Next term: Continue thru ch. 7 of Shifrin

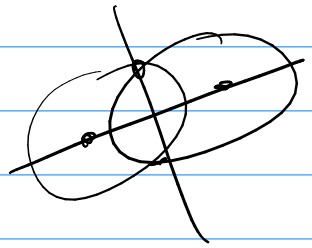
Finish Ch. 4: more on ideals, prime ideals, quotient rings...

Gaussian integers $\mathbb{Z}[i]$
application: Fermat's Xmas thm:
a prime p can be written as x^2+y^2
iff $p=2$ or $p \equiv 1 \pmod 4$
$2 = 1^2+1^2$ $5 = 1^2+2^2$ $13 = 2^2+3^2$
but $3, 7, 11, \ldots$ can't do it

---

field extensions. — polynomials factoring / splitting when we enlarge the field

straightedge + compass constructions:
can't trisect the angle,
duplicate the cube,
square the circle.



---

main thing: group theory
symmetries of polygons + polyhedra
groups acting as symmetries of different sets.
analyze tic-tac-toe using orbits of a group action...

---

taste of Galois theory — symmetry groups of fields
can solve quadratic, cubic, quartic equations
by taking $\sqrt{}$, $\sqrt[3]{}$, $\sqrt[4]{}$, but not quintics!

Last Time: kernels of homomorphisms, ideals generated by elts. of your r.ing.

Def: a subset $I \subset R$ is an <u>ideal</u> if $\forall a, b \in I$, $a+b \in I$ and $\forall r \in R$, $a \in I$, $ra \in I$

For $a \in R$, the (principal) ideal $\langle a \rangle = \{ ra \mid r \in R \}$

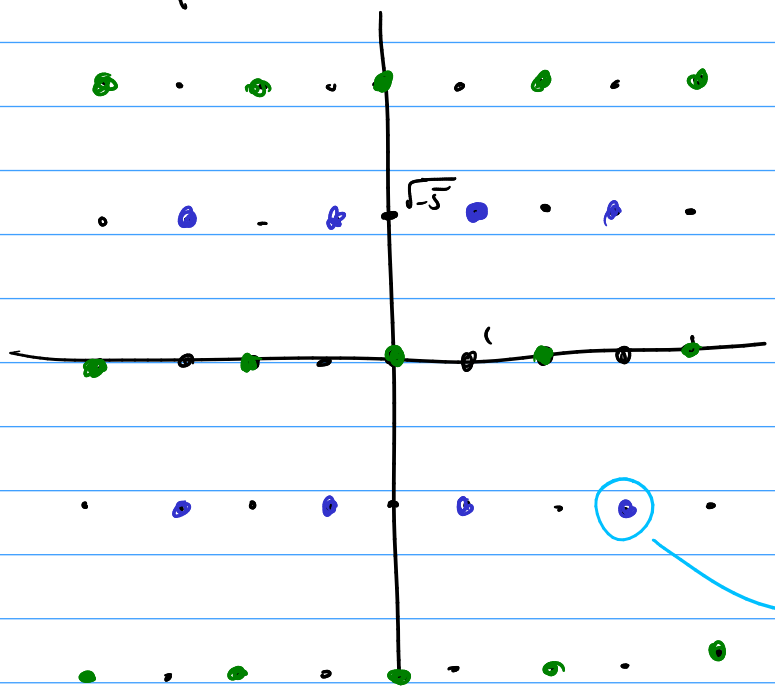
For $a, b \in R$, they generate $\langle a, b \rangle = \{ ra + sb \mid r, s \in R \}$

e.g. in $\mathbb{Z}$, $\langle 6, 10 \rangle = \langle 2 \rangle$

Prop: if $\varphi : R \to S$ is a homomorphism then $\ker \varphi \subset R$ is an ideal.

$i\sqrt{5}$ or $\sqrt{5}\,i$

Another example: $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$



green + $(1+\sqrt{-5})$

if $\bar{a} + \bar{b} = \bar{0}$ in $\mathbb{Z}_2$
then a, b both even
or a, b both odd

$3 - \sqrt{-5}$

$\varphi(3 - \sqrt{-5}) = \bar{3} + (\bar{-1}) = \bar{2} = \bar{0}$

$\varphi : R \longrightarrow \mathbb{Z}_2 \qquad \varphi(a + b\sqrt{-5}) = \bar{a} + \bar{b} \in \mathbb{Z}_2$

check: it's a homomorphism.

what does $\ker \varphi$ look like?

$\varphi(2) = 0$, so $2 \in \ker \varphi$, so $2z \in \ker \varphi \quad \forall z \in R$

$\langle 2 \rangle \subset \ker \varphi$

$\varphi(1 + \sqrt{-5}) = \bar{1} + \bar{1} = \bar{2} = \bar{0}$

so any mult. of $1 + \sqrt{-5}$ is in $\ker \varphi$

also any mult of 2 + any mult. of $1 + \sqrt{-5} \in \ker \varphi$

$\langle 2, 1 + \sqrt{-5} \rangle \subset \ker \varphi$

now we've got all of $\ker \varphi$. $\langle 2, 1 + \sqrt{-5} \rangle = \ker \varphi$.

ask: is $\langle 2, 1 + \sqrt{-5} \rangle$ secretly principal?

is it $\langle z \rangle$ for one $z \in R$? no: worksheet.