Rings.

① Factoring (Fermat's Last theorem)

$x^n + y^n = z^n$ $(n \geq 3)$ no nontrivial solutions in $\mathbb{Q}$.

② Modules (finite generated abelian group, Jordan form)

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$. addition and multiplication.

Defn (ring). A ring R is a set with two compositions (binary operations) $+$, $\times$, such that:

① With $+$, R is an abelian group, identity is denoted by 0. inverse of x is $-x$.

② $\times$ is commutative, associative and has identity 1.

③ Distributive law $a(b+c) = ab + ac$.

Subring. subset closed under $+, \times, -$, and contains 1.

Note: non commutative ring
$\times$ is not commutative.
Example: $M_{n\times n}(\mathbb{R})$ matrices.

We use "ring" to mean "commutative ring"

Zero Ring $R = \{0\}$.

Prop: If $1 = 0$, then $R = \{0\}$.

Prop: $(0+0)a = 0a + 0a = 0a$

so $0 \cdot a = 0$.

$(-b) \cdot a = -ba$.

Let $n = \underbrace{1+1+\cdots+1}_{n}$ in R.

then $n \cdot a = (1+1+\cdots+1)a = \underbrace{a+\cdots+a}_{n}$.

unit   an element that has a multiplicative inverse.

$\mathbb{Z}$. units $\{\pm 1\}$.

$\mathbb{R}$ units $\mathbb{R} - \{0\}$

Polynomial ring.

R ring.

$f(x) = a_n x^n + a_{n-1} x^{n+1} + \cdots + a_0$.

(formal polynomial)

x^i monomial

$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$

$f = g$ iff $m = n$, $a_i = b_i$

$\left(\prod_{i=0}^{n} R\right) \ni (a_0 \cdots a_n, a_{n+1} \cdots -)$

finitely many non-zero elements.

First non-zero element a_n is leading coefficient.

monic polynomial has leading coefficient equal to 1

$$f+g = (a_0+b_0)+(a_1+b_1)x+\cdots$$

$$f\cdot g = a_0b_0 + (a_1b_0+a_0b_1)x + (a_1b_1+a_2b_0+a_0b_2)x^2 + \cdots$$

Division with Remainder.

$$g(x) = f(x)q(x)+r(x). \quad \deg r < \deg f.$$

Prop (DWR) Division with remainder can be done if leading coefficient of f is a unit.

Non Example: $g(x) = x^2+1$, $f(x) = 2x+1$ in $\mathbb{Z}[x]$.

(Fields) $R - \{0\}$ are all units, $R \neq \{0\}$.

Example: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, p prime.

$\mathbb{Z}/p\mathbb{Z}$ is a field because

(Fermat little theorem) (FLT)

$a \neq 0$, $a^{p-1} \equiv 1 \pmod{p}$.

Proof for FLT relies on the following cancellation property

If $a \neq 0$, $ab = ac \Rightarrow b = c$

(or equivalently, non existence of zero divisor)

Defn of zero divisor.

If $ab = 0$, $a \neq 0$, $b \neq 0$. Both a, b are zero divisor.

Zero divisor can not be units. If a has an inverse

$ab = 0 \Rightarrow a^{-1} \cdot a \cdot b = 0 \Rightarrow b = 0$.

If there is no zero divisor, then

If $ab = ac$, $a \neq 0$

$\Rightarrow$ $a(b-c)=0 \Rightarrow b-c=0 \Rightarrow b=c$.

$R=\mathbb{Z}/p\mathbb{Z}$ satisfies this property.

This means the map $m_a: R \to R$.
$b \mapsto ab$

is injective.

Since R is finite set.

m_a is also surjective.

So 1 has an preimage.

so $\exists b$. s.t. $ab=1$.

Choose all the nonzero elements.

$b_1, \cdots, b_{p-1}$.

$m(a)$: $ab_1, \cdots, ab_{p-1}$. are also all the non zero elements.

$b_1 b_2 \cdots b_{p-1} = ab_1 \cdot ab_2 \cdots ab_{p-1}$

$\Rightarrow (b_1 \cdots b_{p-1}) = a^{p-1} \cdot (b_1 \cdots b_{p-1})$

$\Rightarrow a^{p-1} = 1$ in R