Chapter 2. RINGS AND MODULES

§1T. Rings

The next step is to study sets with two operations instead of just one.

(2.1.1) Definition.

- A **ring** is a set R with two operations, **addition** $+: R\times R\to R$ and **multiplication** $\times: R\times R\to R$ (we write $a+b$ instead of $+(a,b)$ and ab or $a\cdot b$ instead of $\times(a,b)$), such that
  a) $(r_1+r_2)+r_3=r_1+(r_2+r_3)$ for all $r_1,r_2,r_3\in R$.
  b) $r_1+r_2=r_2+r_1$ for all $r_1,r_2\in R$.
  c) There exists a **zero** (sometimes called the **additive identity**), $0\in R$, such that $0+r=r$ for all $r\in R$.
  d) For each $r\in R$ there exists an **additive inverse**, $-r\in R$, such that $r+(-r)=0$.
  e) $(r_1r_2)r_3=r_1(r_2r_3)$ for all $r_1,r_2,r_3\in R$.
  f) There exists an **identity** (sometimes called the **multiplicative identity**), $1\in R$, such that $1\cdot r=r\cdot 1=r$ for all $r\in R$.
  g) **Distributive law.** For all $r,s,t\in R$,

$$\begin{aligned} r(s+t)&=rs+rt \quad \text{and}\\ (s+t)r&=sr+tr. \end{aligned}$$

- A **subring** of a ring R is a subset $S\subseteq R$ such that
  a) If $s_1,s_2\in S$ then $s_1+s_2\in S$.
  b) $0\in S$.
  c) If $s\in S$ then $-s\in S$.
  d) If $s_1,s_2\in S$ then $s_1s_2\in S$.
  e) $1\in S$.

- The **zero ring**, (0), is the set containing only 0 with the operations $+$ and $\times$ given by $0+0=0$ and $0\cdot 0=0$ respectively.

Note that a), b), c) and d) in the definition of a ring R mean that R is an abelian group under addition.

The definition of a ring is motivated by the properties of the integers. As a result, knowledge about the integers is an important tool in working with rings.

HW: Show, using Ex. 2.2.5, Part I, that the additive identity $0\in R$ is unique.
HW: Show, using Ex. 2.2.5, Part I, that if $r\in R$ then its additive inverse $-r\in R$ is unique.
HW: Show, using Ex. 2.2.5, Part I, that the identity $1\in R$ is unique.
HW: Show that if $r\in R$ then $0\cdot r=0$ by first showing that $0\cdot r=0\cdot r+0\cdot r$.
HW: Show that if $r\in R$ and $1\in R$ is the identity in R then $(-1)\cdot r=r\cdot(-1)=-r$.

Important examples of rings are:
a) The integers, $\mathbb{Z}$.
b) The $n\times n$ matrices, $M_n(R)$.
c) Polynomial rings, $R[x]$.

Cosets

(2.1.2) Definition.

- An **additive subgroup** of a ring R is a subset $I\subseteq R$ of R such that
  a) If $h_1,h_2\in I$ then $h_1+h_2\in I$.
  b) $0\in I$.
  c) If $h\in I$ then $-h\in I$.

Let R be a ring and let I be an additive subgroup of R. We will use the subgroup I to divide up the ring R.

(2.1.3) Definition.

- A **coset** of I in R is a set $r+I = \{r+i \mid i \in I\}$ where $r \in R$.
- R/I (pronounced "R **mod** I") is the set of cosets of I in R.

(2.1.4) Proposition. *Let R be a ring and let I be an additive subgroup of R. Then the cosets of I in R partition R.*

Notice that the proofs of Proposition 2.1.4 and Proposition 1.1.3 are essentially the same.

HW: Write a very short proof of Proposition 2.1.4 by using Proposition 1.1.3.

Quotient Rings $\leftrightarrow$ Ideals

Let R be a ring and let I be an additive subgroup of R. We can try to make the set R/I of cosets of I into a ring by defining both an addition operation and a multiplication operation on cosets. The only problem is that this doesn't work for the cosets of just any additive subgroup, the subgroup has to have special properties.

HW: Let R be a ring and let I be an additive subgroup of R. Show that I is a normal subgroup of R.

(2.1.5) Definition.

- An **ideal**, I, is a subset of a ring R such that
  a) If $a, b \in I$ then $a+b \in I$.
  b) If $i \in I$ and $r \in R$ then $ir \in R$ and $ri \in R$.
- The **zero ideal**, (0), of R is the ideal containing only the zero element of R.

HW: Show that if I is an ideal of a ring R then $0 \in I$ and if $a \in I$ then $-a \in I$.

HW: Show that an ideal I of a ring R is an additive subgroup of a ring R.

(2.1.6) Proposition. *Let I be an additive subgroup of a ring R. I is an ideal of R if and only if R/I with operations given by*

$$\begin{aligned}(r_1+I)+(r_2+I) &= (r_1+r_2)+I \quad \textit{and} \\ (r_1+I)(r_2+I) &= r_1r_2+I\end{aligned}$$

is a ring.

Notice that the proofs of Proposition 2.1.6 and Proposition 1.1.8 are essentially the same.

HW: Write a shorter proof of Proposition 2.1.6 by using Proposition 1.1.8.

(2.1.7) Definition.

- The **quotient ring**, R/I, is the ring of cosets of an ideal I of a ring R with operations given by $(r_1+I)+(r_2+I) = (r_1+r_2)+I$ and $(r_1+I)(r_2+I) = r_1r_2+I$.

So we have successfully made R/I into a ring when I is an ideal of R.

Homomorphisms

Ring homomorphisms are used to compare rings. Let R and S be rings with identities 1_R and 1_S respectively.

(2.1.8) Definition.

- A **ring homomorphism**, $f: R \to S$, is a mapping between R and S such that
  a) $f(r+s) = f(r)+f(s)$ for all $r, s \in R$.
  b) $f(rs) = f(r)f(s)$ for all $r, s \in R$.
  c) $f(1_R) = 1_S$.
- A **ring isomorphism** is a bijective ring homomorphism.
- Two rings R and S are **isomorphic**, $R \simeq S$, if there exists a ring isomorphism $f: R \to S$ between them.

Two rings are isomorphic if both the elements of the rings and their operations match up exactly. Think of two rings that are isomorphic as being “the same”.

HW: Show that if $1 \in I$, then $I = R$ and $R/I \simeq (0)$.

HW: Give an example of two rings R and S that are isomorphic as groups but not as rings.

In the case of groups, condition b) in the definition of ring homomorphism forced condition c) on us. (See Proposition 1.1.11.) This does not happen here since rings don't necessarily have multiplicative inverses.

(2.1.9) Proposition. *Let $f\colon R \to S$ be a ring homomorphism. Let 0_R and 0_S be the zeros for R and S respectively. Then*

a) $f(0_R) = 0_S$.

b) For any $r \in R$, $f(-r) = -f(r)$.

(2.1.10) Definition.

- The **kernel** of a ring homomorphism $f\colon R \to S$ is the set
$$\ker f = \{r \in R \mid f(r) = 0_S\},$$
where 0_S is the zero in S.
- The **image** of a ring homomorphism $f\colon R \to S$ is the set
$$\operatorname{im} f = \{s \in S \mid f(r) = s \text{ for some } r \in R\}.$$

Note that $\ker f = \{r \in R \mid f(r) = 0_S\}$ not $\{r \in R \mid f(r) = 1_S\}$. If $\ker f$ was $\{r \in R \mid f(r) = 1_S\}$ then $\ker f$ would not necessarily be a subgroup of R (not to mention an ideal) and we couldn't even hope to get homomorphism theorems like we did for groups.

(2.1.11) Proposition. *Let $f\colon R \to S$ be a ring homomorphism. Then*

a) $\ker f$ *is an ideal of* R.

b) $\operatorname{im} f$ *is a subring of* S.

(2.1.12) Proposition. *Let $f\colon R \to S$ be a ring homomorphism. Let 0_R be the zero in R. Then*

a) $\ker f = (0_R)$ *if and only if f is injective.*

b) $\operatorname{im} f = S$ *if and only if f is surjective.*

Notice that the proof of Proposition 2.1.12 b) does not use the fact that $f\colon R \to S$ is a homomorphism, only the fact that $f\colon R \to S$ is a function.

(2.1.13) Theorem.

a) Let $f\colon R \to S$ be a ring homomorphism and let $K = \ker f$. Define

$$\begin{array}{cccc} \hat{f}\colon & R/\ker f & \to & S \\ & r + K & \mapsto & f(r). \end{array}$$

Then $\hat{f}$ is a well defined injective ring homomorphism.

b) Let $f\colon R \to S$ be a ring homomorphism and define

$$\begin{array}{cccc} f'\colon & R & \to & \operatorname{im} f \\ & r & \mapsto & f(r). \end{array}$$

Then f' is a well defined surjective ring homomorphism.

c) If $f\colon R \to S$ is a ring homomorphism, then

$$R/\ker f \simeq \operatorname{im} f$$

where the isomorphism is a ring isomorphism.

Direct Sums

Suppose S and T are rings. The idea is to make $S \times T$ into a ring.

(2.1.14) Definition.

- The **direct sum**, $S \oplus T$, of two rings S and T is the set $S \times T$ with operations given by
$$\begin{aligned}(s_1, t_1) + (s_2, t_2) &= (s_1 + s_2, t_1, t_2) \quad \text{and} \\ (s_1, t_1)(s_2, t_2) &= (s_1 s_2, t_1 t_2)\end{aligned}$$
for all $s_1, s_2 \in S$ and $t_1, t_2 \in T$.
- More generally, given rings $R_1, \ldots, R_n$, the **direct sum** $R_1 \oplus \cdots \oplus R_n$ is the set given by $R_1 \times \cdots \times R_n$ with operations given by
$$\begin{aligned}(s_1, \ldots, s_i, \ldots, s_n) + (t_1, \ldots, t_i, \ldots, t_n) &= (s_1 + t_1, \ldots, s_i + t_i, \ldots, s_n + t_n) \\ (s_1, \ldots, s_i, \ldots, s_n)(t_1, \ldots, t_i, \ldots, t_n) &= (s_1 t_1, \ldots, s_i t_i, \ldots, s_n t_n)\end{aligned}$$
where $s_i, t_i \in R_i$ and $s_i + t_i$ and $s_i t_i$ are given by the operations for the ring R_i. The operations in the direct sum are just the operations from the original rings acting **componentwise**.

HW: Show that these are good definitions, i.e., that, as defined above, $S \oplus T$ and $R_1 \oplus \cdots \oplus R_n$ are rings with zeros given by $(0_S, 0_T)$ and $(0_{R_1}, \ldots, 0_{R_n})$ respectively and identities given by $(1_S, 1_T)$ and $(1_{R_1}, \ldots, 1_{R_n})$ respectively.

Further definitions

There are many things which help to characterize a ring; some of these will be studied in depth in later chapters. Some definitions are given here for reference.

(2.1.15) Definition.

- A ring R is **commutative** if $ab = ba$ for all $a, b \in R$.
- The **center** of a ring R is the set
$$Z(R) = \{a \in R \mid ar = ra \text{ for all } r \in R\}.$$

HW: Give an example of a non-commutative ring.

HW: Prove that $Z(R)$ is a subring of R.

HW: Give an example to show that $Z(R)$ is not necessarily an ideal of R.

HW: What two elements are always in the center of R?

(2.1.16) Definition.

- The **characteristic**, $\operatorname{char}(R)$, of a ring R is the smallest positive integer n such that $1 + 1 + \cdots + 1$ (n times) is 0. If such an integer does not exist, $\operatorname{char}(R)$ is 0.

(2.1.17) Proposition. *Let R be a ring. Let 0_R and 1_R be the zero and the identity in R respectively.*

a) There is a unique ring homomorphism $\varphi\colon \mathbb{Z} \to R$ given by
$$\begin{aligned}\varphi(0) &= 0_R, \\ \varphi(m) &= \underbrace{1_R + \cdots + 1_R}_{m \text{ times}}, \quad \textit{and} \\ \varphi(-m) &= -\varphi(m),\end{aligned}$$
for every $m \in \mathbb{Z}$, $m > 0$.

b) $\ker \varphi = n\,\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ where $n = \operatorname{char}(R)$ is the characteristic of the ring R.

HW: Show that if $\operatorname{char}(R) = 2$ then $1 = -1$ in R.

(2.1.18) Definition.

- A **left inverse** of an element b of a ring R is an element $c \in R$ such that $cb = 1$.
- A **right inverse** of an element b of a ring R is an element $c \in R$ such that $bc = 1$.
- An **inverse** or a **two sided inverse** of an element b of a ring R is an element $c \in R$ such that $cb = bc = 1$.
- A **unit** is an element of a ring that has an inverse.
- If R is a ring, R^* is the **set of units** of R.

HW: Show that if $b \in R$ has both a left inverse and a right inverse then they must be equal.

HW: Give an example of a ring R and an element of R that has a left inverse but not a right inverse.

HW: What element of a ring is always a unit?

HW: Give an example of a ring such that $R^* = R - \{0\}$.

(2.1.19) Definition.

- Let R be a ring and S a subset of R. The **ideal generated by** S is the ideal (S) of R such that
  a) $S \subseteq (S)$.
  b) If T is an ideal of R and $S \subseteq T$ then $(S) \subseteq T$.
- An ideal of a commutative ring is **principal** if it is generated by one element.

(S) is the smallest ideal of R containing S. Think of (S) as gotten by adding to S exactly those elements of R that are needed to make an ideal.

(2.1.20) Definition.

- A **proper ideal** of a ring R is an ideal that is not (0) or R.
- A **maximal ideal** of a ring R is a proper ideal of R that is not contained in any other proper ideal of R.

HW: Show that a proper ideal does not contain any units.

(2.1.21) Proposition. *Every proper ideal I of a ring R is contained in a maximal ideal of R.*

(2.1.22) Definition.

- A **local ring** is a commutative ring with only one maximal ideal.
- A **simple ring** is ring with no proper ideals.
- A ring R is a **division ring** if every nonzero element of R has an inverse in R.
- A **field** is a commutative ring F such that every nonzero element of F has an inverse in F.

Let R be a ring with identity $1 \in R$.

(2.2.1) Definition.

- A **left R-module** is a set M with an addition operation $+: M \times M \to M$ and an action $\times: R \times M \to M$ (we write $m_1 + m_2$ instead of $+(m_1, m_2)$ and rm instead of $\times(r, m)$) such that
  a) $(m_1 + m_2) + m_3 = m_1 + (m_2 + m_3)$ for all $m_1, m_2, m_3 \in M$.
  b) $m_1 + m_2 = m_2 + m_1$ for all $m_1, m_2 \in M$.
  c) There exists a **zero**, $0 \in M$, such that $0 + m = m$ for all $m \in M$.
  d) For each $m \in M$ there exists an **additive inverse**, $-m \in M$, such that $m + (-m) = 0$.
  e) $r_1(r_2 m) = (r_1 r_2)m$ for all $r_1, r_2 \in R$ and $m \in M$.
  f) $1m = m$, for all $m \in M$.
  g) $r(m_1 + m_2) = rm_1 + rm_2$, for all $r \in R$ and $m_1, m_2 \in M$.
  h) $(r_1 + r_2)m = r_1 m + r_2 m$, for all $r_1, r_2 \in R$ and $m \in M$.

- A **submodule** of a left R-module M is a subset $N \subseteq M$ such that
  a) If $n_1, n_2 \in N$ then $n_1 + n_2 \in N$.
  b) $0 \in N$.
  c) If $n \in N$ then $-n \in N$.
  d) If $n \in N$ then $rn \in N$ for all $r \in R$.

- The **zero R-module** or **trivial R-module**, (0), is the set containing only 0 with the operations $+$ and $\times$ given by $0 + 0 = 0$ and $r \cdot 0 = 0$ for all $r \in R$ respectively.

R-modules are the analogues of group actions except for rings.

Note that conditions a), b), c), and d) in the definition of a left R-module imply that every left R-module is an abelian group under addition.

HW: Show, using Ex. 2.2.5, Part I, that the element $0 \in M$ is unique.

HW: Show, using Ex. 2.2.5, Part I, that if $m \in M$ then the element $-m \in M$ is unique.

HW: Show that if M is a left R-module then $0 \cdot m = 0$ for all $m \in M$.

Important examples of modules are:
a) For any ring R, R is a left R-module.
b) All abelian groups are $\mathbb{Z}$-modules.
c) If R is a field then the R-modules are vector spaces.

Cosets

(2.2.2) Definition.

- A **subgroup** of a left R-module M is a subset $N \subseteq M$ such that
  a) If $n_1, n_2 \in N$ then $n_1 + n_2 \in N$.
  b) $0 \in N$.
  c) If $n \in N$ then $-n \in N$.

Let M be a left R-module and let N be a subgroup of M. We will use the subgroup N to divide up the module M.

(2.2.3) Definition.

- A **coset** of N in M is a set $m + N = \{m + n \mid n \in N\}$ where $m \in M$.
- M/N (pronounced "M **mod** N") is the set of cosets of N in M.

(2.2.4) Proposition. *Let M be a left R-module and let N be a subgroup of M. Then the cosets of N in M partition M.*

Notice that the proofs of Proposition 2.2.4 and Proposition 1.1.3 are essentially the same.

HW: Write a very short proof of Proposition 2.2.4 by using Propositon 1.1.3.

Quotient Modules $\leftrightarrow$ Submodules

Let M be a left R-module and let N be a subgroup of M. We can try to make the set M/N of cosets of N in M into an R-module by defining an addition operation and an action of R. This doesn't work with just any subgroup of N, the subgroup must be a submodule.

(2.2.5) Theorem. *Let N be a subgroup of a left R-module M. Then N is a submodule of M if and only if M/N with the operations given by*

$$\begin{aligned}(m_1+N)+(m_2+N)&=(m_1+m_2)+N, \quad \textit{and}\\ r(m_1+N)&=rm_1+N,\end{aligned}$$

is a left R-module.

Notice that the proofs of Proposition 2.2.5 and Proposition 1.1.8 are essentially the same.

HW: Write a shorter proof of Proposition 2.2.5 by using Proposition 1.1.8.

(2.2.6) Definition.

- The **quotient module** M/N is the left R-module of cosets of a submodule N of an R-module M with operations given by $(m_1+N)+(m_2+N)=(m_1+m_2)+N$ and $r(m_1+N)=rm_1+N$.

So we have successfully made M/N into a left R-module when N is a submodule of M.

Homomorphisms

R-module homomorphisms are used to compare R-modules.

(2.2.7) Definition.

- An **R-module homomorphism** is a mapping $f\colon M\to N$ between left R-modules M and N such that
  a) $f(m_1+m_2)=f(m_1)+f(m_2)$ for all $m_1,m_2\in M$.
  b) $f(rm)=rf(m)$ for all $r\in R$ and $m\in M$.
- An **R-module isomorphism** is a bijective R-module homomorphism.
- Two left R-modules M and N are **isomorphic**, $M\simeq N$, if there exists an R-module isomorphism between them.

Note that condition a) in the definition of an R-module homomorphism implies that f is a group homomorphism.

HW: Show that if M and N are left R-modules and if $f\colon M\to N$ is an R-module homomorphism then $f(0_M)=0_N$, where 0_M and 0_N are the zeros in M and N respectively.

HW: Show that if $N=M$ then $M/N\simeq(0)$.

(2.2.8) Definition.

- The **kernel** of an R-module homomorphism $f\colon M\to N$ is the set

  $$\ker f=\{m\in M\mid f(m)=0_N\},$$

  where 0_N is the zero in N.
- The **image** of an R-module homomorphism $f\colon M\to N$ is the set

  $$\operatorname{im} f=\{n\in N\mid f(m)=n \text{ for some } \ m\in M\}.$$

(2.2.9) Proposition. *Let $f\colon M\to N$ be an R-module homomorphism. Then*

a) $\ker f$ *is a submodule of M.*
b) $\operatorname{im} f$ *is a submodule of N.*

(2.2.10) Proposition. *Let $f: M \to N$ be an R-module homomorphism. Let 0_M be the zero in M. Then*

- *a)* $\ker f = (0_M)$ *if and only if f is injective.*
- *b)* $\operatorname{im} f = N$ *if and only if f is surjective.*

Notice that the proof of Proposition 2.2.10 b) does not use the fact that $f: M \to N$ is a homomorphism, only the fact that $f: M \to N$ is a function.

(2.2.11) Theorem.

a) Let $f: M \to N$ be an R-module homomorphism and let $K = \ker f$. Define

$$\begin{array}{rccc} \hat{f}: & M/\ker f & \to & N \\ & m+K & \mapsto & f(m). \end{array}$$

Then $\hat{f}$ is a well defined injective R-module homomorphism.

b) Let $f: M \to N$ be an R-module homomorphism and define

$$\begin{array}{rccc} f': & M & \to & \operatorname{im} f \\ & m & \mapsto & f(m). \end{array}$$

Then f' is a well defined surjective R-module homomorphism.

c) If $f: M \to N$ is an R-module homomorphism, then

$$M/\ker f \simeq \operatorname{im} f$$

where the isomorphism is an R-module isomorphism.

Direct Sums

Suppose M and N are R-modules. The idea is to make $M \times N$ into an R-module.

(2.2.12) Definition.

- The **direct sum**, $M \oplus N$, of two left R-modules M and N is the set $M \times N$ with operations given by

$$\begin{aligned} (m_1, n_1) + (m_2, n_2) &= (m_1 + m_2, n_1 + n_2) \quad \text{and} \\ r(m_1, n_1) &= (rm_1, rn_1) \end{aligned}$$

  for all $m_1, m_2 \in M$, $n_1, n_2 \in N$, and $r \in R$.
- More generally, given left R-modules $M_1, \ldots, M_n$, the **direct sum** $M_1 \oplus \cdots \oplus M_n$ is the set given by $M_1 \times \cdots \times M_n$ with operations given by

$$\begin{aligned} (m_1, \ldots, m_i, \ldots, m_n) + (n_1, \ldots, n_i, \ldots, n_n) &= (m_1 + n_1, \ldots, m_i + n_i, \ldots, m_n + n_n) \quad \text{and} \\ r(m_1, ..., m_i, ..., m_n) &= (rm_1, ..., rm_i, ..., rm_n) \end{aligned}$$

  where $m_i, n_i \in M$ and $m_i + n_i$ and rm_i are given by the operations for the module M_i. The operations on the direct sum are just the operations from the original modules acting **componentwise**.

HW: Show that these are good definitions, i.e., that, as defined above, $M \oplus N$ and $M_1 \oplus \cdots \oplus M_n$ are left R-modules with zeros given by $(0_M, 0_N)$ and $(0_{M_1}, \ldots, 0_{M_N})$ respectively. (0_{M_i} denotes the zero in the left R-module M_i.)

Further Definitions

(2.2.13) Definition.

- Let M be a left R-module and let S be a subset of M. The submodule generated by S is the submodule (S) of M such that
  - a) $S \subseteq (S)$.
  - b) If T is a submodule of M and $S \subseteq T$ then $(S) \subseteq T$.

(S) is the smallest submodule of M containing S. Think of (S) as gotten by adding to S exactly those elements of M that are needed to make a submodule.