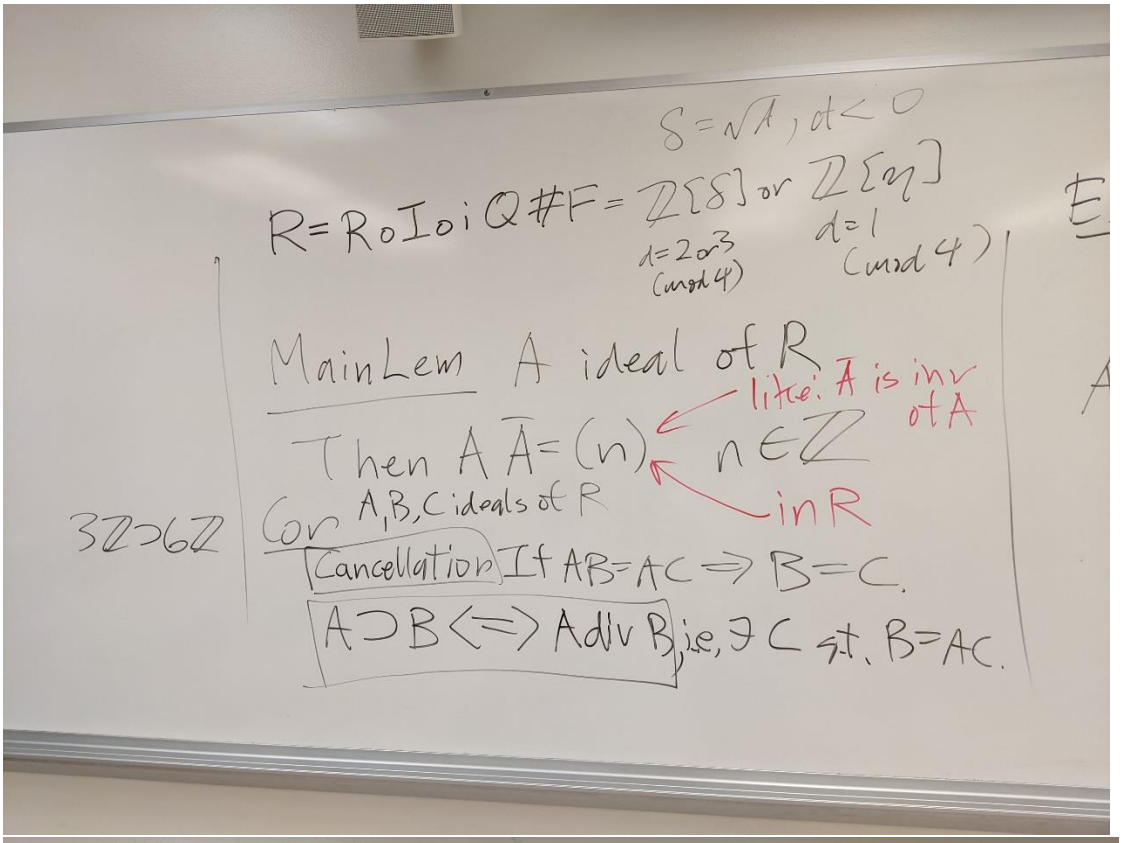
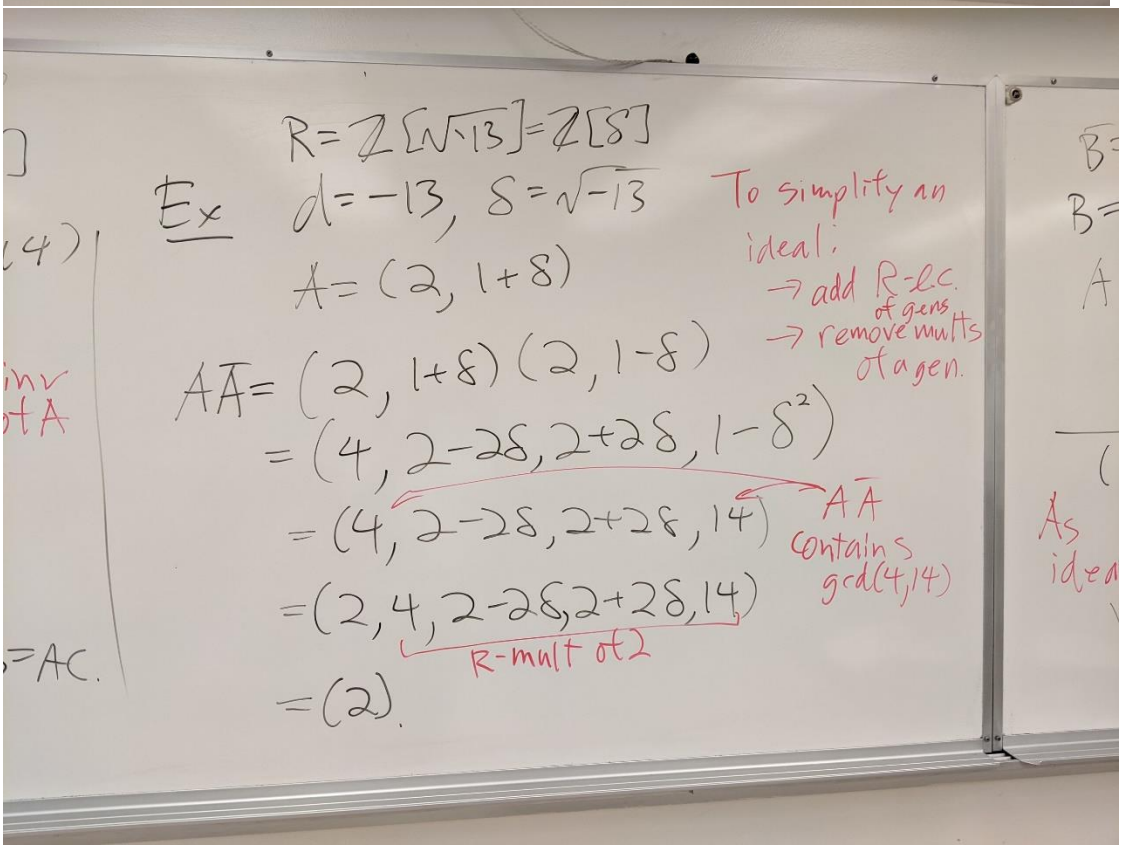
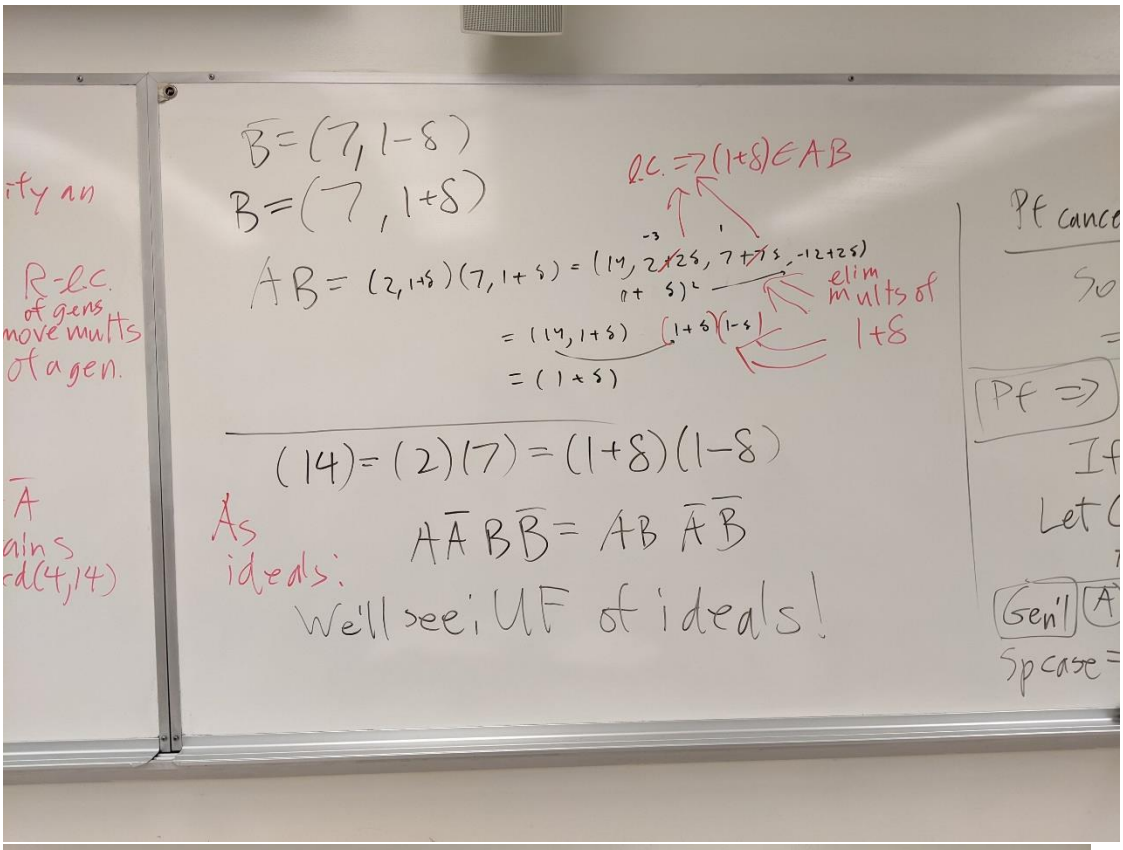
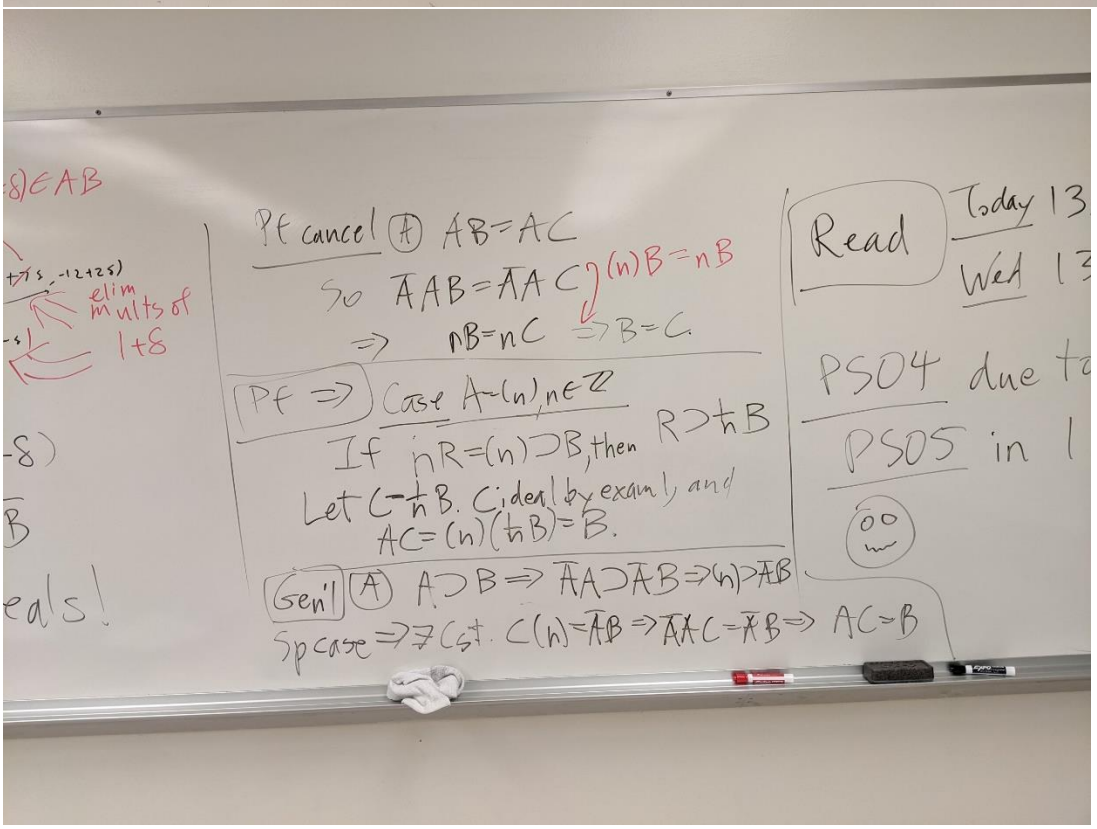
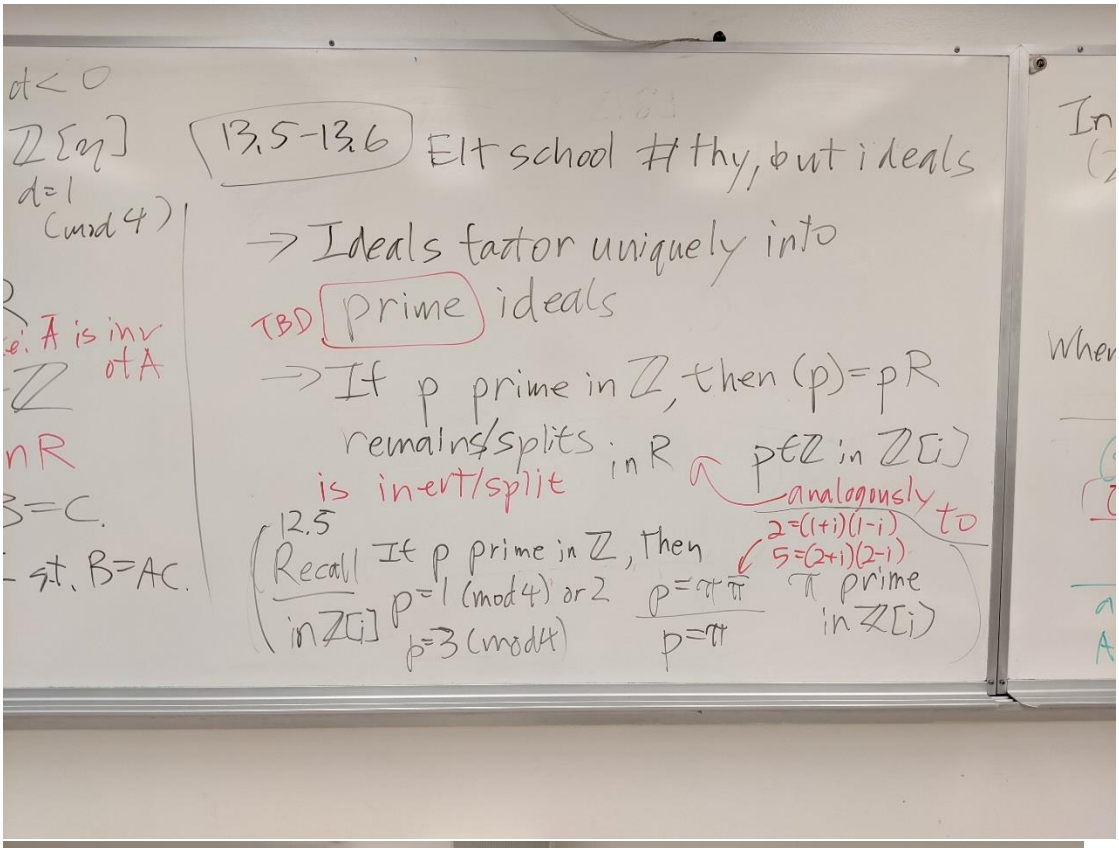
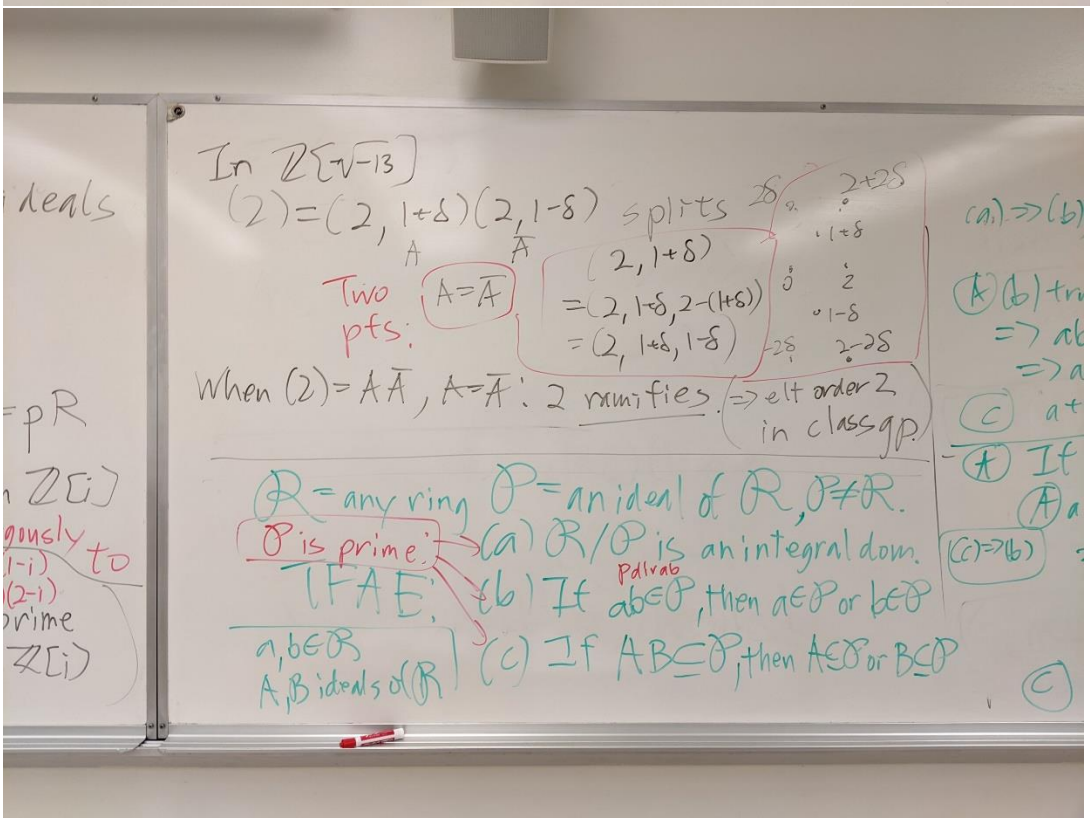

$\delta = \sqrt{d}$, $d < 0$
$R = R_{oI} \text{oi } Q\#F = \mathbb{Z}[\delta]$ or $\mathbb{Z}[\eta]$
$d = 2$ or $3 \pmod 4$
$d = 1 \pmod 4$
Main Lem A ideal of R
Then $A\bar{A} = (n)$ $n \in \mathbb{Z}$ in R
i.e. $\bar{A}$ is inv of A
Cor A, B, C ideals of R
Cancellation If $AB = AC \Rightarrow B = C$.
$A \supset B \Leftrightarrow A \text{ div } B$, i.e. $\exists C$ s.t. $B = AC$.
$3\mathbb{Z} \supset 6\mathbb{Z}$

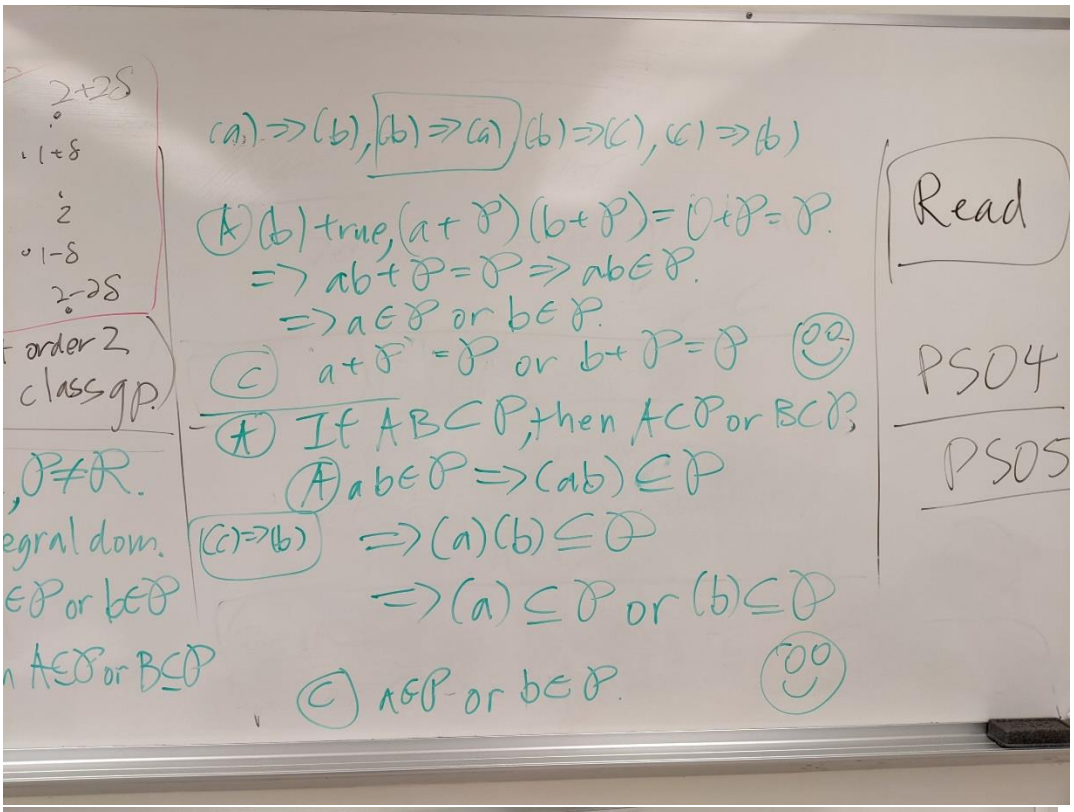

$R = \mathbb{Z}[\sqrt{-13}] = \mathbb{Z}[\delta]$
Ex $d = -13$, $\delta = \sqrt{-13}$
$A = (2, 1+\delta)$
$A\bar{A} = (2, 1+\delta)(2, 1-\delta)$
$= (4, 2-2\delta, 2+2\delta, 1-\delta^2)$
$= (4, 2-2\delta, 2+2\delta, 14)$
$= (2, 4, 2-2\delta, 2+2\delta, 14)$
$= (2)$.
To simplify an ideal:
→ add R-l.c. of gens
→ remove mults of a gen.
$A\bar{A}$ contains gcd(4,14)
R-mult of 2

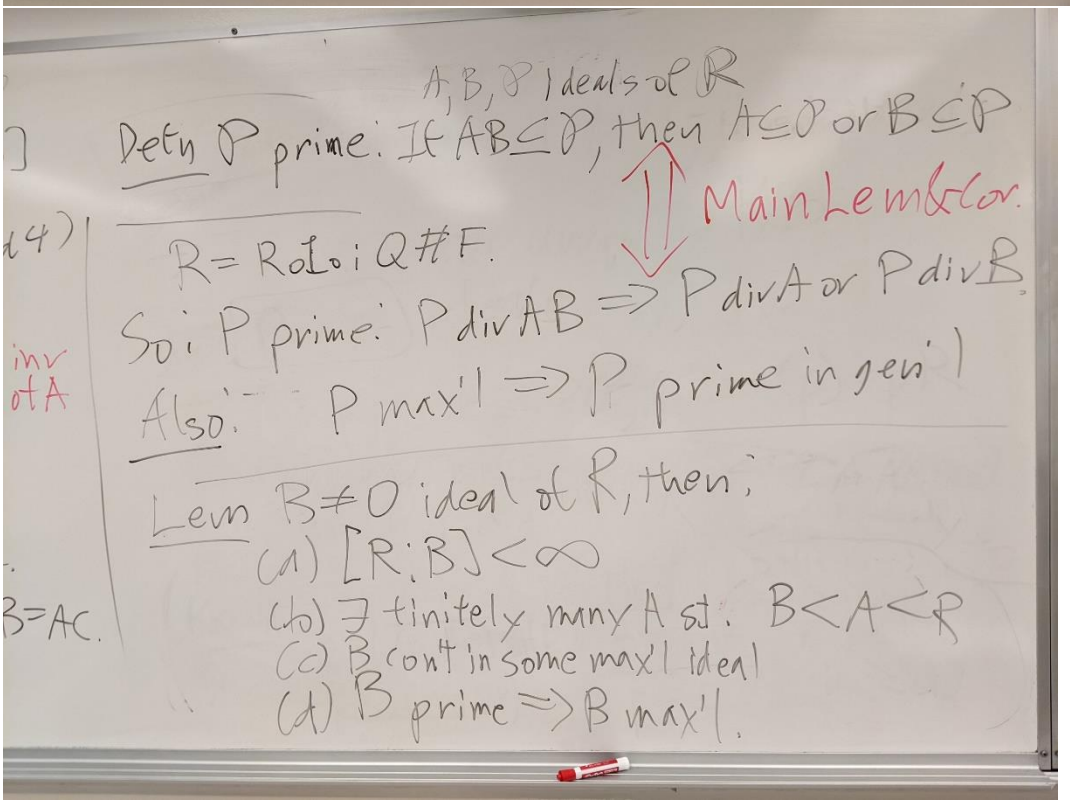

$\bar{B} = (7, 1-8)$
$B = (7, 1+8)$
R.C. $\Rightarrow (1+8) \in AB$
$AB = (2, 1+8)(7, 1+8) = (14, 2+8, 7+7+8, -12+28)$
$= (14, 1+8) \quad (1+8)(1-8)$
$= (1+8)$
elim mults of $1+8$
$(14) = (2)(7) = (1+8)(1-8)$
As ideals: $A\bar{A}B\bar{B} = AB\bar{A}\bar{B}$
We'll see: UF of ideals!
Pf cancel
So
Pf $\Rightarrow$
If
Let
Gen'l
Sp case


elim mults of $1+8$
Pf cancel (A) $AB = AC$
So $\bar{A}AB = \bar{A}AC$ $(n)B = nB$
$\Rightarrow nB = nC \Rightarrow B = C$.
Pf $\Rightarrow$ Case $A = (n), n \in \mathbb{Z}$
If $nR = (n) \supset B$, then $R \supset \frac{1}{n}B$
Let $C = \frac{1}{n}B$. C ideal by exam, and
$AC = (n)(\frac{1}{n}B) = B$.
Gen'l (A) $A \supset B \Rightarrow \bar{A}A \supset \bar{A}B \Rightarrow (n) \supset \bar{A}B$
Sp case $\Rightarrow \exists C$ s.t. $C(n) = \bar{A}B \Rightarrow \bar{A}AC = \bar{A}B \Rightarrow AC = B$
Read
Today 13
Wed 13
PS04 due
PS05 in
:)


d<0
Z[√d]
d=1 (mod 4)
13.5-13.6 Elt school # thy, but ideals
→ Ideals factor uniquely into
TBD prime ideals
→ If p prime in Z, then (p)=pR
remains/splits in R
is inert/split
p∈Z in Z[i]
analogously to
2=(1+i)(1-i)
5=(2+i)(2-i)
π prime in Z[i]
12.5 Recall: If p prime in Z, then in Z[i]
p=1 (mod 4) or 2
p=3 (mod 4)
p=ππ̄
p=ππ
i.e. A is inv of A
Z
nR
B=C.
st. B=AC.


In Z[√-13]
(2)=(2, 1+δ)(2, 1-δ) splits
A Ā
Two pfs:
A=Ā
(2, 1+δ)
=(2, 1-δ, 2-(1+δ))
=(2, 1+δ, 1-δ)
When (2)=AĀ, A=Ā: 2 ramifies.
=> elt order 2 in class gp
R = any ring
P = an ideal of R, P≠R.
P is prime.
TFAE:
(a) R/P is an integral dom.
(b) If ab∈P, then a∈P or b∈P
(c) If AB⊆P, then A⊆P or B⊆P
a,b∈R
A,B ideals of R
pdivab
(a)=>(b)
(c)=>(b)
If


(a) ⇒ (b), (b) ⇒ (a) (b) ⇒ (c), (c) ⇒ (b)
Read
PS04
PS05
order 2
class gp.
P ≠ R.
egral dom.
∈ P or b ∈ P
n A ⊆ P or B ⊆ P
(A) (b) true, (a + P)(b + P) = 0 + P = P.
⇒ ab + P = P ⇒ ab ∈ P.
⇒ a ∈ P or b ∈ P.
(C) a + P = P or b + P = P
(A) If AB ⊂ P, then A ⊂ P or B ⊂ P.
(A) ab ∈ P ⇒ (ab) ⊆ P
(C)⇒(b) ⇒ (a)(b) ⊆ P
⇒ (a) ⊆ P or (b) ⊆ P
(C) a ∈ P or b ∈ P.


A, B, P ideals of R
Defn P prime: If AB ⊆ P, then A ⊆ P or B ⊆ P
Main Lem & Cor.
R = R o L o i Q # F.
So: P prime: P div AB ⇒ P div A or P div B
Also: P max'l ⇒ P prime in gen'l
Lem B ≠ 0 ideal of R, then:
(a) [R : B] < ∞
(b) ∃ finitely many A s.t. B < A < R
(c) B cont in some max'l ideal
(d) B prime ⇒ B max'l.
inv of A
B = AC.