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

$$x = r_1x_1 + \cdots + r_nx_n,$$

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

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

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

Lemma 1.6. *Let $I, J \subset R$ be ideals in the commutative ring R. Then, $IJ \subset I \cap J$.*

Example. Note that for $2\mathbb{Z}, 2\mathbb{Z} \in \mathbb{Z}$, $(2\mathbb{Z})(2\mathbb{Z}) = 4\mathbb{Z}$ but $2\mathbb{Z} \cap 2\mathbb{Z} = 2\mathbb{Z}$. A related example is $R = 2\mathbb{Z}$, $I = 4\mathbb{Z}$, $J = 6\mathbb{Z}$.

Lemma 1.7. *If $I, J \subset R$ are ideals in a unit commutative ring R, and $I + J = R$, then $IJ = I \cap J$.*

Proof. We already know that $IJ \subseteq I + J$. Since $I + J = R$, we can pick $x \in I, y \in J$ such that $x + y = I$. Now pick $a \in I \cap J$, hence $a \cdot 1 = ax + ay \in I \cap J$; but this is also an element of IJ proving $I \cap J \subseteq IJ$. □

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 1.8. *Every field is an integral domain.*

Theorem 1.9. *Every finite integral domain is a field.*

Proof. Let $R = \{x_1, \dots, x_n\}$ be a finite integral domain. We first show that R contains an identity 1. Pick $x \neq 0$, and note that $xx_1, xx_2, \dots, xx_n$ 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 $xx_1, \dots, xx_n$, 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 1.10. *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 1.11. *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 $n = n_1 n_2$ for $n_1, n_1 < n$. Then for any non-zero $x \in R$, write $0 = n(x^2) = (n_1 x)(n_2 x)$. This forces one of $n_1 x, n_2 x = 0$; say $n_1 x = 0$. Now for any $y \in R$, we have $x(n_1 y) = (n_1 x) y = 0$. Since $x \neq 0$, we have $n_1 y = 0$ 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 1.12. *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 1.13. *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 and isomorphisms

Definition 1.14. Let R, S be rings, and let $\varphi\colon R \to S$. We say that φ is a ring homomorphism if

1. $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in R$.
2. $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in R$.
3. $\varphi(1_R) = 1_S$.

We only insist on 3 if both R and S are unit rings.

Remark. The following properties follow immediately.

1. $\varphi(0_R) = 0_S$.
2. $\varphi(-x) = -\varphi(x)$ for all $x \in R$.
3. $\varphi(nx) = n\varphi(x)$ for all $x \in R$, $n \in \mathbb{Z}$.
4. $\varphi(x-y) = \varphi(x) - \varphi(y)$ for all $x, y \in R$.

Example. The map $\varphi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto k \bmod n$ is a homomorphism.

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.

Example. The map $\varphi\colon \mathbb{Z} \to n\mathbb{Z}$, $k \mapsto nk$ is an isomorphism.

Example. The map $\varphi\colon \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ is an isomorphism.

Lemma 1.14. *The only isomorphism $\mathbb{Z} \to \mathbb{Z}$ is the identity map.*

Theorem 1.15. *The only isomorphism $\mathbb{Q} \to \mathbb{Q}$ is the identity map.*

Proof. Let $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ be an isomorphism. We must have $\varphi(1) = 1$, which immediately gives $\varphi(n) = n$ for all $n \in \mathbb{Z}$. Now for any rational $p/q \in \mathbb{Q}$, note that $1 = \varphi(q \cdot 1/q) = q \cdot \varphi(1/q)$, forcing $\varphi(1/q) = 1/q$. Thus, $\varphi(p/q) = p/q$, completing the proof. □

Theorem 1.16. *The only isomorphism $\mathbb{R} \to \mathbb{R}$ is the identity map.*

Proof. Let $\varphi\colon \mathbb{R} \to \mathbb{R}$ be an isomorphism. We must have $\varphi(q) = q$ for all $q \in \mathbb{Q}$.

First we show that φ is strictly increasing. Note that when $x > 0$, $\varphi(x) = \varphi(\sqrt{x})^2 > 0$. Thus when $x > y$, $\varphi(x-y) > 0$, hence $\varphi(x) > \varphi(y)$.

Now let $x \in \mathbb{R}$; if $\varphi(x) \neq x$, we must have one of $\varphi(x) > x$ or $\varphi(x) < x$. Assume the former, and find $q \in \mathbb{Q}$ such that $\varphi(x) > q > x$. Now, $q > x$ gives $q = \varphi(q) > \varphi(x)$, a contradiction. An analogous argument gives a contradiction when $\varphi(x) < x$, completing the proof. □

Theorem 1.17. *The only homomorphism $\mathbb{R} \to \mathbb{R}$ is the identity map.*

Proof. If $\varphi\colon \mathbb{R} \to \mathbb{R}$ is a homomorphism, it is easy to check that $\varphi^{-1}(0)$ is an ideal. Since $\mathbb{R}$ is simple, this must be $\{0\}$ or $\mathbb{R}$; the latter can be ruled out since $\varphi(1) = 1$. In other words, $\varphi^{-1} = \{0\}$ so φ is injective. Following the previous proof, φ must be an isomorphism, hence the identity map. $\square$

Theorem 1.18. *The only isomorphisms $\mathbb{C} \to \mathbb{C}$ which sends $\mathbb{R} \to \mathbb{R}$ are the maps $z \mapsto z$ and $z \mapsto \bar{z}$.*

Proof. The previous theorem guarantees that any such isomorphism $\varphi\colon \mathbb{C} \to \mathbb{C}$ is completely determined by $\varphi(i)$. Now, $-1 = \varphi(-1) = \varphi(i)^2$, forcing $\varphi(i) = \pm i$. $\square$

Lemma 1.19. *The kernel of a ring homomorphism $\varphi\colon R \to S$ is an ideal of R. Its image is a subring of S.*

Proof. If $x \in \ker\varphi$, then $\varphi(x) = 0$, hence for any $r \in R$ we have $\varphi(rx) = \varphi(r)\varphi(x) = 0$. Thus, $rx \in \varphi^{-1}(0)$. Also, recall that $\varphi^{-1}(0)$ is an additive subgroup of R. $\square$

Theorem 1.20 (First isomorphism theorem)**.** *Let $\varphi\colon R \to S$ be a surjective ring homomorphism. Then,*

$$R/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. Denote $I = \ker\varphi$, so the elements of R/I are the cosets $x + I$ for $x \in R$. This gives us the natural map

$$\phi\colon R/I \to S, \qquad x + I \mapsto \varphi(x).$$

It can be shown that this map is well defined: if $x + I = y + I$, then $x - y \in I$ so $\varphi(x - y) = 0$, or $\varphi(x) = \varphi(y)$. Now, $\phi((x + I) + (y + I)) = \varphi(x + y) = \varphi(x) + \varphi(y) = \phi(x + I) + \phi(y + I)$, and $\phi((x + I)(y + I)) = \varphi(xy) = \varphi(x)\varphi(y) = \phi(x + I)\phi(y + I)$. Additionally, if R and S are both unit rings, then $\phi(1_R + I) = \varphi(1_R) = 1_S$. Thus, ϕ is a homomorphism. It is obvious that ϕ is surjective; also observe that $\phi^{-1}(0) = 0 + I$, hence ϕ is also injective. This proves that ϕ is an isomorphism, as desired. $\square$

Theorem 1.21. *Let $I, J \subset R$ be ideals. Then,*

$$(I + J)/J \cong I/(I \cap J).$$

Proof. The map $\phi\colon I \to (I + J)/J$, $x \mapsto x + J$ can be shown to be a surjective homomorphism. It's kernel consists of the elements in I that get mapped to $0 + J$, so $\ker\phi = I \cap J$. Applying the first isomorphism theorem gives the desired result. $\square$

Lemma 1.22. *Let $I \subset R$ be an ideal, and let $\varphi\colon R \to S$ be a surjective ring homomorphism, then $\varphi(I)$ is an ideal in S.*

Theorem 1.23 (Correspondence theorem)**.** *Let $I \subset R$ be an ideal. Then there exists a one-to-one correspondence between the ideals of R containing I with the ideals of R/I.*

Proof. Use the surjective ring homomorphism $\phi\colon R \to R/I$, $x \mapsto x + I$, which maps ideals in R to ideals in R/I. Furthermore, given ideals $J, J' \subset R$ such that $\varphi(J) = \varphi(J')$, note that $x \in J$ implies $\varphi(x) \in \varphi(J) = \varphi(J')$ so $x \in J'$; this shows that $J = J'$, hence our map is injective. Finally, given an ideal K in R/I, its pre-image under our map is the ideal $L = \{x \in R : x + I \in K\}$. □

Theorem 1.24 (Chinese remainder theorem)**.** *Let R be a commutative unit ring, and $I, J \subset R$ be ideals such that $I + J = R$. Then,*

$$R/IJ \cong R/I \times R/J.$$

Proof. Consider the map

$$\varphi\colon R \to R/I \times R/J, \qquad x \mapsto (x + I, x + J).$$

It is clear that this is a ring homomorphism. Furthermore, φ is surjective: to see this, pick $a \in I$, $b \in J$ such that $a + b = 1$. Then

$$\varphi(ay + bx) = (a(y - x) + x + I, b(x - y) + y + J) = (x + I, y + J).$$

Now, note that $\varphi(x) = (I, J)$ forces $x \in I \cap J$; but the latter is just IJ by a previous lemma. Applying the first isomorphism theorem gives the desired result. □

1.7 Quotient field

We recall the standard construction of $\mathbb{Q}$ from $\mathbb{Z}$, and generalize this to the construction of the field $Q(R)$ from an integral domain R. Consider the equivalence relation on the set $R \times R \setminus \{0\}$ defined by

$$(a, b) \sim (c, d) \iff ad = bc.$$

This partitions $R \times R \setminus \{0\}$ into equivalence classes; let $Q(R)$ be the collection of these equivalence classes. Now define addition and multiplication of elements from $Q(R)$ as

$$[a, b] + [c, d] = [ad + bc, bd], \qquad [a, b] \cdot [c, d] = [ac, bd].$$

It can be verified that this is well defined. Furthermore, we have an additive identity $[0, a]$, a multiplicative identity $[a, a]$, and every non-zero element $[a, b]$ has a multiplicative inverse $[b, a]$. The remaining properties can be checked to show that $Q(R)$ is a field. We can now embed R in $Q(R)$ via the map

$$i\colon R \to Q(R), \qquad x \mapsto [ax, a].$$

It can also be shown that $Q(R)$ is the smallest field containing R. Indeed if $j\colon R \to F$ is an embedding of R in the field F, we can embed $Q(R)$ in F using the map $[a, b] \mapsto j(a) \cdot j(b)^{-1}$.

Remark. We do not require R to have a multiplicative identity!

Definition 1.16. The field $Q(R)$ constructed as above is called the field of fractions, or quotient field of the integral domain R.

Lemma 1.25. *Let R_1, R_2 be integral domains. If $R_1 \cong R_2$, then $Q(R_1) \cong Q(R_2)$.*