Chapter 9. Definition and Examples of Rings and Subrings

9.1 Definition: A **ring** is a set R with two binary operations, addition denoted by $+$ and multiplication denoted by $\times$, by $\cdot$ or by concatenation, and an element $0 \in R$ such that

(1) $+$ is associative: $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$,
(2) $+$ is commutative: $a+b = b+a$ for all $a,b,c \in R$,
(3) 0 is an additive identity: $a+0 = 0+a = a$ for all $a \in R$,
(4) every $a \in R$ has an additive inverse: there exists $b \in R$ such that $a+b = b+a = 0$,
(5) $\times$ is associative: $(ab)c = a(bc)$ for all $a,b,c \in R$, and
(6) $\times$ is distributive over $+$: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a,b,c \in R$.

We say that R is **commutative** when $\times$ is commutative, that is $ab = ba$ for all $a,b \in R$. We say that R has an **identity** (or that R has a 1) when it has a multiplicative identity, that is when there is a non-zero element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. When R has a 1, for $a \in R$ we say that a is **invertible** (or that a is a **unit**) when there is an element $b \in R$ with $ab = 1 = ba$. A **division ring** is a ring R with identity such that every non-zero element of R is invertible. A **field** is a commutative division ring.

9.2 Theorem: (*Uniqueness of Identity and Inverse*) *Let R be a ring. Then*

(1) the additive identity 0 is unique in the sense that if $e \in R$ has the property that $a+e = a = e+a$ for all $a \in R$ then $e = 0$,
(2) the additive inverse of $a \in G$ is unique in the sense that for all $a,b,c \in G$ if we have $a+b = 0 = b+a$ and $a+c = 0 = c+a$ then $b = c$,
(3) if R has a 1, then it is unique in the sense that for all $u \in R$, if u has the property that $au = a = ua$ for all $a \in G$ then $u = 1$, and
(4) if R has a 1 and $a \in R$ has an inverse, then it is unique in the sense that for all $a \in G$ if there exist $b,c \in G$ such that $ab = ba = 1$ and $ac = ca = 1$ then $b = c$.

9.3 Notation: Let R be a ring. For $a \in R$ we denote the unique additive inverse of $a \in R$ by $-a$, and for $a,b \in R$ we write $b-a$ for $b+(-a)$. If R has a 1 and $a \in R$ has a multiplicative inverse, we say that a is a **unit** in R, and we denote its inverse by a^{-1}.

9.4 Theorem: (*Cancellation Under Addition*) *Let R be a ring. Then for all $a,b,c \in R$,*

(1) if $a+c = b+c$ then $a = c$,
(2) if $a+b = a$ then $b = 0$, and
(3) if $a+b = 0$ then $b = -a$.

9.5 Note: We do not, in general, have similar rules for cancellation under multiplication. In general, for a,b,c in a ring R, $ac = bc$ does not imply that $a = b$, $ac = a$ does not imply that $c = 1$, $ac = 1$ does not imply that $ca = 1$, and $ac = 0$ does not imply that $a = 0$ or $b = 0$. When $ac = 1$ we say that a is a **left inverse** for c and that c is a **right inverse** for a. When $ac = 0$ but $a \neq 0$ and $b \neq 0$, we say that a and b are **zero divisors**. A commutative ring with 1 which has no zero divisors is called an **integral domain**.

9.6 Theorem: (*Cancellation Under Multiplication*) *Let R be a ring. For all $a,b,c \in R$, if $ac = bc$, or if $ca = cb$, then either $a = b$ or $c = 0$ or c is a zero divisor.*

Proof: Suppose $ac = bc$. Then $ac - bc = 0$ so $(a-b)c = 0$. Either $(a-b) = 0$ so $a = b$, or $c = 0$ or $(a-b)$ and c are zero divisors. The case that $ca = cb$ is similar.

9.7 Theorem: (*Basic Properties of Rings*) *Let R be a ring. Then*
(1) $0 \cdot a = a \cdot 0 = 0$ *for all* $a \in R$,
(2) $(-a)b = -(ab) = a(-b)$ *for all* $a, b \in R$,
(3) $(-a)(-b) = ab$ *for all* $a, b \in R$,
(4) if R *has a 1 then* $(-1)a = -a$ *for all* $a \in R$.

Proof: Let $a \in R$. Then $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Thus $0 \cdot a = 0$ by additive cancellation. The proof that $a \cdot 0 = 0$ is similar, and the other proofs are left as an exercise.

9.8 Notation: Let R be a ring. For $k \in \mathbb{Z}^+$ we write $ka = a + a + \cdots + a$ with k terms in the sum, and we write $(-k)a = k(-a)$, and we write $a^k = a \cdot a \cdot \ldots \cdot a$ with k terms in the product. For $0 \in \mathbb{Z}$ we write $0a = 0$ and if R has a 1 we write $a^0 = 1$. If R has a 1 and $a \in R$ is a unit, we write $a^{-k} = (a^{-1})^k$. For all $k, l \in \mathbb{Z}$ and all $a \in R$ we have $(k + l)a = ka + la$, $(-k)a = -(ka) = k(-a)$, $-(-a) = a$, $-(a + b) = -a - b$, $(ka)(lb) = (kl)(ab)$. For $a \in R$ and $k, l \in \mathbb{Z}^+$ we have $a^{k+l} = a^k a^l$. When R has a 1 and a and b are units, then for $k, l \in \mathbb{Z}$ we have $a^{k+l} = a^k a^l$, $a^{-k} = (a^k)^{-1}$, $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.

9.9 Example: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_n$ are all commutative rings with 1. Of these, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, and also $\mathbb{Z}_p$ when p is prime, are fields.

9.10 Example: The ring of real **quaternions** is the set $\mathbf{H} = \mathbb{R}^4$ in which we write $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$, $k = (0, 0, 0, 1)$ and for $t \in \mathbb{R}$ we write $t = (t, 0, 0, 0)$, $ti = it = (0, t, 0, 0)$, $tj = jt = (0, 0, t, 0)$ and $tk = kt = (0, 0, 0, t)$. We define addition as usual in $\mathbf{H} = \mathbb{R}^4$. and we define multiplication by requiring that $i^2 = j^2 = k^2 = -1$, that $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$, and that every real number commutes with i, j and k. It can be verified that $\mathbf{H}$ is a division ring with

$$(a + ib + jc + kd)^{-1} = \frac{a - ib - jc - kd}{a^2 + b^2 + c^2 + d^2}$$

for all $0 \neq a + ib + jc + kd \in \mathbf{H}$.

9.11 Example: For a set A and a ring R, the set

$$\mathrm{Func}(A, R) = R^A = \big\{\text{fuctions } f : A \to R\big\}$$

is a ring under the operations given by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in A$. If R is commutative then so is $\mathrm{Func}(A, R)$. If R has identity 1 then the identity of $\mathrm{Func}(A, R)$ is the constant function $1 : A \to R$ given by $1(x) = 1$ for all $x \in A$.

9.12 Example: For a group G, an **endomorphism** of G is a group homomorphism $\phi : G \to G$. If G is an additive abelian group then the set

$$\mathrm{End}(G) = \big\{\text{endomorphisms } \phi : G \to G\big\}$$

is a ring under the operations given by $(\phi + \psi)(x) = \phi(x) + \psi(x)$ and $(\phi\psi)(x) = \phi\big(\psi(x)\big)$ for all $x \in G$. The ring $\mathrm{End}(G)$ has an identity, namely the identity function $I : G \to G$ given by $I(x) = x$ for all $x \in G$.

9.13 Example: Let R be a ring with 1. Then the set

$$R^* = \big\{a \in R \big|\ a \text{ is a unit}\big\}$$

is a group under multiplication, called the **group of units** of R.

9.14 Example: For a ring R and a variable symbol x, a **formal power series** in x over R is a sequence $(a_0, a_1, a_2, \cdots)$ with each $a_i \in R$, and we write this sequence as

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots .$$

The elements a_i are called the **coefficients** of f and a_0 is called the **constant coefficient**. A power series of the form $f(x) = a$ with $a \in R$ is called a **constant series**. The set

$$R[[x]] = \{\text{formal power series in } x \text{ over } R\}$$

is a ring, which we call the **ring of formal power series** in x over R, with the following operations: for $f(x) = \sum\limits_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum\limits_{j=0}^{\infty} b_j x^j$ we have

$$(f+g)(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^i \text{ , and } (fg)(x) = \sum_{k=0}^{\infty} c_k x^k \text{ where } c_k = \sum_{i=0}^{k} a_i b_{k-i} .$$

If R is commutative then so is $R[[x]]$, and if R has identity 1 then the identity of $R[[x]]$ is the constant polynomial 1, that is the sequence $1 = (1, 0, 0, \cdots)$. A **polynomial** in x over R is a formal power series with only finitely non-zero coefficients. When we have $a_i = 0$ for all $i > n$ we also write $f(x) = \sum\limits_{i=0}^{n} a_i x^i$. When $a_n \neq 0$ and $a_i = 0$ for all $i > n$ we say that a_n is the **leading coefficient** of f and that the **degree** of f is $\deg(f) = n$. The set

$$R[x] = \{\text{polynomials in } x \text{ over } R\}$$

is a ring, which we call the **ring of polynomials** in x over R, using the same operations as in $R[[x]]$.

9.15 Example: For a ring R and variable symbols $x_1, \cdots, x_n$, a **formal power series** in $x_1, \cdots, x_n$ over R is a function $a : \mathbb{N}^n \to R$, and we write this function as

$$f(x_1, \cdots, x_n) = \sum_{(i_1, \cdots, i_n) \in \mathbb{N}^n} a_{i_1, \cdots, i_n} {x_1}^{i_1} \cdots {x_n}^{i_n} \text{ where } a_{i_1, \cdots, i_n} = a(i_1, \cdots, i_n) .$$

The elements $a_{i_1, \cdots, i_n} \in R$ are called the **coefficients** of the power series. The set

$$R[[x_1, \cdots, x_n]] = \{\text{formal power series in } x_1, \cdots, x_n \text{ over } R\}$$

is a ring, called the **ring of formal power series** in $x_1, \cdots, x_n$ over R, under the following operations: for $f(x) = \sum a_{i_1, \cdots, i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}$ and $g(x) = \sum b_{j_1, \cdots, j_n} {x_1}^{j_1} \cdots {x_n}^{j_n}$ we define

$$(f+g)(x) = \sum (a_{k_1, \cdots, k_n} + b_{k_1, \cdots, k_n}) {x_1}^{k_1} \cdots {x_n}^{k_n}$$
$$(fg)(x) = \sum c_{k_1, \cdots, k_n} {x_1}^{k_1} \cdots {x_n}^{k_n}$$

where $c_{k_1, \cdots, k_n}$ is the sum of all terms $a_{i_1, \cdots, i_n} b_{j_1, \cdots, j_n}$ for which $i_\alpha + j_\alpha = k_\alpha$ for all $\alpha = 1, \cdots, n$. A **polynomial** in $x_1, \cdots, x_n$ over R is a formal power series with only finitely many non-zero coefficients, and the set

$$R[x_1, x_2, \cdots, x_n] = \{\text{polynomials in } x_1, \cdots, x_n \text{ over } R\}$$

is a ring using the same operations as in $R[[x_1, \cdots, x_n]]$.

9.16 Example: For a ring R, the set

$$M_n(R) = \{n \times n \text{ matrices with entries in } R\}$$

is a ring under matrix addition and matrix multiplication, which we call the **ring of** $n \times n$ **matrices over** R. If R has identity 1 then the identity of $M_n(R)$ is the $n \times n$ identity matrix I.

9.17 Example: If R and S are rings then the cartesian product

$$R \times S = \{(a,b) \big| a \in R, b \in S\}$$

is a ring, called the **product ring** of R and S, with operations

$$(a,b) + (c,d) = (a+c, b+d) \text{ and } (a,b)(c,d) = (ac, bd)\,.$$

More generally, if $R_1, \cdots, R_n$ are rings then so is the product

$$\prod_{i=1}^{n} R_i = R_1 \times \cdots \times R_n = \{(a_1, \cdots, a_n) \big| \text{each } a_i \in R_i\}\,,$$

which we call the **product ring** of $R_1, \cdots, R_n$, under the operations

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) = \big(a_1 + b_1, \cdots, a_n + b_n\big)\ \text{, and}$$
$$(a_1, \cdots, a_n)(b_1, \cdots, b_n) = \big(a_1, b_1, \cdots, a_n b_n\big)\,.$$

More generally still, if A is any set and R_α is a ring for each $\alpha \in A$, then the product

$$\prod_{\alpha \in A} R_\alpha = \{f : A \to \bigcup_{\alpha \in A} R_\alpha \big| f(\alpha) \in R_\alpha \text{ for all } \alpha \in A\}$$

is a ring, called the **product ring** of the rings $R_\alpha, \alpha \in A$, under the operations

$$(f+g)(\alpha) = f(\alpha) + g(\alpha) \text{ and } (fg)(\alpha) = f(\alpha)g(\alpha).$$

9.18 Theorem: *Let R be a finite ring. Then R is a field if and only if R is an integral domain.*

Proof: Suppose that R is a field. Let $a, b \in R$. Suppose that $ab = 0$ and $a \neq 0$. Then $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Thus R has no zero divisors.

Conversely, suppose that R is an integral domain. We must show that every non-zero element in R is a unit. Let $0 \neq a \in R$. Consider the left multiplication map $L_a : R \to R$ given by $L_a(x) = ax$. For $x, y \in R$ we have $L_a(x) = L_a(y) \Longrightarrow ax = ay \Longrightarrow x = y$ by cancellation, since $a \neq 0$ and a is not a zero divisor. Thus L_a is injective. Since R is finite, this implies that L_a is bijective. In particular, we can choose $b \in R$ so that $L_a(b) = 1$, that is $ab = 1$. Similarly, right multiplication R_a is bijective, and so we can choose $c \in R$ so that $ca = 1$. Then we have $c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$, and so a is a unit with $a^{-1} = b = c$.

9.19 Definition: Let R be a ring with 1. We define the **characteristic** of R, written as $\text{char}(R)$, to be the smallest $n \in \mathbb{Z}^+$ such that $n \cdot 1 = 0$ if such an n exists, and if no such n exists then the characteristic of R is 0. Note that when $n \cdot 1 = 0$ we have $n \cdot a = 0$ for all $a \in R$ because $n\,a = a + a + \cdots + a = (1 + 1 + \cdots 1)a = (n \cdot 1)\,a$.

9.20 Theorem: *Let R be a ring with 1 with no zero divisors. Then either* $\mathrm{char}(R) = 0$ *or* $\mathrm{char}(R)$ *is prime.*

Proof: Suppose $\mathrm{char}(R) = n \in \mathbb{Z}^+$. Suppose, for a contradiction, that n is composite, say $n = kl$ with $1 < k, l < n$. Then $0 = n \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1)$. Since R has no zero divisors, either $k \cdot 1 = 0$ or $l \cdot 1 = 0$. This contradicts the definition of $n = \mathrm{char}(R)$.

9.21 Definition: A **subring** of a ring R is a subset $S \subseteq R$ which is a ring using the same operations used in R. Similarly, a **subfield** of a field F is a subset $K \subseteq F$ which is also a field using the same operations used in F.

9.22 Theorem: *If S be a subset of a ring R, then S is a subring of R if and only if*
(1) $0 \in S$,
(2) S is closed under addition, that is $a + b \in S$ for all $a, b \in S$,
(3) S is closed under multiplication, that is $ab \in S$ for all $a, b \in S$, and
(4) S is closed under additive inverse, that is $-a \in S$ for all $a \in S$.
Similarly, if K is a subset of a field F then K is a subfield of F if and only if
(1) $0 \in K$ and $1 \in K$,
(2) K is closed under addition, that is $a + b \in K$ for all $a, b \in K$,
(3) K is closed under multiplication, that is $ab \in K$ for all $a, b \in K$,
(4) K is closed under additive inverse, that is $-a \in S$ for all $a \in K$, and
(5) K s closed under multiplicative inverse, that is $a^{-1} \in K$ for all $0 \neq a \in F$.

9.23 Example: $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ is a subring of $\mathbb{R}$, $\mathbb{R}$ is a subring of $\mathbb{C}$, and $\mathbb{C}$ is a subring of $\mathbf{H}$. Also, $\mathbb{Q}$ is a subfield of $\mathbb{R}$ which is a subfield of $\mathbb{C}$.

9.24 Example: In $\mathbb{Z}$, the subgroups are of the form $\langle n \rangle = \{kn \,|\, k \in \mathbb{Z}\}$ where $0 \leq n \in \mathbb{Z}$. Each of these subgroups is also a subring of $\mathbb{Z}$. In $\mathbb{Z}_n$, the subgroups are of the form $\langle d \rangle = \{kd | k \in \mathbb{Z}_{n/d}\}$ where $d|n$, and each of these subgroups is also a subring.

9.25 Example: In $\mathbb{Z}_{12}$ we have the subring $\langle 3 \rangle = \{0, 3, 6, 9\}$. Notice that $9 \cdot 0 = 0$, $9 \cdot 3 = 3$, $9 \cdot 6 = 6$ and $9 \cdot 9 = 9$, so 9 is the identity element in the group $\langle 3 \rangle$. This example shows that the identity element in a subring of R does not need to be equal to the identity element of R.

9.26 Example: Define

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\} \text{ , and}$$
$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\} \,.$$

Then $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$ and $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$ because

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \,.$$

In fact $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$ because for $a, b \in \mathbb{Q}$, if $a + b\sqrt{2} \neq 0$ then $a^2 \neq 2b^2$ and

$$(a + b\sqrt{2}) \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \right) = 1 \,.$$

9.27 Example: More generally, if R is a subring of S and $A \subseteq S$, then we write $R[A]$ for the smallest subring of S which contains R and A, or equivalently the intersection of all subrings of S which contain $R \cup A$. Some particular cases of this include the subrings

$$\begin{aligned} \mathbb{Z}[i] &= \big\{a + bi \,\big|\, a, b \in \mathbb{Z}\big\} \subseteq \mathbb{C} \\ \mathbb{Q}[\alpha] &= \big\{a + b\alpha + c\alpha^2 \,\big|\, a, b, c \in \mathbb{Q}\big\} \subseteq \mathbb{C} \text{ , where } \alpha = e^{i\,2\pi/3} \\ \mathbb{Q}[\sqrt{2}, \sqrt{3}] &= \big\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,\big|\, a, b, c, d \in \mathbb{Q}\big\} \subseteq \mathbb{R}. \end{aligned}$$

As an exercise, check that these are all rings and that $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ are fields.

9.28 Example: We sometimes use notation, similar to the notation used in the above example, for some other rings. For example, we write

$$\mathbb{Z}_n[i] = \big\{a + bi \,\big|\, a, b \in \mathbb{Z}_n\big\}\,.$$

This is a ring under the operations given by $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

9.29 Example: For an interval $A \subseteq \mathbb{R}$, let $\mathcal{C}^0(A, \mathbb{R})$ denote the set of continuous functions $f : A \to \mathbb{R}$, for $k \in \mathbb{Z}^+$ let $\mathcal{C}^k(A, \mathbb{R})$ denote the set of functions $f : A \to \mathbb{R}$ such that the k^{th} derivative $f^{(k)}$ exists and is continuous in A, and let $\mathcal{C}^\infty(A, \mathbb{R})$ denote the set of infinitely differentiable functions $f : A \to \mathbb{R}$. Then $\mathcal{C}^\infty(A, \mathbb{R})$ is a subring of $\mathcal{C}^k(A, \mathbb{R})$ which is a subring of $\mathcal{C}^0(A, \mathbb{R})$ which, in turn, is a subring of $\text{Func}(A, \mathbb{R})$.

9.30 Example: For a ring R, the polynomial ring $R[x]$ is a subring of the formal power series ring $R[[x]]$. More generally, $R[x_1, \cdots, x_n]$ is a subring of $R[[x_1, \cdots, x_n]]$. If S is a subring of R then $S[x]$ is a subring of $R[x]$ and $S[[x]]$ is a subring of $R[[x]]$, and more generally, $S[x_1, \cdots, x_n]$ is a subring of $R[x_1, \cdots, x_n]$ and $S[[x_1, \cdots, x_n]]$ is a subring of $R[[x_1, \cdots, x_n]]$. We can regard R as a subring of $R[x]$ by identifying an element $a \in R$ with the corresponding constant polynomial in $R[x]$. Similarly, we can regard $R[x_1, \cdots, x_n]$ as a subring of $R[x_1, \cdots, x_n, x_{n+1}]$ and $R[[x_1, \cdots, x_n]]$ as a subring of $R[[x_1, \cdots, x_n, x_{n+1}]]$.

9.31 Example: Although we can regard the polynomial ring $\mathbb{R}[x]$ as a subring of the ring of functions $\text{Func}(\mathbb{R}, \mathbb{R})$ (since we can regard a polynomial as a kind of function), in general given a ring R we cannot regard $R[x]$ as a subring of $\text{Func}(R, R)$. For example, if R is finite, say with $|R| = n$, then $\big|\text{Func}(R, R)\big| = n^n$ but $\big|R[x]\big| = \infty$ (or more precisely $\big|R[x]\big| = \aleph_0$).

9.32 Example: For a ring R, the set $T_n(R)$ of upper-triangular matrices with entries in R is a subring of $M_n(R)$. If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$.

9.33 Definition: For a ring R, we define the **centre** of R to be the ring

$$Z(R) = \big\{a \in R \big| ax = xa \text{ for all } x \in R\big\}.$$

As an exercise, verify that $Z(R)$ is in fact a subring of R.