$\mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{ [a]_n \mid \gcd(a,n) = 1 \}$.

- Euler $\phi$-function,

  $\phi(n) := \left| \{ a \mid 1 \leq a \leq n, \gcd(a,n) = 1 \} \right|$.

- $|\mathbb{Z}_n^*| = \phi(n)$.

- $c_n : \mathbb{Z} \to \mathbb{Z}_n$, $c_n(a) = [a]_n$ is a ring homomorphism, and $\ker c_n = n\mathbb{Z}$.

- $\mathbb{Z}_n$ is a field $\iff$ $\mathbb{Z}_n$ is an integral domain $\iff$ $n$ is prime.

(Chinese Remainder Theorem) If $\gcd(m,n) = 1$, then

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}.$$  

- If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m) \phi(n)$.

- If $p$ is prime, then $\phi(p^k) = p^k - p^{k-1}$.

$\mathbb{Z}_n$ was used to introduce rings, units, fields, integral domains, ring homomorphisms, kernel, and ring isomorphisms.
Characteristic

\[ \text{Char}(R) = \text{smallest positive integer } n \text{ such that } nx = 0 \text{ for all } x \in R \]

if there is no such positive integer, \( \text{Char}(R) = 0 \).

\( R \) unital \( \Rightarrow \text{Char}(R) = \begin{cases} \text{the additive order of } 1 \text{ if finite} \\ 0 \text{ otherwise} \end{cases} \)

Suppose \( R_1, \ldots, R_m \) are unital rings and \( \text{Char}(R_i) < \infty \). Then \( \text{Char}(R_1 \times \cdots \times R_m) = \text{l.c.m.} (\text{Char}(R_1), \ldots, \text{Char}(R_m)) \).

If \( D \) is an integral domain, then \( \text{Char}(D) \) is either 0 or a prime.

Integral domain

- Unital commutative non-trivial without zero-divisors.
- Cancellation law.
- Field \( \Rightarrow \text{integral domain} \). Converse is not true in general.
- Finite integral domain \( \Rightarrow \text{Field} \).
- Any integral domain has a field of fractions.
Summary

Suppose \( D \) is an integral domain. Then we constructed

\[
\mathbb{Q}(D) = \{ \frac{a}{b} | a \in D, b \in D \setminus \{0\} \}.
\]

① \( \mathbb{Q}(D) \) is a field.

② \( \varphi: D \rightarrow \mathbb{Q}(D) \), \( \varphi(a) = \frac{a}{1} \) is an injective ring homomorphism.

Suppose \( \Theta: D \rightarrow F \) is an injective ring homomorphism and \( F \) is a field. Then \( \Theta: \mathbb{Q}(D) \rightarrow F \),

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

is a well-defined injective ring homomorphism.

We used this property to show \( \mathbb{Q}([i]) \cong \mathbb{Q}[i] \).

Step 1. \( \mathbb{Q}[i] \) is a field.

Step 2. Get \( \Theta \) using the universal property.

Step 3. Show \( \Theta \) is surjective.
Ring of polynomials

1. If $D$ is an integral domain, then
   \[ \forall f, g \in D[x], \quad \deg (fg) = \deg f + \deg g. \]

2. If $D$ is an integral domain, then $D[\mathbb{x}]$ is an integral domain.

3. If $D$ is an integral domain, then $D[\mathbb{x}]^x = D$.

Polynomial vs. functions. Based on Fermat’s little theorem

If $p$ is prime, $\forall a \in \mathbb{Z}_p, \quad a^p = a$; but $x^p \neq x$ as two polynomials.

Evaluation map. $F \subseteq E$ and $\alpha \in E$

\[ \phi_\alpha : F[\mathbb{x}] \rightarrow E, \quad \phi_\alpha (g(x)) = g(\alpha) \quad \text{is a ring hom}. \]

\[ \ker (\phi_\alpha) = \{ g(x) \in F[\mathbb{x}] | g(\alpha) = 0 \}. \]

Long Division; existence. $R$: unital commutative

$f, g \in R[\mathbb{x}]$, the leading coeff. of $g$ is a unit $\implies$

\exists q, r \in R[\mathbb{x}], \begin{align*}
1 & f(x) = g(x)q(x) + r(x) \quad (2) \quad \deg r < \deg g.
\end{align*}
Long division; uniqueness. Suppose $D$ is an integral domain. $\forall f, g \in D[x]$, leading coeff. of $D$ is a unit. Then there are unique $q, r \in D[x]$ s.t.

1. $f(x) = q(x)q(x) + r(x)$
2. $\deg r < \deg q$.

Factor Theorem. Suppose $R$ is a unital commutative ring; $f(x) \in R[x], a \in R$. Then

$$f(a) = 0 \iff \exists q(x) \in R[x], f(x) = (x-a)q(x).$$

Generalized Factor Theorem. Suppose $D$ is an integral domain; $f(x) \in D[x]$. If $f(a_1) = \cdots = f(a_m) = 0$ and $a_i \neq a_j$ for $i \neq j$, then $\exists q(x) \in D[x]$ s.t.

$$f(x) = (x-a_1) \cdots (x-a_m) q(x).$$

This was used to show $\sum_{i=0}^{p-2} x^i = x(x-1) \cdots (x-(p-1))$ in $\mathbb{Z}_p[x]$.

We used this to prove Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$ ($p$ is prime.) Later this was extended to all finite fields.
Recalled binomial expansion \((x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\)

where \(\binom{n}{i} = \frac{n!}{i! (n-i)!}\). Used this to show that
if \(\text{Char}(R) = p\) is prime, then
\[
F_p : R \rightarrow R, \quad F_p(a) = a^p
\]
is a ring homomorphism.
(This was an alternative way of proving Fermat’s little theorem.)

**Algebraic numbers**

\(\alpha \in \mathbb{C}\) is called algebraic if \(\exists g(\alpha) \in \mathbb{Q}[x] \setminus \{0\}\), \(g(\alpha) = 0\). Alternatively if \(\ker(\phi_\alpha) \neq 0\).

To understand \(\ker(\phi_\alpha)\) we started the study of

**Ideals and Factor rings**. \(R: \text{commutative}\).

\(\emptyset \neq I \subseteq R\) is called an ideal if

1. \(\forall x, y \in I, \ x - y \in I\),
2. \(\forall x \in I, \ \forall r \in R, \ rx \in I\).
If $I \triangleleft R$, then we constructed the factor ring $R/I$. and showed $\pi : R \to R/I$, $\pi(r) = r + I$ is an onto ring homomorphism and $\ker(\pi) = I$. The 1st Isomorphism Theorem.

Suppose $f : R \to S$ is a ring homomorphism. Then

1) $\ker f \triangleleft R$, $\text{Im}(f) \subseteq S$ is a subring.

2) $\overline{f} : R/\ker f \to \text{Im}(f)$, $\overline{f}(r + \ker f) = f(r)$ is a well-defined ring homomorphism.

Ideals generated by $a_1, \ldots, a_n$; principal ideals; PID. The smallest ideal that contains $a_1, \ldots, a_n$ is denoted by $\langle a_1, \ldots, a_n \rangle$ and it is

$$\{ \sum r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots, r_n \in R \}$$

when $R$ is a unital commutative ring.

$\langle a \rangle = Ra$ is called a principal ideal.
An integral domain \( D \) is called a Principal Ideal Domain (PID) if all of its ideals are principal.

**Theorem** \( \mathbb{Z} \) and \( F[x] \) are PIDs if \( F \) is a field.

**Theorems on algebraic numbers** \( \alpha \in \mathbb{C} \) algebraic.

(Minimal polynomial). \( \exists! \) monic irreducible \( m_\alpha(x) \in \mathbb{Q}[x] \) s.t.

\[
\ker \phi_\alpha = < m_\alpha(x) >.
\]

- \( f(x) \in \mathbb{Q}[x] \) and \( f(\alpha) = 0 \) implies \( m_\alpha(\alpha) | f(x) \).

- If \( p(x) \in \mathbb{Q}[x] \) is monic and irreducible and \( p(\alpha) = 0 \), then \( m_\alpha(x) = p(x) \).

\( \mathbb{Q}[\alpha] := \text{Im} \phi_\alpha \) Suppose \( \deg m_\alpha = d \).

- \( \mathbb{Q}[\alpha] \) is the \( \mathbb{Q} \)-span of \( 1, \alpha, \ldots, \alpha^{d-1} \); that means

\[
\mathbb{Q}[\alpha] = \mathbb{Q} \alpha = \sum_{i=0}^{d-1} a_i \alpha^i, \quad a_i \in \mathbb{Q}.
\]

- \( 1, \alpha, \ldots, \alpha^{d-1} \) are \( \mathbb{Q} \)-linearly independent; that means

\[
b_0 + b_1 \alpha + \cdots + b_{d-1} \alpha^{d-1} = c_0 + c_1 \alpha + \cdots + c_{d-1} \alpha^{d-1} \Rightarrow b_i = c_i, \quad b_i, c_i \in \mathbb{Q}.
\]
. \( \mathbb{Q}[\alpha] \cong \mathbb{Q}[\alpha]/\langle m_\alpha(x) \rangle \) (using the 1st isomorphism theorem.)

. \( \mathbb{Q}[\alpha] \) is a field.

To prove the last item we studied maximal ideals.

**Maximal and Prime Ideals**

\( I \triangleleft R \) is called a maximal ideal if

1. \( I \) is a proper ideal; that means \( I \neq R \),
2. \( I \neq J \implies J = R. \)

\[ J \triangleleft R \]

**Theorem.** \( I \) is maximal \( \iff R/_{I} \) is a field.

\( I \triangleleft R \) is called a prime ideal if

1. \( I \) is a proper ideal;
2. \( ab \in I \implies a \in I \) or \( b \in I \).

**Theorem.** \( I \) is prime \( \iff R/_{I} \) is an integral domain.

. \( I \) maximal \( \implies I \) prime.

. Suppose \( R/_{I} \) is finite; \( I \) prime \( \iff I \) maximal.
Theorem. Suppose $D$ is a PID and $0 \neq a \in D$.

Then $\langle a \rangle$ is maximal $\iff$ $a$ is irreducible.

($\mathbb{Q}[x] : \text{PID}; m_a(x) : \text{irred.}; \mathbb{Q}[x] \sim \mathbb{Q}[x]/\langle m_a(x) \rangle$

and the above theorem imply $\mathbb{Q}[x]$ is a field.)

Theorem. $D$: PID and $0 \neq I \subset D$. Then

$I$ prime $\iff I$ maximal.

To show an integral domain $D$ is not a PID it is enough to find $a \in D$ s.t.

(1) $a$ is irreducible (2) $\langle a \rangle$ is not prime.

We used the above to show $\mathbb{Z}[\sqrt{-10}]$ is not a PID.

We used $N: \mathbb{Z}[\sqrt{-10}] \to \mathbb{Z}$, $N(a + \sqrt{-10} \cdot b) := a^2 + 10b^2$

to show $\sqrt{-10}$ is irreducible. Then we showed

$\langle \sqrt{-10} \rangle$ is not prime;

$2 \cdot 5 \in \langle \sqrt{-10} \rangle$ and $2 \notin \langle \sqrt{-10} \rangle$, $5 \notin \langle \sqrt{-10} \rangle$. 
We defined a **Unique Factorization Domain** (UFD): an integral domain such that

1. \( \forall a \in D \text{ and } a \neq 0, a \in D^\times \), \( a \) can be written as a product of irreducibles (Existence).

2. If \( p_i \)'s and \( q_j \)'s are irreducible and
   \[ p_1 \cdots p_n = q_1 \cdots q_m, \text{ then } n = m \text{ and } \]
   \[ p_i = u_i q_{\sigma_i} \quad \text{for some } u_i \in D^\times \text{ and a permutation } \sigma. \text{ (Uniqueness).} \]

**Theorem.** In a PID the uniqueness part holds.

(Proof of the above theorem was based on induction and the following result:

\( p, q_1, \ldots, q_m \text{ irred. } p \mid q_1 \cdots q_m \) implies 

\[ \exists i \text{ and } u \in D^\times \text{ s.t. } p = u q_i. \]

**Theorem.** \( \mathbb{F}[x] \text{ is a UFD.} \)

(\( \mathbb{Z} \text{ is a UFD.} \))
Finding a zero in a larger field.

Theorem. Suppose $F$ is a field and $f(x) \in F[x]$ is a manic irreducible polynomial. Then there are $E$ and $\alpha \in E$ s.t.

1. $E$ is a field and $\exists \ i : F \rightarrow E$ an injective ring homomorphism (we say $E$ is a field extension of $F$.)

2. $f(\alpha) = 0$ (It is more formal to write $i(f)(\alpha) = 0$ where

\[ i(a_0 + a_1 x + \ldots + a_d x^d) = i(a_0) + i(a_1) x + \ldots + i(a_d) x^d. \]

3. $E = \left\{ \sum b_0 + b_1 x + \ldots + b_{d-1} x^{d-1} : b_i \in F \right\}$ where $d = \deg f$.

4. $c_0 + c_1 x + \ldots + c_{d-1} x^{d-1} = c'_0 + c'_1 x + \ldots + c'_{d-1} x^{d-1}$

$c_i, c'_i \in F \quad \Rightarrow \quad c_i = c'_i \quad \forall i$. 
Applying the previous theorem repeatedly we got:

**Theorem.** Suppose $F$ is a field and $f(x) \in F[x] \setminus \{0\}$.

Then $\exists$ a field $E$ and $\alpha_1, \ldots, \alpha_n \in E$ s.t.

$$f(x) = c \ (x-\alpha_1) \ (x-\alpha_2) \ldots \ (x-\alpha_n)$$

for some $c \in F$.

**Finite fields**

**Theorem.** Suppose $f(x) \in \mathbb{Z}_p[x]$ is monic and irreducible, and $\deg f = d$. Then there are $E$ and $\alpha \in E$ s.t.

1. $E$ is a field, $\mathbb{Z}_p \subseteq E$;
2. $|E| = p^d$.
3. $f(\alpha) = 0$.
4. $f(x) \mid x^{p^d} - x$.

**Theorem.** Suppose $p$ is prime and $d$ is a positive
integer; then \( \exists \) a finite field \( \mathbb{F}_p^d \) s.t.
\[ |\mathbb{F}_p^d| = p^d.\]

**Theorem.** \( \chi^d - \chi = \prod_{\alpha \in \mathbb{F}_p^d} (\chi - \alpha) \).

(We recalled that in a finite group \( G \) of order \( n \) we have \( g^n = 1 \) \( \forall g \in G \); used this to show
\[ \forall \alpha \in \mathbb{F}_p^n, \quad \alpha^n = \alpha. \])