2/24
Monday
week 6

Last time

R is an integral domain

- $r \in R$, $r \neq 0$, r is not a unit

  r is <u>irreducible</u> if whenever

  $r = ab$ for $a, b \in R$

  then either a is a unit or b is a unit.

- $r \in R$ is <u>prime</u> if $r \neq 0$ and (r) is a prime ideal.

Prop: Let R be an integral domain. If $p \in R$ is prime, then p is irreducible.

proof: Let $p \in R$ be prime. So $p \neq 0$ and (p) is a prime ideal.

Let's show p is irreducible.

Suppose $\boxed{p = ab}$ for some $a, b \in R$.

Note that $ab = p \cdot 1 \in (p)$

Recall:

$(p) = \{ px \mid x \in R \}$

Since $ab \in (p)$ and (p) is a prime ideal, either $a \in (p)$ or $b \in (p)$. } Using def of prime ideal

case 1:

Suppose $b \in (p)$.

Then $\boxed{b = pk}$ where $k \in R$.

So, $p = ab = apk$.

Thus, $p(1 - ak) = 0$.

Since R is an integral domain, either $p = 0$ or $1 - ak = 0$.

Since $p \neq 0$ we have $1 - ak = 0$.

Thus, $ak = 1$. Therefore a is a unit.

Case 2: If $a \in (p)$, the same proof as above would give that b is a unit.

Therefore, p is irreducible. $\blacksquare$

Prop: Let R be a PID.
Let $p \in R$ with $p \neq 0$.
p is prime iff p is irreducible.

proof:

($\Rightarrow$) A PID is an integral domain
So just showed prime
implies irreducible in this case.

($\Leftarrow$) Let $p \in R$ with $p \neq 0$. Assume p is irreducible.
We want to show that (p) is
a prime ideal, and hence p is prime.

We will show (p) is maximal.
We know maximal implies prime,
so that will take care of
the proof.

Suppose $(p) \subseteq I \subseteq R$.
Since R is a PID,
$I = (d)$ where $d \in R$.
So, $(p) \subseteq (d) \subseteq R$.
Thus, $p \in (d)$.
Hence, $\boxed{p = d\ell}$ where $\ell \in R$.
Since p is irreducible either
d is a unit or ℓ is a unit.

Case 1:
So, $I =$
Thus, b

Case 2:
Then
Therefore
Since (
So, $(p) =$

Case 1: Suppose d is a unit.

So, $I=(d)$ contains a unit.
Thus, by a previous result, $I=R$.

Case 2: Suppose ℓ is a unit.

Then $\ell^{-1}\in R$ exists and $p\ell^{-1}=d$.
Therefore $(d)\subseteq(p)$.

If $x\in(d)$, then $x=dk$, $k\in R$.
So, $x=dk=p(\ell^{-1}k)\in(p)$

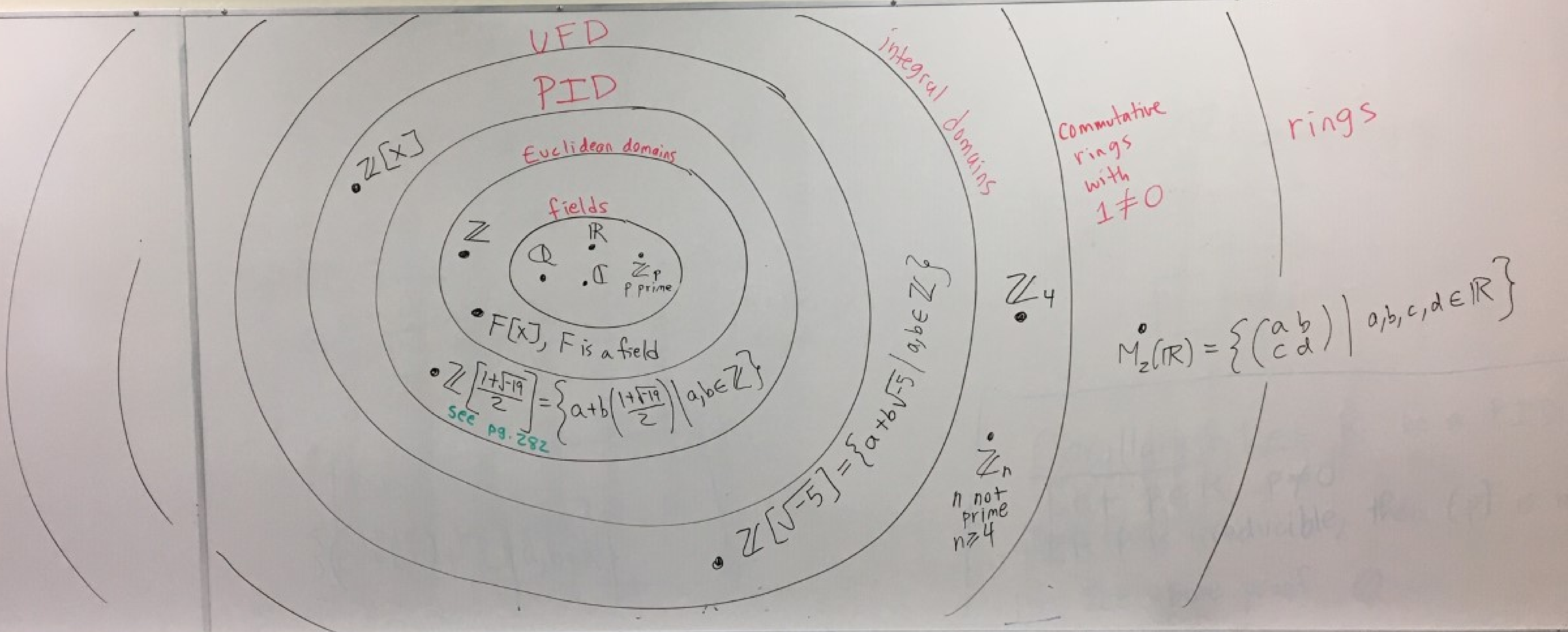
Since $(p)\subseteq(d)$ and $(d)\subseteq(p)$.
So, $(p)=I=(d)$.

So given an ideal I with $(p)\subseteq I\subseteq R$ we have $(p)=I$ or $I=R$.

Thus, (p) is maximal and hence prime. $\blacksquare$

Corollary: Let R be a PID. Let $p\in R$, $p\neq 0$. If p is irreducible, then (p) is maximal.

pf: See above proof. $\blacksquare$


UFD
PID
Euclidean domains
fields
integral domains
Commutative rings with $1 \neq 0$
rings
$\mathbb{Z}[x]$
$\mathbb{Z}$
$\mathbb{R}$
$\mathbb{Q}$
$\mathbb{C}$
$\mathbb{Z}_p$ p prime
$F[x]$, F is a field
$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a+b\left(\frac{1+\sqrt{-19}}{2}\right) \middle| a,b \in \mathbb{Z}\right\}$
see pg. 282
$\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$
$\mathbb{Z}_4$
$\mathbb{Z}_n$ n not prime $n \geq 4$
$M_2(\mathbb{R}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{R}\right\}$