ϕ and φ are the same letter (phi)
\phi   \varphi   in $\TeX$.

Dictionary:

numbers (or polynomials)	ideals in a comm. ring.
$\gcd(a,b)$	$I+J$
$\operatorname{lcm}(a,b)$	$I\cap J$
$a\cdot b$	$I\cdot J$
$a \mid b$	$J\subset I$
$a = \text{unit}\cdot b$	$I=J$
$a = \text{unit}$	$I=\langle 1\rangle$
p is prime	...?

$\langle 1\rangle = R$

The statement
If $K\subset I$ and $K\subset J$ then $K\subset I\cap J$.
generalizes
If $a\mid c$ and $b\mid c$ then $\operatorname{lcm}(a,b)\mid c$.

Prime Ideals

Euclid's lemma: if $p\mid ab$ then $p\mid a$ or $p\mid b$.
(for prime numbers p)

Def: Let R be a commutative ring.
An ideal $P\subsetneq R$ is prime if
$\forall a,b\in R$, $ab\in P$ implies $a\in P$ or $b\in P$.

Remark Might have wanted the def. to be
$\forall$ ideals $I, J \subset R$, $IJ \subset P$ implies $I \subset P$ or $J \subset P$.
Turns out this is equivalent to def. above
but it's harder to check.

Examples: $\langle 3 \rangle \subset \mathbb{Z}$ is prime. $\langle 6 \rangle \subset \mathbb{Z}$ is not.

$\langle x^2+1 \rangle \subset \mathbb{R}[x]$ is prime bec. x^2+1 is irreducible in $\mathbb{R}[x]$

$\langle x^2+1 \rangle \subset \mathbb{C}[x]$ is not prime
because $(x+i)(x-i) \in \langle x^2+1 \rangle$
but $x+i$ and $x-i \notin \langle x^2+1 \rangle$

not the same set!

In $\mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

the ideal $\langle 3 \rangle$ is not prime,

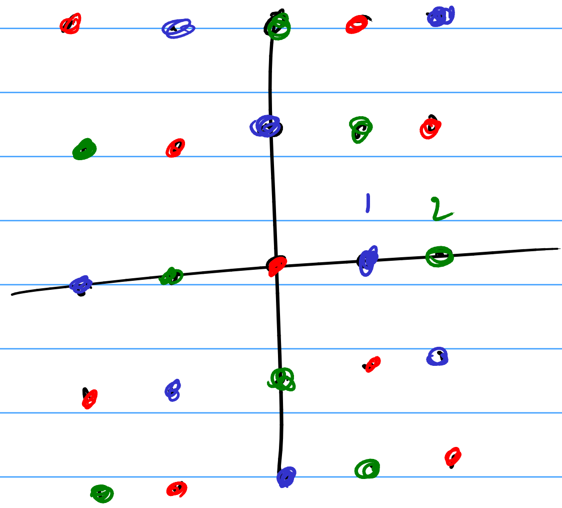
because $(1+\sqrt{-5})(1-\sqrt{-5}) \in \langle 3 \rangle$

but $1+\sqrt{-5}$ and $1-\sqrt{-5} \notin \langle 3 \rangle$ as we've seen.

Let $K = \langle 3, 1-\sqrt{-5} \rangle \subset \mathbb{Z}[\sqrt{-5}]$ related to recent homework.

I claim K is prime.

$K = \langle 3, 1-\sqrt{-5} \rangle \subset \mathbb{Z}[\sqrt{-5}]$



K is the kernel of the homomorphism

$\phi : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_3$

$a + b\sqrt{-5} \longmapsto \bar{a} + \bar{b}$

red $\equiv 0 \pmod K$

blue $\equiv 1 \pmod K$

green $\equiv 2 \pmod K$

proof that K is prime:

let $z, w \in \mathbb{Z}[\sqrt{-5}]$

if $z \cdot w \in K$

then $\phi(zw) = \bar{0}$ in $\mathbb{Z}_3$

So $\phi(z) \cdot \phi(w) = \bar{0}$ in $\mathbb{Z}_3$

so $\phi(z) = \bar{0}$ or $\phi(w) = 0$ because $\mathbb{Z}_3$ is an integral domain

so $z \in K$ or $w \in K$.

(and that's what it means for K to be prime)

Last remark: $R/K = \{ \bar{0}, \bar{1}, \bar{2} \}$

it looks like R/K "is" $\mathbb{Z}_3$

the map $\phi : R \longrightarrow \mathbb{Z}_3$ tells how to match them up.

First iso thm: $\phi : R \longrightarrow S$ surjective hom.

gives an iso $R/\ker\phi \cong S$

(talk next week)