Def. A ring $R$ is an abelian gp (under $+$) equipped with a multiplication, i.e. a binary operation $\cdot$. 

1) $a \cdot (b+c) = ab + ac$

2) $(a+b) \cdot c = ba + ca$

3) $(ab) \cdot c = a \cdot (bc)$

Blanket assumption: All rings are commutative ($ab = ba$) and contain 1 unless otherwise stated.

Def. A field $F$ is a ring in which each nonzero element has
a multiplicative inverse, i.e. 
\( ha = 0 \) \( \exists a^{-1} \) s.t. \( a^{-1} \cdot a = 1 \)

**Def:** An integral domain \( D \) is a ring in which \( a \cdot b = 0 \) \( \Rightarrow a = 0 \) or \( b = 0 \).

**Examples:** \( \mathbb{Z}/6 = \text{integers mod } 6 \)
\[ = \{0, 1, 2, 3, 4, 5\} \]
is not an ID because \( 2 \cdot 3 = 0 \)

**Def:** If \( a \cdot b = 0 \) with \( a, b \neq 0 \), then \( a \) and \( b \) are zero divisors.

**Examples:** \( \mathbb{Z} \) is a domain. 
Any field \( \mathbb{F} \) is a domain.
If \( a, b \neq 0 \in F \) and \( a \cdot b = 0 \)

then \( a^{-1} \cdot a \cdot b = b = a^{-1} \cdot 0 = 0 \)

CONTRADICTION. QED

Thm 6.3.14. Every finite domain \( D \) is a field.

Proof: Let \( a \neq 0 \in D \). Let \( n = \#D \)

Consider the set \( S \) of all non-zero elements of \( D \)

\[ S = \{ x \in D : x \neq 0 \} \quad n - 1 \text{ elements} \]

as \( S = \{ a x \in D : x \neq 0 \} \)

Note: \( 0 \notin S \). If \( a \neq 0 \) has \( n - 1 \) distinct elements, one of them must be 1,

so \( ax = 1 \) for some \( x \in D \)
and \( x = a^{-1} \).

**Assume** \( ax_1 = ax_2 \) for \( x_1 \neq x_2 \)

\[
a x_1 - a x_2 = 0
\]

\[
a (x_1 - x_2) = 0 \quad \text{so} \quad a = 0 \quad \text{on} \quad x_1 - x_2 = 0
\]

**CONTRADICTION**

Hence, \( D \) is a field. QED

Later we will see that for each prime \( p \) and each integer \( n \geq 0 \), there is a field with \( p^n \) elements, unique up to isomorphism.

Each finite \( D \) is one of these.

E.g., \( \mathbb{Z}/p \) is a field for each prime \( p \).

E.g., \( \mathbb{Z}/691 \).
Def: An ideal $I$ in a ring $R$ is a subgroup under $+$ such that if $a \in I$ and $x \in R$ then $ax \in I$.

This is a stronger condition than being a subring.

Example:
1. $R = \mathbb{Q}$, rational # 5
   $I = 2\mathbb{Z}$ = integers
   This is a subring but not an ideal.

2. $R = \mathbb{Z}$
   $I = \{4n : n \in \mathbb{Z}\}$ = $4\mathbb{Z}$ = (4)

3. $R$ any ring and $x \in R$
   $I = \{ax : a \in R\mathbb{Z}\}$ is an ideal
   $= (x) = \text{ideal generated by } x.$
This is called a principal ideal.

④ $(0) = \text{zero ideal} = \{0\}$

⑤ $(1) = \text{unit ideal} = R$

⑥ $R = \mathbb{Z}[x] = \text{polynomials in} \ x \ \text{with integer coefficients}$

$I = (2, x) = \text{ideal generated by} \ 2 \ \text{and} \ x$

$$= \left\{ 2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x] \right\}$$

$$= \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_0 \ \text{even} \right\}$$

$I$ contains the ideals $(2)$ and $(x)$.

$2 \in I \ \text{but not in} \ (x)$

$x \in I \ \text{but not in} \ (2)$
I is not a principal ideal.

Then in $\mathbb{Z}$ every ideal is principal.

e.g. $I=(5,7) \implies 7-5=2 \implies 4 \in I$

$5-4=1 \in I$

$I=(15,35)$

$2 \cdot 15 = 30 \in I$

$35-30=5 \in I$

$I=(5)$

In general $(m,n) = (\gcd(m,n))$

This can always be done.

Euclidean algorithm will be discussed later.

Def: A principal ideal domain (PID)
is an integral domain in which every ideal is principal.

e.g. \( \mathbb{Z} \) is a PID
\( \mathbb{Z}[x] \) is not a PID.

Any subring of \( \mathbb{Q} \) is a PID

e.g. \( \sum \frac{n}{15^n} \)

is a subring of \( \mathbb{Q} \) and a PID.

Let \( S \) be a set of primes.

\( \mathbb{Z}[S^{-1}] = \left\{ \frac{a}{b} : a \in \mathbb{Z}, \ b \text{ is a product of powers of primes in } S \right\} \)

Any subring of \( \mathbb{Q} \) is one of these.
Let \( R \rightarrow S \) be a ring homomorphism.

What about \( \ker \phi \)?

\[
\ker \phi = \{ x \in R : \phi(x) = 0 \} \supset
\]

Claim it is an ideal.

If \( x, y \in \ker \phi \) then

\[
\phi(x + y) = \phi(x) + \phi(y) = 0 + 0 = 0
\]

\( \Rightarrow \) \( x + y \in \ker \phi \). Hence \( \ker \phi \) is a subgroup.

Let \( a \in R \) and \( x \in \ker \phi \)

\[
\phi(ax) = \phi(a) \phi(x) = \phi(a) 0 = 0
\]

Hence \( ax \in \ker \phi \Rightarrow \ker \phi \) is an ideal.

Conversely, every ideal \( I \) is the kernel of some ring hom.
Consider the group \( R/I \). It inherits a multiplication from \( R \) given \( a, b \in R/I \). Choose \( a, b \) after mapping to \( a \) and \( b \) under \( R \to R/I \), a group homomorphism.

Claim we can define \( ab = \phi(ab) \).

We need to show this is independent of the choice of \( a \) and \( b \).

Suppose \( a' \) and \( b' \) are different preimages (under \( \phi \)) of \( a \) and \( b \).

Let \( c = a' - a \) and \( d = b' - b \).

\[
\begin{align*}
    a' &= a + c \\
    b' &= b + d
\end{align*}
\]
c, d ∈ \text{ker } \phi = I
\phi(a', b') = \phi((a+c)(b+d))
= \phi(ab + cb + ad + cd)
= \phi(ab) + \phi(cb) + \phi(ad) + \phi(cd)
= \phi(ab)

This means the product in \( R/I \) is well defined. It is independent of the choice of \( a \) and \( b \).

**Def.** An ideal \( I \) is **prime** if
\[ ab \in I \Rightarrow a \in I \text{ or } b \in I. \]
An ideal \( I \subset R \) is **maximal** if
The only bigger ideal is \( R \).

\[ \text{e.g. } R = \mathbb{Z}[x] \quad I_1 = (2) \quad \text{prime ideals} \]

\[ I_2 = (x) \]

But neither is maximal. Both are contained in \((2, x)\).

**Thm 7.2.27** Let \( I \) be an ideal in \( R \).

i) \( I \) is prime \( \iff \) \( R/I \) is an integral domain

ii) \( I \) is maximal \( \iff \) \( R/I \) is a field.

**Recitation**

Monday 6:30 Money 502