1. ELEMENTARY PROPERTIES

§1.1. Definitions

A ring $R$ is a set on which binary operations of $+$ and $\times$ are defined such that: $(R, +)$ is an abelian group, $(R, \times)$ is a semigroup and $\times$ is distributive over $+$. We write $a \times b$ as $ab$ and powers as $a^n$ in the usual way. A commutative ring also satisfies the Commutative Law: $ab = ba$ for all $a, b \in G$. A ring with 1 satisfies that contains an element $1 \neq 0$ such that $1a = a1 = a$. An integral domain is a commutative ring with 1 such that $ab = 0 \rightarrow a = 0$ or $b = 0$. A division ring is a ring with 1 where for all $a \neq 0$ there exists $a^{-1}$ such that $aa^{-1} = 1 = a^{-1}a$ for all $a \in R$. A field is a commutative division ring.

§1.2. Elementary Properties

Theorem 1: Let $R$ be a ring. Then for all $a, b \in R$:

(i) $a0 = 0 = 0a$;
(ii) $(-a)b = -ab = a(-b)$;
(iii) $(-a)(-b) = ab$.

Proof: (i) $0 + a0 = a0 = a(0 + 0) = a0 + a0$.
(ii) $0 = 0b = [a + (-a)]b = ab + (-a)b$.
(iii) $(-a)(-b) = -a(-b) = ab$.

A non-empty subset $S$ of a ring is a subring if it is closed under $+$, $-$ and $\times$. We use the same notation as for groups: $S \leq R$.

Examples 1:

$\mathbb{Z} \leq \mathbb{Q}$. The set of diagonal matrices is a subring of $M_n(F)$, the ring of $n \times n$ matrices over the field $F$.

A left ideal, $I$, of $R$, is a subring where $a \in R$, $b \in I \rightarrow ab \in I$. A right ideal has $a \in I$, $b \in R \rightarrow ab \in I$. A (2-sided) ideal is one that is both left and right. We use the same notation as for normal subgroups: $I \triangleleft R$.

Examples 2:

(i) $2\mathbb{Z} \triangleleft \mathbb{Z}$

(ii) The set of matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal of $M_2(F)$ but is not a right ideal.

The sum of two subrings $S$ and $T$ of $R$ is $S + T = \{s + t \mid s \in S, t \in T\}$. If $S$, $T$ are 2-sided ideals of $R$ and $S \cap T = 0$ we say that the sum is direct and write it as $S \oplus T$.

If $S, T$ are any two rings, their (external) direct sum is $S \oplus T = \{(s, t) \mid s \in S, t \in T\}$.

If $I$ is a 2-sided ideal of $R$ then $R/I$ is defined to be $\{a + I \mid a \in R\}$, made into a ring under the operations:

$(a + I) + (b + I) = (a + b) + I$;
$(a + I)(b + I) = ab + I$

These are well-defined operations.
If $R$, $S$ are rings a map $\varphi: R \to S$ is a homomorphism if, for all $a, b \in R$:

(i) $(a + b)\varphi = a\varphi + b\varphi;$
(ii) $(ab)\varphi = (a\varphi)(b\varphi)$.

A homomorphism $\varphi$ is an isomorphism if it is 1-1 and onto. If there exists an isomorphism $\varphi: R \to S$ we say that $R$ is isomorphic to $S$, and write $R \cong S$.

In an analogous way to group theory we have the three isomorphism theorems. The kernel of a homomorphism $\varphi: R \to S$ is $\ker \varphi = \{ r \in R \mid r\varphi = 0 \}$.

**Theorem 2 (First Isomorphism Theorem):** If $\varphi: R \to S$ is a hom and $K = \ker \varphi$ then $K \triangleleft R$ and $R/K \cong \im \varphi$.

**Proof:** Define $\Psi: R/\ker \varphi \to \im \varphi$ by $(r + K)\Psi = r\varphi$.

**Theorem 3 (Second Isomorphism Theorem):**
If $S \trianglelefteq R$ and $T \triangleleft R$ then $S \cap T \triangleleft S$ and $(S + T)/T \cong S/(S \cap T)$.

**Proof:** Define the homomorphism $\varphi: S \to ST/T$ by $s\varphi = s + T$ and use the First Isomorphism Theorem.

**Theorem 4 (Third Isomorphism Theorem):**
If $I, J \triangleleft R$ then $J/I \triangleleft R/I$ and $R/J \cong (R/I)/(J/I)$.

**Proof:** Define $\varphi: R/I \to R/J$ by $(r + I)\varphi = r + J$ and use the First Isomorphism Theorem.

If $X, Y$ are subrings of $R$ then $XY = \{ \sum x_iy_i \mid x_i \in X, y_i \in Y \}$. If $X$ is a left ideal so is $XY$. If $Y$ is a right ideal so is $XY$. In particular $R^2 = RR$ is a 2-sided ideal of $R$.

$R$ is a zero ring if $R^2 = 0$, that is, if all products are zero. Every abelian group $G$ can be made into the zero ring $\text{Zero}(G)$ by defining all products to be zero. A ring $R$ is simple if $R^2 \neq 0$ and 0, $R$ are the only 2-sided ideals of $R$. A commutative ring with 1 is simple if and only if it is a field.

**Theorem 5: $M_n(F)$ is simple.**

**Proof:** Suppose $I$ is a non-zero ideal of $M_n(F)$, let $A = (a_{ij})$ be a non-zero element of $I$ and let $a_{ij} \neq 0$. By pre- and post- multiplying by suitable matrices we can make all other components zero. By multiplying by a suitable scalar matrix we can make this non-zero component take any desired value, and by pre- and post- multiplying by suitable permutation matrices we can move this to any position. All these products will remain within $I$. Now, adding such matrices we can thus obtain any $n \times n$ matrix and so $I = M_n(F)$.

If $G$ is a (multiplicative) group, we define the group ring to be the set of all formal linear combinations of the elements of $G$ with addition and multiplication defined in the obvious way. It is denoted by $FG$. So $FG = \{ \sum \lambda_i g_i \mid \lambda_i \in F, g_i \in G \}$. The group elements are a basis for $FG$ and so, if $G$ is finite, $FG$ is finite-dimensional.

A ring $R$ has the descending chain condition (DCC) on right ideals if every descending chain of right ideals has a least. DCC on left ideals and DCC on 2-sided ideals are defined similarly. A ring $R$ has the ascending chain condition (ACC) on right ideals if every ascending chain of right ideals has a greatest. ACC on left ideals and ACC on 2-sided ideals are defined similarly.
§1.3. Some Interesting Examples of Rings

R1 = \text{Zero}(\mathbb{Z}_2^\times) = \text{zero ring on the abelian group} \\
\mathbb{Z}_2^\times = \langle a_0, a_1, a_2, \ldots \mid 2a_0 = 0, 2a_{i+1} = a_i \text{ for each } i \rangle.

R2 = \text{The set of rational numbers of the form } \frac{\text{even}}{\text{odd}}.

R3 = \text{the set row finite matrices over } \mathbb{R}, \text{ that is matrices where the number of rows and columns are countably infinite and where all but a finite number of components in each row are non-zero.}

R4 = \mathbb{Z}_2(x, y) = \text{rational functions, over } \mathbb{Z}_2, \text{ in non-commuting indeterminates } x, y.

R5 = \left\{ \sum_{0 < x < 1} \lambda_x a_x \mid \lambda_x \in \mathbb{R} \right\} \text{ where } a_x a_y = \begin{cases} a_{x+y} & \text{if } x + y < 1 \\ 0 & \text{if } x + y \geq 1 \end{cases}

R6 = \{ax + by \mid a \in \mathbb{Q}\} \text{ where: } x^2 = x, \ xy = y, \ y^2 = 0. \\
\text{The associative law is not obvious. However } (xx)x = x(xx) \text{ simplifies to } x = x, \ (yx)x = y(xx) \text{ simplifies to } y = y, \text{ and all other instances of the associative law involving } x, y \text{ simplify to } 0 = 0. \text{ Another proof of the associative law involves constructing an isomorphic model of } R6 \\
\text{within the ring of } 2 \times 2 \text{ matrices by taking } x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \text{ As well as checking that they satisfy the equations we must also check that they are additively independent.}

R7 = \{ax + by \mid a, b \in \mathbb{Q}\} \text{ where: } x^2 = 0, \ xy = yx = x, \ y^2 = y.$$