HW 2 due NOW.

Exam 1 Friday.

Today: Review.

Let R be an integral domain

DEF: R is Euclidean if $\exists$ function $N: R - \{0\} \to \mathbb{N}$ such that (for all $a, b \neq 0$ $\exists$ q, r with

- $a = qb + r$
- $N(r) < N(b)$ OR $r = 0$.)

That's it. N doesn't need extra properties

DEF: R is a PID if every ideal $I \subseteq R$ is principal. i.e. $\exists$ $a \in R$ with $I = (a)$.

DEF: R is a UFD if

(1) Every element can be factored into irreducibles

(2) Such a factorization is unique up to associates.

Theorem: Euclidean $\Rightarrow$ PID.

Proof: Consider ideal $I \subseteq R$.

If $I = (0)$, done.

Otherwise choose $a \in I$, $a \neq 0$, with $N(a)$ minimum (well-ordering).

For any other $b \in I$ we have

- $b = qa + r$
- $N(r) < N(a)$ OR $r = 0$

Then $r = b - qa \in I \Rightarrow r = 0 \Rightarrow b \in (a)$. $\blacksquare$

Theorem: PID $\Rightarrow$ UFD.

(1) Existence.

Suppose some element has an infinite chain of proper divisors. We get

$(a_1) < (a_2) < (a_3) < \cdots$ forever

Lemma: $\bigcup_{i=1}^{\infty} (a_i)$ is an ideal. Proof: easy $\square$

PID $\Rightarrow \bigcup_i (a_i) = (d) \Rightarrow d \in \bigcup_i (a_i)$

$\Rightarrow d \in (a_n)$ for some n.

But then $(d) \subseteq (a_n) < (d)$ $\times$ $\boxed{\quad}$

(2) Uniqueness follows from "Euclid's Lemma": irreducible $\Rightarrow$ prime.

Proof of E.L:

Take p irred, $p \mid ab$, $p \nmid a$. Want: $p \mid b$.

$p \nmid a \Rightarrow (a) \not\subseteq (p)$.

$\Rightarrow (p) < (p) + (a)$

PID $\Rightarrow (p) < (p) + (a) = (d) \subseteq (1)$.

p irred $\Rightarrow (d) = (1)$.

$\Rightarrow 1 \in (p) + (a)$

$\Rightarrow 1 = ax + py$ for some x, y.

$\Rightarrow b = abx + pby$

$b = pkx + pby$ since $p \mid ab$.

$b = p(kx + by)$. $\boxed{\quad}$

Finally

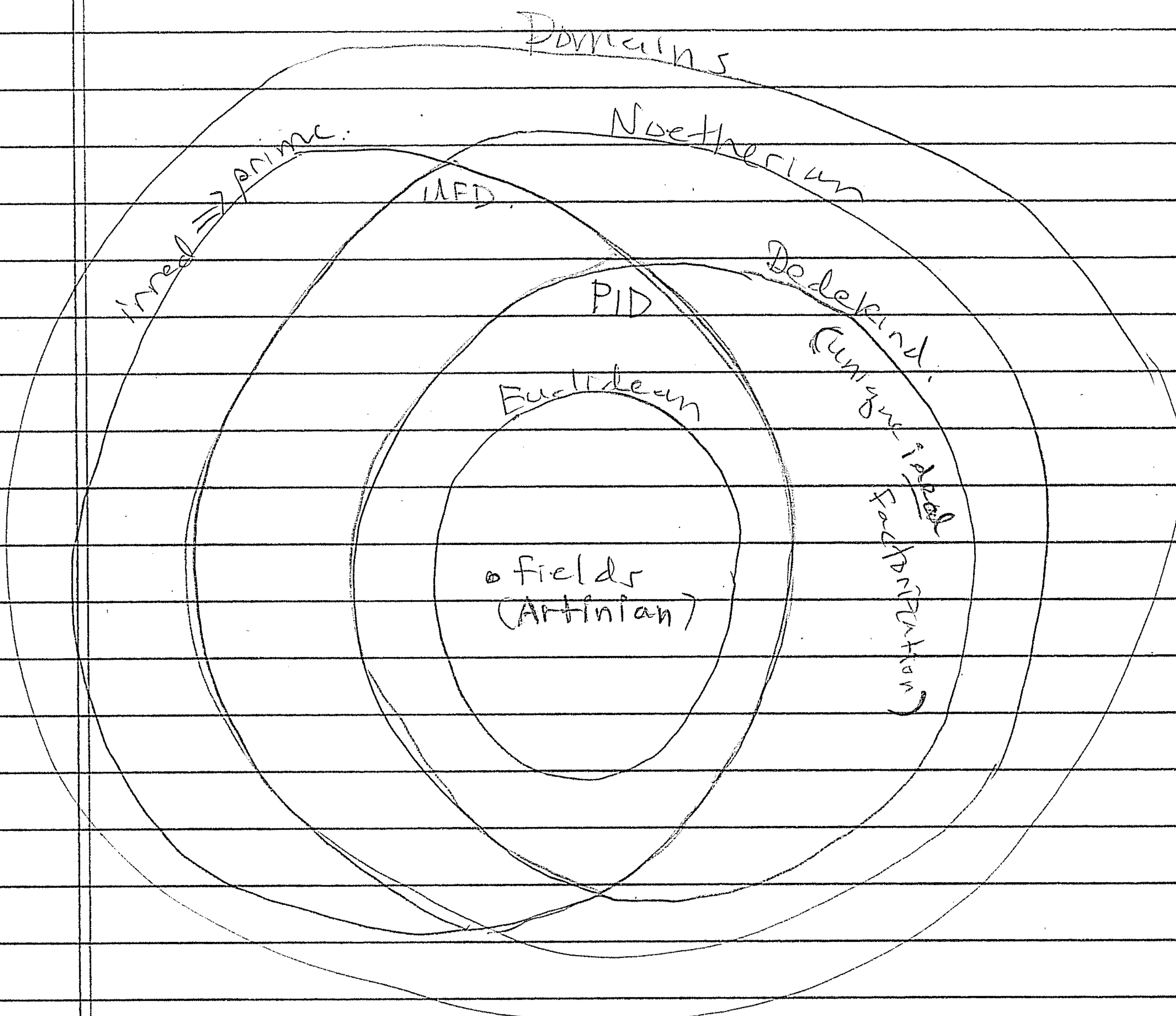
$\alpha = a_1 a_2 \cdots a_m = b_1 b_2 \cdots b_n$ irred.

WLOG

$\Rightarrow a_1, b_1$ are associate.

cancel and repeat $\boxed{\quad}$

The Domain of Domains:



Discuss HW2 problems 4 & 5.