Algebra II: Introduction to Rings

Arjun Vardhan

January 2022

1 Basic Definitions

- $(R, +, \cdot)$ is a ring if:
  1. R is an abelian group with respect to $+$.
  2. $(a \cdot b) \cdot c = (a \cdot b) \cdot c$ for all $a, b, c \in R$.
  3. $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.
  4. $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.
- R is a commutative ring if $a \cdot b = b \cdot a$ for all $a, b \in R$.
- R is said to have an identity if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. In such a case R is also called a ring with unity.
- A ring R with identity 1, where $1 \neq 0$, is called a division ring or a skew field if for all $a \neq 0$, $a \in R$, there exists $b \in R$ such that $a \cdot b = b \cdot a = 1$.
- Trivial rings are those obtained by taking any abelian group and letting $a \cdot b = 0$ for all $a, b \in R$. The simplest example is the zero ring, $\{0\}$. Trivial rings are commutative.
- **Let R be a ring. Then:**
  1. $a \cdot 0 = 0$ **for all** $a \in R$**.** *Proof:* $a \cdot 0 = a \cdot (0 + 0) = a \cdot +a \cdot 0$. So $a \cdot 0 = 0$. ■
  2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$**, for all** $a, b \in R$**.** *Proof:* $a \cdot b + (-a) \cdot b = b \cdot (a + (-a)) = b \cdot 0 = 0$. So $(-a) \cdot b = -(a \cdot b)$. ■
  3. $(-a) \cdot (-b) = ab$ **for all** $a, b \in R$**.** *Proof:* $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$. ■
  4. **If R has an identity 1, then that identity is unique and** $-a = (-1) \cdot a$**.** *Proof:* Suppose there exists another identity $\psi \in R$. Then $\psi \cdot 1 = 1 \cdot \psi = \psi = 1$. $a + (-1) \cdot a = a \cdot (1 + (-1)) = a \cdot 0 = 0$. So $-a = (-1) \cdot a$. ■
- $a \in R$, $a \neq 0$ is called a zero divisor if there exists $b \in R$ such that $ab = 0$ or $ba = 0$.
- Let R have an identity $1 \neq 0$. $u \in R$ is called a unit in R if there exists $v \in R$ such that $uv = vu = 1$.
- The set of all units in a ring R is a group under multiplication. It is denoted $R^\times$.
- **If u is a unit in R, then so is $-u$.** *Proof:* There exists $v \in R$ such that $uv = vu = 1$. Then $(-u)(-v) = uv = 1$. ■
- **Let R be a ring with identity and let S be a subring of R such that $1 \in S$. If u is a unit in S then u is a unit in R. The converse is not necessarily true.** *Proof:* Let u be a unit in S. Then there exists $v \in S$ such that $uv = 1$. Since $u, v \in S$, $u, v \in R$ and thus u is a unit in R. Consider $\mathbb{R}$ and $\mathbb{Z}$. $\mathbb{Z}$ is a subring of $\mathbb{R}$. 2 is a unit in $\mathbb{R}$ but not in $\mathbb{Z}$. ■
- **A zero divisor cannot be a unit.** *Proof:* Suppose a is a unit in R and that $ab = 0$ for some $b \in R$, $b \neq 0$. Then $va = 1$ for some $v \in R$, so $b = 1b = vab = v(ab) = v0 = 0$, which is a contradiction. Similarly, if $ba = 0$ then a cannot be a unit. ■
- **If $\overline{a} \neq \overline{0}$ and $\gcd(a, n) \neq 1$, then $\overline{a}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$.** *Proof:* Let $d = \gcd(a, n)$ and let $b = \frac{n}{d}$. $d > 1$ so $0 < b < n$ and thus $\overline{b} \neq \overline{0}$. But since $\frac{ab}{bd} = \frac{a}{d}$, $n \mid ab$ and so $\overline{ab} = \overline{0}$. Thus $\overline{a}$ is a zero divisor. ■

- A field is a commutative ring with identity $1 \neq 0$ where every nonzero element is a unit.
- A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.
- **Suppose a, b, c belong to a ring R such that a is not a zero divisor and $ab = ac$. Then, either $a = 0$ or $b = c$. In particular, if R is an integral domain, then $a = 0$ or $b = c$.** *Proof:* If $ab = ac$ then $a(b - c) = 0$. Since a is not a zero divisor, $a = 0$ or $b - c = 0$. The second part follows from the definition of an integral domain. ■
- **Any finite integral domain is a field.** *Proof:* Let R be a finite integral domain and let $a \in R$, $a \neq 0$. By the cancellation law, the map $f : R \to R$, $f(x) = ax$ is an injective function. Since R is finite this map is also surjective. So there exists some $b \in R$ such that $ab = 1$, thus a is a unit. ■
- A subring of R is a subgroup of R that is closed under multiplication.
- To check that $S \subset R$ is a subring of R, it suffices to check that $S \neq \phi$ and that S is closed under subtraction and multiplication.
- **Let $\{S_i\}$ be a nonempty collection of subrings of R. Then $\bigcap_i S_i$ is also a subring of R.** *Proof:* Every subring of R must contain 0, so $\bigcap_i S_i$ is nonempty. Suppose $a, b \in \bigcap_i S_i$. Then $a, b \in S_i$ for all i, so $a - b$, $ab \in S_i$ for all i. ■
- The center of a ring R is the set of all elements that commute with every element of R, i.e, $\{z \in R : zr = rz,\ \forall r \in R\}$.
- **The center of a ring R is a subring of R.** *Proof:* Let the center of R be denoted by C. $0r = r0 = 0$ for all $r \in R$ so $0 \in C$. Suppose $a, b \in C$. Then $(a - b)r = ar - br = ra + (-1)br = ra + (-1)rb = ra - rb = r(a - b)$ for all $r \in R$. So $a - b \in C$. Also, $abr = arb = rab$ for all $r \in R$. Thus $ab \in C$. ■
- **The center of a division ring is a field.** *Proof:* Let R be a division ring and let C be the center of R. Every nonzero element in R is a unit so the same is true for C. $1r = r1 = r$ for all $r \in R$ so $1 \in C$. C is commutative by definition. Therefore C is a field. ■
- **Any subring of a field which contains 1 is an integral domain.** *Proof:* Let F be a field and let $S \subset F$ be a subring of F such that $1 \in S$. Since F is commutative, so is S. Every nonzero element in F is a unit in F, and a unit cannot be a zero divisor, so S has no zero divisors. Thus S is an integral domain. ■
- An element $x \in R$ is called nilpotent if $x^m = 0$ for some $m \in \mathbb{Z}^+$.
- **Let x be a nilpotent element of a commutative ring R. Then,**
  1. **x is either 0 or a zero divisor.** *Proof:* Suppose $x \neq 0$ and $x^n = 0$, where n is the smallest such integer. Then $xx^{n-1} = 0$, where $x^{n-1} \neq 0$. So x is a zero divisor. Now suppose that x is not a zero divisor and $x^n = 0$ and n is the smallest such integer. Then $xx^{n-1} = 0$ where $x^{n-1} \neq 0$. If $x \neq 0$ then x would be a zero divisor, which is a contradiction. So $x = 0$. ■
  2. **rx is nilpotent for all $r \in R$.** *Proof:* Suppose $x^n = 0$. Then $(rx)^n = r^n x^n = r^n 0 = 0$. So rx is nilpotent. ■
  3. **$1 + x$ is a unit in R.** *Proof:* Suppose $x^k = 0$, where k is the smallest such integer. Then $(1 - x)(1 - x + x^2 - x^3 + ... + (-1)^k x^{k+1}) = 1 + (-1)^k x^{k+1} = 1 + 0 = 1$. ■
  4. **If u is a unit, then $u + x$ is a unit.** *Proof:* Suppose $x^k = 0$, where k is the smallest such integer and $uv = vu = 1$. Then $(u + x)v = 1 + vx$. Since vx is nilpotent, $1 + vx$ is a unit. So $u + x = u(1 + vx)$. Since the set of all units is closed under multiplication, $u + x$ is a unit. ■
- A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$.
- **Every Boolean ring is commutative.** *Proof:* Let $a, b \in R$, where R is a boolean ring. First we show that every element in a Boolean ring is its own additive inverse. $(a + a) = (a + a)^2 = a^2 + 2a^2 + a^2 = (a + a) + (a + a) \implies a + a = 0$. Now, $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = (a + b) + (ab + ba) \implies ab = -ba = ba$. ■

2 Polynomial Rings, Matrix Rings, Group Rings

3 Ring Homomorphisms and Quotient Rings

- Let R and S be rings. A ring homomorphism is a map $\gamma : R \to S$ such that $\gamma(a+b) = \gamma(a) + \gamma(b)$ and $\gamma(ab) = \gamma(a)\gamma(b)$ for all $a, b \in R$.
- The kernel of the ring homomorphism γ, denoted $\mathrm{Ker}(\gamma)$, is the set of all elements in R that map to 0 in S.
- A bijective ring homomorphism is called an isomorphism.
-

4 Properties of Ideals

5 Rings of Fractions

6 Chinese Remainder Theorem