MA3202

Algebra II

Spring 2022

Satvik Saha
19MS154

Indian Institute of Science Education and Research, Kolkata,
Mohanpur, West Bengal, 741246, India.

Contents

1 Rings

1.1 Basic definitions

Definition 1.1. A ring is a set R equipped with two binary operations, namely addition and multiplication, such that

1. $(R, +)$ is an abelian group.
   (a) $a + b \in R$ for all $a, b \in R$.
   (b) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
   (c) $a + b = b + a$ for all $a, b \in R$.
   (d) There exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
   (e) For each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
2. $(R, \cdot)$ is a semi-group.
   (a) $a \cdot b \in R$ for all $a, b \in R$.
   (b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
3. Multiplication distributes over addition.
   (a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$.
   (b) $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$.

Remark. The following properties follow immediately,

1. $0 \cdot a = 0$ for all $a \in R$.
2. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ for all $a, b \in R$.
3. $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$ for all $a, b \in R$.

Example. The integers $\mathbb{Z}$ form a ring, under the usual addition and multiplication.

Example. All fields, for instance the rational numbers $\mathbb{Q}$ or the real numbers $\mathbb{R}$, are rings.

Example. The integers modulo n, namely $\mathbb{Z}/n\mathbb{Z}$, form a ring.

Example. If R is a ring, then the algebra of polynomials $R[X]$ with coefficients from R form a ring.

Example. If R is a ring, then the $n \times n$ matrices $M_n(R)$ with entries from R form a ring.

Definition 1.2. If R is a ring and $(R, \cdot)$ is a monoid i.e. has an identity, then this identity is unique and called the unity of the ring R. Such a ring R is called a unit ring. Note that we typically demand that this identity is distinct from the zero element.

Example. The even integers $2\mathbb{Z}$ form a ring, but do not contain the identity.

Example. The trivial ring $\{0\}$ is typically not considered to be a unit ring, since must serve as the additive identity as well as the multiplicative identity.

Definition 1.3. If R is a ring and $(R, \cdot)$ is commutative, then R is called a commutative ring.

Definition 1.4. Let R be a unit ring. An element $a \in R$ is called a unit if there exists $b \in R$ such that $a \cdot b = 1 = b \cdot a$. This $b \in R$ is unique, and denoted by a^{-1}.

Example. The units in $\mathbb{Z}$ are $\{1, -1\}$.

1.2 Subrings

Definition 1.5. Let R be a ring, and let $S \subseteq R$. We say S is a subring of R if the structure $(S, +, \cdot)$ is a ring, with addition and multiplication inherited from R.

Example. The rings $n\mathbb{Z}$ for $n \in \mathbb{N}$ are all subrings of $\mathbb{Z}$.

Example. Consider the rings $2\mathbb{Z} \subset \mathbb{Z}$. Here, $\mathbb{Z}$ is a unit ring but $2\mathbb{Z}$ is not.

Example. Consider the rings $4\mathbb{Z}/12\mathbb{Z} \subset 2\mathbb{Z}/12\mathbb{Z}$. Here, $2\mathbb{Z}/12\mathbb{Z}$ is not a unit ring but $4\mathbb{Z}/12\mathbb{Z}$ is.

Lemma 1.1. *Let S be a subring of R. Since $(R, +)$ is an abelian group, $(S, +)$ is a normal subgroup of $(R, +)$. Thus, we can make sense of the quotient group $(R/S, +)$.*

Lemma 1.2. *Let S be a subring of R. Then, the quotient $(R/S, +, \cdot)$ is a ring with multiplication $(a + S) \cdot (b + S) = ab + S$ if and only if $ab - xy \in S$ for all $a, b, x, y \in R$ such that the cosets $a + S = x + S$, $b + S = y + S$.*

Example. Consider the ring $\mathbb{Z}$ and the subring $n\mathbb{Z}$. Then, the quotient $\mathbb{Z}/n\mathbb{Z}$ is indeed a ring.

Example. Consider the ring $\mathbb{Q}$ and the subring $\mathbb{Z}$. It cal be shown that $\mathbb{Q}/\mathbb{Z}$ is not a ring under the 'natural' multiplication.

1.3 Ideals

Definition 1.6. Let R be a ring and let I be a subset of R. We say that I is an ideal of R if $(I, +)$ is a subgroup of $(R, +)$, and $rx, xr \in I$ for all $r \in R$, $x \in I$.

Example. Consider the ring $\mathbb{Z}$, and the subring $n\mathbb{Z}$. This is an ideal of $\mathbb{Z}$, since $m(n\mathbb{Z}) \subseteq n\mathbb{Z}$. Indeed, every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$. This will follow from Euclid's Division Lemma.

Example. The subsets $\{0\}$ and R of any ring R are trivial ideals.

Lemma 1.3. *Let R be a ring, and I be an ideal of R. Then, the quotient R/I is a ring.*

Proof. Note that whenever $a - x \in I$, $b - y \in I$, we demand that $ab - xy \in I$. This can be rewritten as $(a - x)b + x(b - y) \in I$, which is clearly true by the properties of the ideal I. □

Definition 1.7. An ideal $I \subset R$ is called finitely generated if there exist $x_1, x_2, \ldots, x_n \in I$ such that every element of I can be written as a finite linear combination

$$x = r_1 x_1 + \cdots + r_n x_n,$$

where $r_i \in R$. We denote $I = (x_1, x_2, \cdots, x_n)$.

Definition 1.8. An ideal generated by a single element is called a principal ideal.

Example. Every ideal of $\mathbb{Z}$ is a principal ideal.

Lemma 1.4. *Let R be a unit ring, and $I \subseteq R$ be an ideal. Then, $I = R$ if and only if I contains a unit.*

Definition 1.9. The sum of two ideals $I, J \subset R$ is defined

$$I + J = \{x + y : x \in I, y \in J\}.$$

Their product is defined

$$IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J\}.$$

Lemma 1.5. *The sum and product of two ideals of a ring are also ideals of that ring.*

1.4 Integral domains

Definition 1.10. Let R be a ring and $a, b \in R$, $a, b \neq 0$. If $ab = 0$, we call a a left zero divisor and b a right zero divisor.

Example. Consider $2, 3 \in \mathbb{Z}/6\mathbb{Z}$; then $2 \cdot 3 = 6 \equiv 0$.

Definition 1.11. A commutative ring R is called an integral domain if it has no zero divisors.

Example. When p is prime, the rings $\mathbb{Z}/p\mathbb{Z}$ are integral domains. Note that this set is a group under both $+$ and $\cdot$.

Lemma 1.6. *Every field is an integral domain.*

Theorem 1.7. *Every finite integral domain is a field.*

Proof. Let $R = \{x_1, \ldots, x_n\}$ be a finite integral domain. We first show that R contains an identity 1. Pick $x \neq 0$, and note that $xx_1, xx_2, \ldots, xx_n$ must all be distinct: otherwise $xx_i = xx_j$ would force $x(x_i - x_j) = 0$. This forces $x = xx_k$ for some $x_k \neq 0$. Now, we claim that x_k is our identity. Indeed, given any $y \neq 0$, we write $y = xx_l$ for some $x_l \neq 0$, hence $yx_k = xx_lx_k = x_l(xx_k) = x_lx = y$.

Next, we show that every non-zero $x \in R$ has an inverse. Indeed, $1 = x_k$ must be one of the $xx_1, \ldots, xx_n$, hence $1 = xx_m$ for some non-zero x_m. This means that $x_m = x^{-1}$. □

Definition 1.12. Let R be a ring. The characteristic of R is the smallest positive integer n such that $nx = 0$ for all $x \in R$. If no such number n exists, we say that the characteristic of R is zero. We denote the characteristic of R by $\mathrm{ch}(R)$.

Example. We have $\mathrm{ch}(\mathbb{Z}) = 0$, $\mathrm{ch}(\mathbb{Z}/n\mathbb{Z}) = n$.

Lemma 1.8. *Let R be a unit ring. Then, $\mathrm{ch}(R)$ is the smallest positive integer n such that $n \cdot 1 = 0$; if no such n exists, then $\mathrm{ch}(R)$ is zero.*

Theorem 1.9. *Let R be an integral domain. Then, $\mathrm{ch}(R)$ is either zero or a prime.*

Proof. Let R be an integral domain such that $\mathrm{ch}(R) = n \neq 0$. If n is not a prime, write $n = n_1n_2$ for $n_1, n_1 < n$. Then for any non-zero $x \in R$, write $0 = n(x^2) = (n_1x)(n_2x)$. This forces one of $n_1x, n_2x = 0$; say $n_1x = 0$. Now for any $y \in R$, we have $x(n_1y) = (n_1x)y = 0$. Since $x \neq 0$, we have $n_1y = 0$ for all $y \in R$, contradicting the minimality of n. □

1.5 Simple rings

Definition 1.13. A simple ring is one which has no non-trivial ideals. We typically demand that multiplication in R is non-trivial.

Lemma 1.10. *Every field is a simple ring.*

Proof. If R is a field and $I \subset R$ is an ideal with non-zero $a \in I$, then $a^{-1} \in R$ hence $a^{-1}a = 1 \in I$. This immediately forces $I = R$. □

Lemma 1.11. *If R is a commutative, simple, unit ring, then R is a field.*

Proof. Pick non-zero $a \in R$, and set $I = (a)$. Since R is simple, $I = R$, hence $1 \in I = (a)$. In other words, $1 = ab$ for some $b \in R$. □

1.6 Homomorphisms

Definition 1.14. Let R, S be rings, and let $\varphi\colon R \to S$. We say that φ is a ring homomorphism if $\varphi(x+y) = \varphi(x)+\varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in R$. If R and S are unit rings, we also demand that $\varphi(1_R) = 1_S$.

Definition 1.15. A bijective homomorphism between two rings is called an isomorphism. If an isomorphism exists between two rings, we say that they are isomorphic.