Lecture 32   Rings and Fields.

**Definition** A **Ring** is a nonempty set \( R \) with two binary operations \( (a, b) \mapsto a + b \) called **addition**, \( (a, b) \mapsto a \cdot b \) called **multiplication**.

Both are maps \( R \times R \to R \) (so \( R \) is closed under the operations). They must also satisfy:

1. \((R, +)\) is an abelian group:
2. Multiplication is associative \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \) \((\forall a, b, c \in R)\)
3. Multiplication distributes over addition: for all \( a, b, c \in R \), \( a \cdot (b + c) = a \cdot b + a \cdot c \) \((\forall a, b, c \in R)\). 

\( \bullet \) That \((R, +)\) be an abelian group means
- Addition is associative and commutative: for all \( a, b, c \in R \), \( a + (b + c) = (a + b) + c \), \( a + b = b + a \).
- There is an identity element for addition; we use \( 0 \) (zero) for this, or \( 0_R \) if it may be ambiguous.
  \((\forall a \in R)\) \( 0 + a = a = a + 0 \)
- There are additive inverses. We use \(-a\) for this: \((\forall a \in R)\) \(-a \) exists and \( a + (-a) = 0 = (-a) + a \)

\( \bullet \) In our definition, a ring is **not required to have a multiplicative identity**. If there is one, we denote it by \( 1 \) or \( 1_R \).

It has the property that \((\forall a \in R)\) \((1 \cdot a = a = a \cdot 1) \).

We call \( R \) a **ring with 1** or **ring with multiplicative identity**.
If \( R \) is a ring with 1, we can ask if multiplicative inverses exist. We write \( a^{-1} \) for an element such that \( a a^{-1} = 1 = a^{-1} a \), if it exists. If \( a^{-1} \) exists, we say \( a \) is invertible or \( a \) is a unit. We write \( R^* = \{ a \in R \mid a^{-1} \text{ exists in } R \} \) for the set of units in \( R \). \( R^* \) is always a group under multiplication.

The multiplication is **not required** to be commutative. If it is \( (\forall a, b \in R, a \cdot b = b \cdot a) \) then we say \( R \) is a **commutative ring**.

A commutative ring with 1 in which every non-zero element is invertible is called a **field**. If \( R \) is a field, then \( R^* = R \setminus \{0\} \).

(We require \( 1 \neq 0 \) for a field, so \( \{0\} \) is not a field)

**Def** Let \( (R, +, \cdot) \) be a ring. A subset \( S \subseteq R \) is called a **subring** if it is closed under \( + \) and \( \cdot \) and those operations make \( S \) into a ring itself.

**Examples:**
- \( \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are fields
- \( \mathbb{Z}_p \) is a field if \( p \) is prime. \( \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} \)
- \( \mathbb{Z} \) is a commutative ring with 1. \( \mathbb{Z}^* = \{ \pm 1 \} \)
- \( \mathbb{Z}_n \) is a commutative ring with 1, not a field if \( n \) is composite
  \( \mathbb{Z}_n^* = \{ [k] \mid \gcd(k, n) = 1 \} \)
- \( n \mathbb{Z} = \{ kn \mid k \in \mathbb{Z} \} \) is a commutative ring, but does not have a multiplicative identity (unless \( n = \pm 1 \))
- \( n \mathbb{Z} \subseteq \mathbb{Z} \) is a subring.
A more exotic ring \( \mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \} \)

It's a subring of \( \mathbb{R} \)

\[
(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}
\]

\[
(a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + ab'\sqrt{2} + a'b\sqrt{2} + b'b(2)\sqrt{2} = q + q\sqrt{2} \in \mathbb{Q}(\sqrt{2})
\]

It contains 0 and additive inverses.

In fact, \( \mathbb{Q}(\sqrt{2}) \) is a field! It has multiplicative inverses.

\[
(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}
\]

if \( a \) and \( b \) are not both 0.

Indeed

\[
\left( \frac{a - b\sqrt{2}}{a^2 - 2b^2} \right)(a + b\sqrt{2}) = \frac{a^2 - (b\sqrt{2})^2}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1
\]

Note: the denominator \( a^2 - 2b^2 \) cannot be zero when \( a, b \in \mathbb{Q} \), unless \( a = b = 0 \). For if \( a^2 - 2b^2 = 0 \), then \( \left( \frac{a}{b} \right)^2 = 2 \). But \( \frac{a}{b} \in \mathbb{Q} \), and \( \sqrt{2} \) is irrational.

You check: \( \mathbb{Q}(i) = \{ a + bi \mid a, b \in \mathbb{Q} \} \leq \mathbb{C} \) is a subfield.

(\( i^2 = -1 \))

General construction: Let \( R \) be a ring, \( S \) any set.

Then \( R^S = \{ f: S \to R \} \), the set of all functions \( S \to R \) is a ring, with operations, for \( f, g \in R^S \)

\[
(f + g)(s) = f(s) + g(s) \quad (fg)(s) = f(s) \cdot g(s)
\]

addition in \( R \)

multiplication in \( R \).
We can also consider functions with some property.

Let $S \subseteq \mathbb{R}^n$ be a subset. Let $C(S, \mathbb{R}) = \{ f : S \rightarrow \mathbb{R} \mid f \text{ is continuous} \}$
then $C(S, \mathbb{R}) \subseteq \mathbb{R}^S$ is a subring.

Instead of continuous functions, we may simply consider polynomials. This can actually be done completely abstractly, for any "coefficient ring" $R.$

Let $R$ be a commutative ring. Polynomials over $R$ in the variable $x$
is the ring
$$R[x] = \left\{ \sum_{i=0}^{N} a_i x^i \mid N \geq 0, \ a_i \in R \text{ for } i = 0, 1, \ldots, N \right\}$$

Note that $x$ is just a symbol (it need not have any interpretation).

The addition is defined to be
$$\sum_{i=0}^{N} a_i x^i + \sum_{j=0}^{M} b_j x^j = \sum_{i=0}^{\max(N,M)} (a_i + b_i) x^i \quad \begin{cases} a_i = 0 \text{ if } i > N \\ b_i = 0 \text{ if } i > M \end{cases}$$

The multiplication is defined to be
$$\left( \sum_{i=0}^{N} a_i x^i \right) \left( \sum_{j=0}^{M} b_j x^j \right) = \sum_{k=0}^{N+M} \left( \sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

If $R$ has 1, so does $R[x].$

Can also consider more variables $R[x, y] \quad R[x, x_2, \ldots, x_n].$