OCTOBER 31 NOTES

1. 7.1: Introduction to rings: basic definitions and examples

Definition 1.1. A **ring** R is a set with two binary operations, $+$ and $\times$ (called *addition* and *multiplication*) such that:

(1) $(R, +)$ is an abelian group, where we denote the identity element by 0 and the inverse of some $a \in R$ by $-a$,
(2) $\times$ is an associative binary operation, and
(3) the *distributive laws* hold: for all $a, b, c \in R$,
$$(a + b) \times c = (a \times c) + (b \times c)$$
and
$$a \times (b + c) = (a \times b) + (a \times c).$$

Definition 1.2. Let R be a ring. R is **commutative** if $\times$ is commutative. R is said to have an **identity** if there exists an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Definition 1.3. Let R be a ring with identity 1 where $1 \neq 0$. If every nonzero element $a \in R$ has a multiplicative inverse, i.e. for all $a \in R$ there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$, then R is called a **division ring**. If R is a commutative division ring, then R is called a **field**.

Example 1.4. (1) $\mathbb{Z}$ is a ring. It is not a division ring or a field.
(2) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings. They are all fields.
(3) $\mathbb{Z}_n$ is a ring with $+ = + \pmod{n}$ and $\times = \times \pmod{n}$. Exercise: it is a field if and only if $n = p$ is prime.
(4) Let $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, \quad i, j, k \in Q_8\}$ with addition defined pointwise:
$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$
and multiplication defined by the distributive law. Then, one can show that $\mathbb{H}$ is a ring, and in fact $\mathbb{H}$ is a division ring. It is not a field because multiplication is not commutative.

Some properties and other definitions:

Proposition 1.5. *Let R be a ring. Then:*

(1) $0a = a0 = 0$ *for all* $a \in R$.
(2) $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$.
(3) $(-a)(-b) = ab$ *for all* $a, b \in R$.
(4) If R has an identity, then it is unique and $-a = (-1)a$.

Definition 1.6. Let R be a ring.

(1) A nonzero element $a \in R$ is called a **zero divisor** if there exists some $b \in R$, $b \neq 0$, such that $ab = 0$ or $ba = 0$. A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has *no* zero divisors.
(2) If R has an identity $1 \neq 0$, an element $u \in R$ is called a **unit** if u has a multiplicative inverse $u^{-1} \in R$. The set of all units in a ring R are by definition a *group under multiplication*, so is called the **group of units** of R and denoted by $R^\times$.

Some remarks:

- A field is a commutative ring F with identity $1 \neq 0$ such that $F^\times = F - \{0\}$.

- A zero divisor in R can *never* be a unit: suppose $a \in R$ such that $ab = 0$ and $a^{-1}a = 1$ for $b, a^{-1} \in R$. Then, $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$, so $b = 0$. Therefore, if a is a unit, there is no nonzero b such that $ab = 0$.

More examples:

Example 1.7. (1) $\mathbb{Z}$ has no zero divisors and $\mathbb{Z}^\times = \{1, -1\}$.
(2) If n is not prime, $\mathbb{Z}_n$ has zero divisors, which cannot be units. Indeed, suppose $n = ab$ for $a, b > 1$. Then, $a, b \in \mathbb{Z}_n$, but $ab = 0 \pmod{n}$, so both a and b are zero divisors.
(3) If $M_n(\mathbb{R})$ is the set of all $n \times n$ matrices with entries in $\mathbb{R}$, then $M_n(\mathbb{R})$ is a ring. For $n > 1$, it has many zero divisors. The group of units is $M_n(\mathbb{R})^\times = GL_n(\mathbb{R})$.

If a ring has no zero divisors/is an integral domain, then we have a cancellation law:

Proposition 1.8. *If $a, b, c \in R$ where R is a ring and a is not a zero divisor such that $ab = ac$, then either $a = 0$ or $b = c$. In particular, if R is an integral domain and $a \neq 0$, then $ab = ac$ implies $a = c$.*

Proof. If $ab = ac$, then $a(b - c) = 0$. Because R has no zero divisors, then either $a = 0$ or $b - c = 0$, i.e. $b = c$. □

Proposition 1.9. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain and let $a \in R$ be a nonzero element. Let $f : R \to R$ be the function $f(x) = ax$. By the cancellation law, this is an injective function, so because R is finite, it is also surjective. Therefore, there exists some element $b \in R$ such that $f(b) = 1$, i.e. $ab = 1$, so $b = a^{-1}$ exists. □

Definition 1.10. Let R be a ring. A **subring** of R is a subgroup of R that is closed under multiplication (i.e. a subset of R that is also a ring).

A perhaps more interesting example of several notions above:

Example 1.11. Let $D \in \mathbb{Q}$ be a rational number that is not a perfect square in $\mathbb{Q}$ (not the square of any rational number).

Let $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}\}$. This is called a **quadratic field.** It is a subring of $\mathbb{C}$ because it is a subgroup of $\mathbb{C}$ and $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D})$, so it is closed under multiplication. (In fact, if $\sqrt{D} \in \mathbb{R}$, it is a subring of $\mathbb{R}$.) It is also commutative and has identity $1 = 1 + 0\sqrt{D})$.

It turns out that $\mathbb{Q}(\sqrt{D})$ is also a field. If $a + b\sqrt{D}$ is a nonzero element, then $a^2 - b^2D \neq 0$ (this would imply that $D = a^2/b^2$ so is a perfect square) which them implies it has a multiplicative inverse given by $\frac{a - b\sqrt{D}}{a^2 - b^2D}$, which can be written as $c + d\sqrt{D}$ for $c, d \in \mathbb{Q}$.

One comment: we will often assume that D is actually a square-free integer, meaning it is not divisible by the square of any prime number. Indeed, if $D = \frac{a}{b} \in \mathbb{Q}$, then $D = \frac{s^2}{b^2}D'$ where $D' = \frac{a}{s^2}b$ where s^2 is the largest perfect square that divides a. If D is not a square and written in lowest form (so $(a, b) = 1$), then D' is an integer that is square-free. Furthermore, $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$ because $\sqrt{D} = \frac{1}{b}\sqrt{D'}$, so $c + d\sqrt{D} = c + \frac{d}{b}\sqrt{D'}$. Therefore, in any example of quadratic field, we can assume without any loss of generality that D is a square-free integer.

2. 7.2: More examples

Definition 2.1. Let R be a commutative ring with identity. The **ring of polynomials in one variable** over R is $R[x]$, where:

$$R(x) = \{a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \mid n \geq 0, a_i \in R\}.$$

Addition and multiplication are defined as the usual addition and multiplication of polynomials using the distributive law.

If $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ and $a_n \neq 0$, then $a_n x^n$ is called the **leading term**, a_n is called the **leading coefficient**, and $p(x)$ has **degree** n. If $a_n = 1$, the polynomial is **monic**.

Example 2.2. The ring R makes a very big difference in the behavior of the polynomials. For instance, if $R = \mathbb{Z}$, then the polynomial equation $x^2 + 1 = 0$ has no solutions. But, if $R = \mathbb{Z}_2$, then $1 \in \mathbb{Z}_2$ is a solution to $x^2 + 1 = 0$ because $1^2 + 1 = 0 \pmod 2$.

If R is an integral domain, the ring $R[x]$ behaves 'as expected.'

Proposition 2.3. *If R is an integral domain and $p(x), q(x)$ are nonzero elements of $R[x]$, then:*

(1) $\deg p(x)q(x) = \deg p(x) + \deg q(x)$,
(2) $R[x]^\times = R^\times$*, and*
(3) $R[x]$ *is an integral domain.*

Proof. Exercise! □

Definition 2.4. Let R be a ring and $n \geq 1$ a positive integer. The **ring of $n \times n$ matrices over R** is $M_n(R)$, the set of all $n \times n$ square matrices with entries in R.

If $n \geq 2$ and R has any nonzero elements, then $M_n(R)$ is not commutative and has zero divisors. If R has an identity 1, then $M_n(R)$ has identity matrix with 1's along the diagonal and 0's elsewhere.

The group of units of $M_n(R)$ (if R has identity) is called the **general linear group** $GL_n(R)$.

Definition 2.5. Let R be a commutative ring with identity $1 \neq 0$ and $G = \{g_1, \ldots, g_n\}$ any finite group. The **group ring** RG is the set

$$RG = \{a_1 g_1 + \cdots + a_n g_n \mid a_i \in R\}.$$

Addition is defined componentwise as for the quaternions and polynomial rings and multiplication is defined using the distributive laws and that $(ag_i)(bg_j) = (ab)g_k$ where $g_k = g_i g_j$.

From this equation, we see that RG is commutative if and only if G is a commutative group.