Lecture 23 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 $a,b,c \in R$,
$$a\cdot(b+c) = a\cdot b + a\cdot c \qquad (b+c)\cdot a = b\cdot a + c\cdot a.$$

⊛ That $(R,+)$ be an abelian group means

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

⊛ 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 $aa^{-1} = 1 = a^{-1}a$, if it exists. If a^{-1} exists, we say a is <u>invertible</u> or a is a <u>unit</u>. We write

$R^\times = \{a \in R \mid a^{-1} \text{ exists in } R\}$ for the set of units in R.

$R^\times$ 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 <u>commutative ring</u>.

⊛ A commutative ring with 1 in which every nonzero element is invertible is called a <u>field</u>.
If R is a field, then $R^\times = R \setminus \{0\}$.
(We require $1 \neq 0$ for a field, so $\{0\}$ is not a field)

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

<u>Examples</u>: · $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields
· $\mathbb{Z}_p$ is a field if p is prime. $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{[0]\}$

· $\mathbb{Z}$ is a commutative ring with 1. $\mathbb{Z}^\times = \{1, -1\}$
· $\mathbb{Z}_n$ is a commutative ring with 1, not a field if n is composite
$\mathbb{Z}_n^\times = \{[k] \mid \gcd(k,n) = 1\}$
· $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ 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 $\mathbb{R}$

$$(a+b\sqrt{2}) + (a'+b'\sqrt{2}) = \underbrace{(a+a')}_{\in \mathbb{Q}} + \underbrace{(b+b')}_{\in \mathbb{Q}}\sqrt{2}$$

$$(a+b\sqrt{2})(a'+b'\sqrt{2}) = aa' + ab'\sqrt{2} + a'b\sqrt{2} + bb'\sqrt{2}\sqrt{2}$$
$$= \underbrace{(aa'+2bb')}_{\in \mathbb{Q}} + \underbrace{(ab'+a'b)}_{\in \mathbb{Q}}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

It contains 0 and additive inverses.

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

$$(a+b\sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2} \quad \text{if } a \text{ and } b \text{ are not both } 0.$$

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 <u>cannot be zero</u> 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: $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$ is a subfield.
(subring which is a field). $(i^2=-1)$

<u>General construction</u>: 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 $f,g \in R^S$

$$(f+g)(s) = f(s) \underset{\substack{\uparrow \\ \text{addition in } R}}{+} g(s) \qquad (f\cdot g)(s) = f(s) \underset{\substack{\uparrow \\ \text{multiplication in } R.}}{\cdot} g(s)$$

We can also consider functions with some property.

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

Let R be a commutative ring. Polynomials over R in the variable x is the ring

$$R[x] = \left\{ \sum_{i=0}^{N} a_i x^i \;\middle|\; N \geq 0,\ a_i \in R \text{ for } i=0,1,\dots,N \right\}$$

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

The addition is defined to be

$$\sum_{i=0}^{N} a_i x^i + \sum_{j=0}^{M} b_j x^j = \sum_{i=0}^{\max(N,M)} (a_i + b_i) x^i \quad \left\{ \text{set } \begin{array}{l} a_i = 0 \text{ if } i > N \\ b_i = 0 \text{ if } i > M \end{array} \right.$$

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 $R[x,y]$ $\quad R[x_1, x_2, \dots, x_n]$

Polynomials over a field

Let K be a field $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, \dots)$, and let $K[x]$ be the ring of polynomials in the variable x over K.
A general element $f \in K[x]$ is a polynomial

$$f = \sum_{n=0}^{N} a_n x^n = a_N x^N + a_{N-1} x^{N-1} + \cdots + a_1 x + a_0$$

where the coefficients a_n are elements of K.

Def: The <u>degree of f</u>, $\deg(f)$ is the greatest n such that $a_n \neq 0$. Then a_n is called the <u>leading coefficient</u>

Ex: $f \in \mathbb{R}[x]$ $\quad f = e^2 x^4 + \pi x + 2$:
$\deg(f) = 4$ $\quad$ leading coefficient $= e^2 \in \mathbb{R}$.

Convention: when some terms aren't written, it means the corresponding coefficient is zero: $f = e^2 x^4 + \pi x + 2 = e^2 x^4 + 0 \cdot x^3 + 0 \cdot x^2 + \pi \cdot x + 2$

$a_4 = e^2 \quad a_3 = 0 \quad a_2 = 0 \quad a_1 = \pi \quad a_0 = 2$

At the other extreme, the term a_0 is called the <u>constant term</u>.
We can regard the field K as a subring of $K[x]$ consisting of polynomials that have only a constant term. We write $K \subseteq K[x]$.

The zero polynomial $f = 0$ has no nonzero coefficients, so technically its degree is undefined. But it is useful to make the convention that $\deg(0) = -\infty$.

Proposition: If $f, g \in K[x]$, $f \neq 0$, $g \neq 0$, then

① $\deg(fg) = \deg(f) + \deg(g)$

② $\deg(f+g) \leq \max(\deg(f), \deg(g))$
and equality holds if $\deg(f) \neq \deg(g)$.

Proof of ①: let $f = \sum_{n=0}^{N} a_n x^n$, $g = \sum_{m=0}^{M} b_m x^m$, with $N = \deg(f)$, $M = \deg(g)$

So the leading coefficients are $a_N \neq 0$ and $b_M \neq 0$.

Then
$$fg = \sum_{k=0}^{N+M} \left(\sum_{n=0}^{k} a_n b_{k-n} \right) x^k$$

the $k = N+M$ coefficient $\sum_{n=0}^{N+M} a_n b_{(N-n)+M} = a_N b_M$

since $a_n = 0$ for $n > N$ and $b_{(N-n)+M} = 0$ for $n < N$

in other words, the highest power of x that can appear in fg is x^{N+M}, and the coefficient is $a_N b_M$.

Since $a_N \neq 0$ and $b_M \neq 0$, and K is a field, $a_N b_M \neq 0$.

So $\deg(fg) = N+M = \deg(f) + \deg(g)$

[In any field K, $0 \cdot a = 0$ for all $a \in K$:

Proof: $1 \cdot a = (0+1) \cdot a = 0 \cdot a + 1 \cdot a$ (distributive law)

$a = 0 \cdot a + a$ (multiplicative identity)

$0 = 0 \cdot a$ (since $(K,+)$ is a group, we have cancellation law for addition)

In a field K, If $a \neq 0$ and $b \neq 0$, then $a \cdot b \neq 0$.

Proof: If $a \neq 0$ and $b \neq 0$, but $a \cdot b = 0$, then multiply by b^{-1}:

$$ab b^{-1} = 0 \cdot b^{-1} = 0$$
$$a \cdot 1 = 0$$
$$a = 0 \quad \text{contradiction.}$$

Proof of ②: Exercise.