Lecture notes for Abstract Algebra: Lecture 17

1 Rings

Definition 1. A nonempty set R is a ring if it has two closed binary operations, addition $(+)$ and multiplication $(\cdot)$, satisfying the following conditions.

1. $a + b = b + a$ for $a, b \in R$.
2. $(a + b) + c = a + (b + c)$ for $a, b, c \in R$.
3. There is an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
4. For every element $a \in R$, there exists an element $-a$ in R such that $a+(-a) = 0$.
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for $a, b, c \in R$.
6. For $a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

This last condition, the distributive axiom, relates the binary operations of addition and multiplication. Notice that the first four axioms simply require that a ring be an abelian group under addition, so we could also have defined a ring to be an abelian group $(R, +)$ together with a second binary operation satisfying the fifth and sixth conditions given above. If there is an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for each element $a \in R$, we say that R is a **ring with unity or identity**. A ring R for which $ab = ba$ for all $a, b \in R$ is called a **commutative ring**. The product $a \cdot b$ will sometimes be written as simply ab.

Definition 2. A commutative ring with identity is called an **integral domain** if

$$a.b = 0 \qquad \Rightarrow \qquad a = 0 \quad \text{or} \quad b = 0.$$

A **non-zero element** $a \in R$ such that $a.b = 0$ for some **non-zero** element $b \in R$, is called a **divisor of zero**.

Definition 3. A commutative ring with identity where **every non-zero element has a multiplicative inverse** is called a **field**.

Example 4. The integers form a ring. In fact, $\mathbb{Z}$ is an integral domain. Certainly if $ab = 0$ for two integers a and b, either $a = 0$ or $b = 0$. However, $\mathbb{Z}$ is not a field. The only integers with multiplicative inverses are 1 and -1.

Example 5. We can define the product of two elements a and b in $\mathbb{Z}_n$ by $ab \pmod{n}$. For instance, in $\mathbb{Z}_{12}$, $5 \cdot 7 = 11 \,(\mathrm{mod}\, 12)$. This product makes the abelian group $\mathbb{Z}_n$ into a ring. Certainly $\mathbb{Z}_n$ is a commutative ring; however, it may fail to be an integral domain. If we consider $3 \cdot 4 = 0 \,(\mathrm{mod}\,)$ in $\mathbb{Z}_{12}$, it is easy to see that a product of these two nonzero elements in the ring is equal to zero. The elements 3 and 4 are zero divisors in $\mathbb{Z}_{12}$.

Example 6. Consider the ring $R = \mathbb{Z}_n$. Let $x \in R$. The existence of an element $y \in R$ such that

$$x \cdot y \equiv 1 \pmod{n}$$

is equivalent to the existence of $y, z \in \mathbb{Z}$ satisfying the equation

$$xy - 1 = nz \iff xy - nz = 1.$$

This last equation is equivalent to $\gcd(n, x) = 1$ and therefore an element $x \in \mathbb{Z}_n$ **is a unit if and only if the greatest common divisor** $\gcd(x, n) = 1$. In particular, **the ring $\mathbb{Z}_p$, for p a prime number, is a field** since a prime number has $\gcd(p, x) = 1$ for every $0 < x < p$.

Example 7. Under the ordinary operations of addition and multiplication, all of the familiar number systems are rings with unit: the rationals, $\mathbb{Q}$; the real numbers, $\mathbb{R}$; and the complex numbers, $\mathbb{C}$. Each of these rings is in fact **a field**.

Example 8. The following example, also referred to as Hamilton's quaternions $\mathbb{H}$, is an example of a non-commutative ring where every non-zero element has a multiplicative inverse: this is referred to as **a division ring**. Consider

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

and $\mathbb{H} = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$. The rule of multiplication are done using the relations:

$$\mathbf{i}^2 = -\mathbf{1}, \quad \mathbf{j}^2 = -\mathbf{1} \quad \mathbf{k}^2 = -\mathbf{1}$$

$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}$$

$$\mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j}$$

To show that the quaternions are a division ring, we must be able to find an inverse for each nonzero element. To that end, we observe the identity:

$$(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 + b^2 + c^2 + d^2.$$

Remark 9. Let R be a ring and S a subset of R. Then S is a subring of R if and only if the following conditions are satisfied.

1. $S \neq \emptyset$.
2. $r \cdot s \in S$ for all $r, s \in S$.
3. $r - s \in S$ for all $r, s \in S$.

For example, the ring $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Notice that even though the original ring may have an identity, we do not require that its subring have an identity. We have the following chain of subrings:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Example 10. The set of 2×2-matrices with entries in $\mathbb{R}$ form a ring R, denoted $\mathbb{M}_2(\mathbb{R})$. This ring is $R = \mathbb{M}_2(\mathbb{R})$ is **not a field or an integral domain** because is not commutative. Explicitly we can find matrices like for example

$$M = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$$

that do not admit an inverse. It is **also not an integral domain** since we can get

$$M_1 \cdot M_2 = \begin{pmatrix} 0 & 0 \\ 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & -2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

meaning that $M_1 = \begin{pmatrix} 0 & -2 \\ 0 & 3 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & 0 \\ 3 & 2 \end{pmatrix}$ are zero-divisors in R. Similar calculations can be made for the ring R_n of $n \times n$-matrices with real coefficients.

Example 11. Consider the subset T of upper triangular matrices in R, then T is a subring of R. How do they look like?

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

The multiplication of two upper triangular matrices will again be upper triagular:

$$M_1 \cdot M_2 = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix}.$$