ring. It is called the quotient ring.

14.6 Definition Ring Homomorphisms
Let $R$ and $S$ be rings, a map $f : R \rightarrow S$ is a ring homomorphism if it satisfies:

\[
f(r_1 + r_2) = f(r_1) + f(r_2) \\
f(r_1 r_2) = f(r_1) f(r_2)
\]

for all $r_1, r_2 \in R$. Between any two rings $R$ and $S$, homomorphisms always exist, eg. $f \equiv 0$ (the trivial homomorphism).

14.7 Theorem
Let $f : R \rightarrow S$ be a ring homomorphism. Then

1. If $R_1$ is a subring of $R$, then $f(R_1) = \{f(r) \mid r \in R_1\}$ is a subring.
2. If $I_1$ is an ideal of $R$, then the image $f(I_1)$ is not necessarily an ideal of $S$.
3. Let $S_1$ be a subring of $S$. Then the pre-image $f^{-1}(S_1) = \{r \in R \mid f(r) \in S_1\}$ is a subring of $R$.
4. If $J_1$ is an ideal of the co-domain $S$, then $f^{-1}(J_1) = \{r \in R \mid f(r) \in J_1\}$ is an ideal of $R$.

14.8 Proposition
If $f : R \rightarrow S$ is a surjective (everything in $S$ is used and tight) ring homomorphism, then the image of an ideal in $R$ is an ideal in $S$. 
14.9 Definition
Let $R$ be a commutative ring, and $I$ is an ideal of $R$.

1. $I$ is **proper** if $I \neq R$ (some books also rule out $\{0\}$)
2. $I$ is **prime** if it is proper and has the property $a, b \in R, ab \in I \Rightarrow a \in I$ or $b \in I$
3. $I$ is **maximal** if there are no ideals $J$ or $R$ which is truly in between $I$ and $R$, i.e. the only ideal $I$ satisfying $I \subset J \subset R$ are $J = I$ or $R$.

14.10 Theorem
Let $R$ be a commutative ring with unity 1. Let $I$ be a proper ideal of $R$. Then

i. $I$ is prime iff $R/I$ is an integral domain.
ii. $I$ is maximal iff $R/I$ is a field.

14.11 Corollary
Maximal ideals are prime.

14.12 Theorem
If $\phi : R \to S$ is a ring homomorphism, if $R$ has a unity and if $\phi$ is surjective, then $\phi(1)$ is the unity of $S$, i.e. $\phi(1) = 1$.

14.13 Theorem
A ring homomorphism $\phi : R \to S$ is injective if and only if Ker $\phi = \{0\}$.

14.14 Corollary
If $F$ is a field and $\phi : F \to S$ is a ring homomorphism, then $\phi$ is either the zero map or it is an embedding of $F$ into $S$.

14.15 Theorem The Fundamental Theorem of Ring Homomorphisms or The First Isomorphism Theorem
Let $\phi : R \to S$ be a ring homomorphism. Then $R/Ker(\phi) \simeq \phi(R)$.

14.16 Definition
Let $F_1$ and $F_2$ be two fields. We say that $F_1$ is an extension of $F_2$ if $F_2 \subset F_1$ as a subfield, or more generally, there exists and embedding $\phi : F_2 \to F_1$. For example, $\mathbb{C}$ is a field extension of $\mathbb{R}$.

14.17 Proposition
If $F_1$ is an extension of $F_2$, and $F_2$ is a extension of $F_3$, then $F_1$ is an extension of $F_3$ (transitive).

14.18 Proposition
Let $F$ be a field. Suppose that char($F$) = 0. Then $F$ is field extension of the field of rationales $\mathbb{Q}$.

14.19 Proposition
Let $F$ be a field, and let the char($F$) = $p$, a finite strictly positive integer. Then $p$ must be a prime. Moreover, the subfield generated by 1 in $F$ is isomorphic to $\mathbb{Z}_p$. Hence $F$ is an extension of $\mathbb{Z}_p$. 
14.20 Theorem
Let $E$ be a field extension of $F$. Then $E$ is a vector space over $F$.

14.21 Theorem (from linear algebra)
Every vector space over a field $F$ has a basis.

14.22 Corollary
Let $E$ be a finite field. Let $\text{char}(E) = p$, where $p$ is prime. So, $E$ is a field extension of $\mathbb{Z}_p$. Let $B$ be a basis for $E$ over $\mathbb{Z}_p$. $B$ must then be finite. If $|B| = n$, then $E \cong \mathbb{Z}^n$ (as vector spaces over $\mathbb{Z}_p$).

14.23 Corollary
No field can be of size 10, as 10 is not prime.

14.24 Claim
For every prime $p$, and positive integer $n$, there exists a field who size is $p^n$. Moreover, any 2 such fields having size $p^n$ are isomorphic.

* * * * * * *