Math 521A

3.2 – Basic Properties of Rings

Theorem (Uniqueness of the additive identity)

Given a ring R, the element 0_R (additive identity) is unique.

The proof is on the board.

Theorem (Uniqueness of the inverse)

Let R be a ring. Suppose $a, b, c \in R$ satisfy

$$\begin{cases} a+b = b+a = 0_R. \\ a+c = c+a = 0_R. \end{cases}$$

Then $b = c$.

The latter theorem means that the equation $x + a = 0_R$ has a unique solution, denoted by $-a$. Note that

$$a + (-a) = (-a) + a = 0_R.$$

Subtraction in a ring is then defined as $b - a = b + (-a)$.

Theorem

If $a + b = a + c$ in a ring R, then $b = c$.

Theorem

For all $a, b \in R$,

1. $a \cdot 0 = 0 = 0 \cdot a$.
2. $a(-b) = -ab = (-a)b$.
3. $-(-a) = a$.
4. $-(a + b) = (-a) + (-b)$.
5. $-(a - b) = -a + b$.
6. $(-a)(-b) = ab$.
7. *If $1 \in R$ then $(-1)a = -a$.*

The proofs of some of the above properties are on the board.

Remarks:

- If a ring R has a unity 1_R, then it is unique (assume R has another unity $1'_R$ and then show that $1'_R = 1_R$). "Unity" is another name for multiplicative identity; do not confuse it with "unit."
- Suppose S is a subring of R. Then:
  (a) $0_S = 0_R$, but
  (b) 1_R does not necessarily have to be equal to 1_S. For example, consider $R = \mathbb{Z}_{10}$, $S = \{0, 2, 4, 6, 8\}$ and check that $1_S = 6$.

Theorem

Let R be a ring and $S \subseteq R$. If

(i) $S \neq \emptyset$;

(ii) $x \in S, y \in S \Longrightarrow x - y \in S$ *and* $xy \in S$,

then S is a subring of R.

The proof of the theorem is on the board.

Notation: For $n > 0$, define $a^n = \underbrace{a \cdot a \cdots a}_{n \text{ copies}}$.

For $n \in \mathbb{Z}, n > 0$: $n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ copies}}$.

For $n \in \mathbb{Z}, n < 0$: $n \cdot a = \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n \text{ copies}}$.

Thus, if we let a and b be elements of a ring R, then:

$$\begin{aligned}
(a+b)^2 &= (a+b)\cdot(a+b) = a(a+b) + b(a+b) \\
&= a^2 + ab + ba + b^2. \\
(a-b)^2 &= (a+(-b))(a+(-b)) \\
&= a(a+(-b)) + (-b)(a+(-b)) \\
&= a^2 - ab - ba + b^2.
\end{aligned}$$

Definition

Let R be a ring with unity 1_R. Then $a \in R$ is called a unit if $\exists\, u \in R$ such that $au = ua = 1_R$.

Remark: It is possible to show that the element u (in the above definition) is unique. It is called the multiplicative inverse of a and is denoted a^{-1}.

Units in $\mathbb{Z} = \{-1, 1\}$; Units in $\mathbb{Q} = \mathbb{Q} \setminus \{0\}$;
Units in $M_n(\mathbb{R}) = \{\text{invertible matrices}\}$;
Units in $\mathbb{Z}_3 = \{1, 2\}$; Units in $\mathbb{Z}_6 = \{1, 5\}$.

Recall from Chapter 2: $(a, n) = 1$ if and only if $ax = 1$ has a solution in $\mathbb{Z}_n$. Thus, units in $\mathbb{Z}_n = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$.

Theorem

Let $a \in R$ be a unit. Then $ax = b$ has a unique solution in R.

Definition

An nonzero element a in a ring R is called a zero divisor if $\exists\, c \in R$, $c \neq 0_R$, such that $ac = 0_R$ or $ca = 0_R$.

In $\mathbb{Z}_{10}$, $2, 4, 5, 6, 8$ are all zero divisors. Note that it is possible that $ac = 0_R$ but $ca \neq 0_R$. Consider for example,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \text{ However,}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Remarks:

- A zero divisor is never a unit; a unit is never a zero divisor;
- It is possible that an element in a ring is neither a unit nor a zero divisor. For example, $2 \in \mathbb{Z}$.

The proofs of the next results are on the board:

Theorem

Every field is an integral domain.

Theorem

Let R be an integral domain and let $a \neq 0$ be an element of R. Then $ab = ac \Rightarrow b = c$.

Theorem

Every finite integral domain is a field.

Some additional properties:

1. Let S, T be subrings of a ring R. Then:
   (a) $S \cap T$ is a subring of R;
   (b) $S \cup T$ may not be a subring of R. For example, let $R = \mathbb{Z}_{12}, S = \{0, 3, 6, 9\}, T = \{0, 4, 8\}$.

2. The center C of a ring R is defined as

$$C := \{a \in R \mid ra = ar \ \forall\, r \in R\}.$$

   For example, let $M_n(\mathbb{R})$ denote the ring of all $n \times n$ matrices with entries in $\mathbb{R}$. The operations $+$ and $\cdot$ are the usual matrix addition and multiplication. If $R = M_n(\mathbb{R})$, then $C = \{k \cdot I_n \mid k \in \mathbb{R}\}$ and $I_n = n \times n$ identity matrix.

3. Suppose a, b are units in a ring R. Then $(ab)^{-1} = b^{-1}a^{-1}$.