CHAPTER R

STRUCTURE AND ACTION: ALGEBRAS AND MODULES

The standard abstract algebra course presents the basic properties of groups, rings, and fields. The motivation is to study the properties of the number systems that we use, some of these being:

(a) the positive integers, $\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$,
(b) the integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
(c) the rational numbers, $\mathbb{Q} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}_{>0}\right\}$,
(d) the real numbers, $\mathbb{R}$,

with the operations of addition and multiplication. We need to find exactly what properties these structures have and what the implications of these properties are.

R.1. Rings=$\mathbb{Z}$-algebras

We start by identifying the key properties of the integers $\mathbb{Z}$, as a number system. *The terms "$\mathbb{Z}$-algebra" and "ring" are synonyms, they mean exactly the same thing.*

Definition R.1.1. —

- A **$\mathbb{Z}$-algebra**, or **ring**, is a set A with two operations, **addition** $+\colon A \times A \to A$ and **multiplication** $\times\colon A \times A \to A$ $\big($write $a+b$ instead of $+(a,b)$ and ab or $a \cdot b$ instead of $\times(a,b)\big)$, such that
  (a) If $r_1, r_2, r_3 \in A$ then $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$,
  (b) If $r_1, r_2 \in A$ then $r_1 + r_2 = r_2 + r_1$,
  (c) There exists a **zero** (sometimes called the **additive identity**), $0 \in A$, such that if $r \in A$ then $0 + r = r$,
  (d) If $r \in A$ then there exists an **additive inverse**, $-r \in A$, such that $r + (-r) = 0$,
  (e) If $r_1, r_2, r_3 \in A$ then $(r_1 r_2) r_3 = r_1 (r_2 r_3)$,
  (f) There exists an **identity** (sometimes called the **multiplicative identity**), $1 \in A$, such that if $r \in A$ then $1 \cdot r = r \cdot 1 = r$,
  (g) **Distributive law.** If $r, s, t \in A$ then
  $$r(s+t) = rs + rt \qquad \text{and} \qquad (s+t)r = sr + tr.$$
- A **subalgebra**, or **subring**, of a $\mathbb{Z}$-algebra A is a subset $S \subseteq A$ 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 $s_1 s_2 \in S$.
  (e) $1 \in S$.

Notes of Arun Ram aram@unimelb.edu.au, Version: 8 April 2020

- The **zero $\mathbb{Z}$-algebra**, or **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.

The properties (a), (b), (c) and (d) in the definition of a $\mathbb{Z}$-algebra A mean that A is an abelian group under addition.

The definition of a ring, or $\mathbb{Z}$-algebra, is motivated by the properties of the integers. As a result, knowledge about the integers is an important tool in working with $\mathbb{Z}$-algebra.

HW: Show that the additive identity $0\in A$ is unique.
HW: Show that if $r\in A$ then its additive inverse $-r\in A$ is unique.
HW: Show that the identity $1\in A$ is unique.
HW: Show that if $r\in A$ then $0\cdot r=0$ by first showing that $0\cdot r=0\cdot r+0\cdot r$.
HW: Show that if $r\in A$ and $1\in A$ is the identity in A then $(-1)\cdot r=r\cdot(-1)=-r$.

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

Ring homomorphisms are used to compare rings. A ring homomorphism must preserve the structures that distinguish a ring: the addition, the multiplication and the multiplicative identity (the additive identity and the additive inverse come "for free", see Proposition R.1.1).

Definition R.1.2. — Let R and A be $\mathbb{Z}$-algebras with identities 1_R and 1_A respectively.

ring homo

- A **$\mathbb{Z}$-algebra homomorphism**, of **ring homomorphism**, is a function $f\colon R\to A$ such that
  (a) If $r_1,r_2\in R$ then $f(r_1+r_2)=f(r_1)+f(r_2)$,
  (b) If $r_1,r_2\in R$ then $f(r_1r_2)=f(r_1)f(r_2)$,
  (c) $f(1_R)=1_A$.
- A **ring isomorphism**, or **$\mathbb{Z}$-algebra isomorphism**, is a ring homomorphism $f\colon R\to A$ such that the inverse function $f^{-1}\colon A\to R$ exists and f^{-1} is a ring homomorphism.
- Two $\mathbb{Z}$-algebras R and A are **isomorphic**, $R\simeq A$, if there exists a ring isomorphism $f\colon R\to A$ between them.

Two rings are isomorphic if both the elements of the rings and their operations match up exactly. Think of two $\mathbb{Z}$-algebras that are isomorphic as being "the same".

HW: Show that $f\colon R\to A$ is a ring isomorphism if and only if $f\colon R\to A$ is a bijective ring homomorphism.
HW: Give an example of two $\mathbb{Z}$-algebras R and A that are isomorphic as groups but not as $\mathbb{Z}$-algebras.

In the case of groups, condition (b) in the definition of ring homomorphism forced condition (c) on us (see Proposition G.1.1). This does not happen here since rings don't necessarily have multiplicative inverses.

Proposition R.1.1. — *Let $f\colon R\to A$ be a $\mathbb{Z}$-algebra homomorphism. Let 0_R and 0_A be the zeros for R and A respectively. Then* *(a)* $f(0_R) = 0_A$,

(b) If $r \in R$ *then* $f(-r) = -f(r)$.

R.1.1. Cosets. —

Definition R.1.3. —

- 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 A be a $\mathbb{Z}$-algebra and let I be an additive subgroup of A. We will use the subgroup I to divide up the $\mathbb{Z}$-algebra A.

Definition R.1.4. —

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

Proposition R.1.2. — *Let A be a $\mathbb{Z}$-algebra and let I be an additive subgroup of A. Then the cosets of I in A partition A.*

Notice the analogy between Proposition R.1.2 and Proposition F.2.2 and Proposition R.2.2 and Proposition G.1.2.

R.1.2. Quotient Rings ↔ Ideals. — Let A be a $\mathbb{Z}$-algebra and let I be an additive subgroup of A. We can try to make the set A/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 A be a ring and let I be an additive subgroup of A. Show that I is a normal subgroup of A.

Definition R.1.5. —

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

HW: Show that if I is an ideal of a $\mathbb{Z}$-algebra A 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.

Proposition R.1.3. — *Let I be an additive subgroup of a $\mathbb{Z}$-algebra R. I is an ideal of R if and only if R/I with operations given by*

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \qquad \textit{and} \qquad (r_1 + I)(r_2 + I) = r_1 r_2 + I$$

is a ring.

Notice the analogy between Theorem F.2.3, Theorem R.2.3, Theorem R.1.3 and Theorem G.1.5.

Definition R.1.6. —

- The **quotient $\mathbb{Z}$-algebra**, A/I, is the $\mathbb{Z}$-algebra of cosets of an ideal I of a $\mathbb{Z}$-algebra A 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 A/I into a ring when I is an ideal of A.

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

R.1.3. Kernel and image of ring homomorphism. —

Definition R.1.7. —

- The **kernel** of a $\mathbb{Z}$-algebra homomorphism $f\colon R \to A$ is the set
$$\ker f = \{r \in R \mid f(r) = 0_A\},$$
where 0_A is the zero in A.
- The **image** of a ring homomorphism $f\colon R \to A$ is the set
$$\mathrm{im} f = \{f(r) \mid r \in R\}.$$

Note that $\ker f = \{r \in R \mid f(r) = 0_A\}$ *not* $\{r \in R \mid f(r) = 1_A\}$. If $\ker f$ was $\{r \in R \mid f(r) = 1_A\}$ 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 those for groups.

Proposition R.1.4. — *Let $f\colon R \to A$ be a ring homomorphism. Then*

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

(b) $\mathrm{im} f$ *is a subring of* A.

Proposition R.1.5. — *Let $f\colon R \to A$ be a $\mathbb{Z}$-algebra homomorphism. Let 0_R be the zero in R. Then*

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

(b) $\mathrm{im}\, f = A$ *if and only if f is surjective.*

Notice that the proof of Proposition R.1.5(b) does not use the fact that $f\colon R \to A$ is a homomorphism, only the fact that $f\colon R \to A$ is a function.

Theorem R.1.6. —

(a) Let $f\colon R \to A$ be a ring homomorphism and let $K = \ker f$. Define
$$\begin{array}{rccc} \hat{f}\colon & R/\ker f & \to & A \\ & r+K & \mapsto & f(r). \end{array}$$
Then $\hat{f}$ is a well defined injective $\mathbb{Z}$-algebra homomorphism.

(b) Let $f\colon R \to A$ be a $\mathbb{Z}$-algebra homomorphism and define
$$\begin{array}{rccc} f'\colon & R & \to & \mathrm{im} f \\ & r & \mapsto & f(r). \end{array}$$
Then f' is a well defined surjective ring homomorphism.

(c) If $f\colon R \to A$ is a ring homomorphism, then
$$R/\ker f \simeq \mathrm{im} f$$
where the isomorphism is a $\mathbb{Z}$-algebra isomorphism.

R.1.4. Direct Sums. — Suppose S and T are $\mathbb{Z}$-algebra. The idea is to make $S \times T$ into a $\mathbb{Z}$-algebra.

Definition R.1.8. —

- The **direct sum** $S \oplus T$ of two rings S and T is the set $S \times T$ with operations given by
$$(s_1, t_1) + (s_2, t_2) = (s_1 + s_2, t_1, t_2) \qquad \text{and} \qquad (s_1, t_1)(s_2, t_2) = (s_1 s_2, t_1 t_2),$$
for $s_1, s_2 \in S$ and $t_1, t_2 \in T$.
- More generally, given $\mathbb{Z}$-algebras $R_1, \ldots, R_n$, the **direct sum** $R_1 \oplus \cdots \oplus R_n$ is the set $R_1 \times \cdots \times R_n$ with operations given by
$$(s_1, \ldots, s_i, \ldots, s_n) + (t_1, \ldots, t_i, \ldots, t_n) = (s_1 + t_1, \ldots, s_i + t_i, \ldots, s_n + t_n) \qquad \text{and}$$
$$(s_1, \ldots, s_i, \ldots, s_n)(t_1, \ldots, t_i, \ldots, t_n) = (s_1 t_1, \ldots, s_i t_i, \ldots, s_n t_n),$$
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 is just the operations from the original $\mathbb{Z}$-algebras 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 $\mathbb{Z}$-algebras 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.

R.1.5. Further definitions. — There are many things which help to characterize a ring. Some definitions are given here for reference.

Definition R.1.9. —

- A **commutative $\mathbb{Z}$-algebra** is a ring R such that if $a, b \in R$ then $ab = ba$.
- The **center** of a $\mathbb{Z}$-algebra R is the set
$$Z(R) = \{z \in R \mid \text{if } r \in R \text{ then } zr = rz\}.$$

HW: Give an example of a non-commutative $\mathbb{Z}$-algebra.

HW: Prove that $Z(R)$ is a $\mathbb{Z}$-subalgebra 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?

Definition R.1.10. —

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

Proposition R.1.7. — *Let R be a $\mathbb{Z}$-algebra. Let 0_R and 1_R be the zero and the identity in R respectively.*

(a) There is a unique $\mathbb{Z}$*-algebra 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 $m \in \mathbb{Z}_{>0}$*.*

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

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

Definition R.1.11. —

- A **left inverse** of an element b of a $\mathbb{Z}$-algebra R is an element $c \in R$ such that $cb = 1$.
- A **right inverse** of an element b of a $\mathbb{Z}$-algebra R is an element $c \in R$ such that $bc = 1$.
- An **inverse** or a **two sided inverse** of an element b of a $\mathbb{Z}$-algebra R is an element $c \in R$ such that $cb = bc = 1$.
- A **unit** is an element of a $\mathbb{Z}$-algebra that has an inverse.
- If R is a $\mathbb{Z}$-algebra, $R^\times$ 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 A and an element of A that has a left inverse but not a right inverse. PUT IN PASSMAN'S LITTLE EXAMPLE.

HW: What element of a $\mathbb{Z}$-algebra is always a unit?

HW: Prove that if R is a ring then $R^\times$ is a group (under multiplication).

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

HW: Give an example of a $\mathbb{Z}$-algebra such that $R^\times \neq R - \{0\}$.

Definition R.1.12. —

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

The ideal $\langle S \rangle$ is the smallest ideal of R containing S. Think of $\langle S \rangle$ as gotten by adding to S exactly those elements of R that are needed to make an ideal.

Definition R.1.13. —

- A **proper ideal** of a $\mathbb{Z}$-algebra A is an ideal that is not (0) or A.
- A **maximal ideal** of a ring A is a proper ideal of A that is not contained in any other proper ideal of A.

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

Proposition R.1.8. — *Every proper ideal I of a $\mathbb{Z}$-algebra A is contained in a maximal ideal of A.*

Definition R.1.14. —

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

HW: Show that a commutative division algebra is a field.

HW: Let R be a $\mathbb{Z}$-algebra and let I be an ideal of R. Show that I is a maximal ideal if and only if R/I is a division algebra.

HW: Show that $\mathbb{Q}[x]$ is a local ring.

HW: Show that $\mathbb{Z}$ is not a local ring.

HW: Show that the quaternions $\mathbb{H}$ is a division algebra that is not a field.

HW: Let $\mathbb{F}$ be a field and let $n \in \mathbb{Z}_{>0}$. Show that the $\mathbb{Z}$-algebra $M_n(\mathbb{F})$ of $n \times n$ matrices with entries in $\mathbb{F}$ is a simple $\mathbb{Z}$-algebra.

HW: Show that $\mathbb{Z}$ is not a simple $\mathbb{Z}$-algebra.