Math 525 Class 11 Sept. 18

Universal Nonsense.

Q: Theorem 15, p. 261, part 2 is titled "uniqueness of Q" $= D^{-1}R$

How is this long statement "uniqueness"

A: Meta-Theorem: Objects defined by a universal property are unique up to isomorphism.

Q: How can you ever get any results out of this "universal nonsense"?

A: The story of the Theorem of The Cube

The Summary of Ch. 8.

(1) A Euclidean Domain is a Principal Ideal Domain

A PID is a Unique Factorization Domain.

Proof of ①: Apply the extreme principle.

Consider an element of minimal (nonzero) norm in the ideal. Show that it generates.

Facts about principal ideal domains.

A PID is Noetherian: "ascending chain condition" ACC.

Any ascending chain of ideals stops:

if R is Noetherian and $I_1 \subseteq I_2 \subseteq \cdots$ are ideals of R, then there is some N such that $I_j = I_N$ for all $j \geq N$.

Note that most of our standard examples, e.g. $\mathbb{Z}[x,y]$, $\mathbb{Z}$, $F[x,y]$ are Noetherian. Also $\mathcal{O}_K$ for $K/\mathbb{Q}$ finite.

An example that is NOT Noetherian

$C[0,1]$: continuous fcns from $[0,1] \to \mathbb{R}$.

$(x) \subset C[0,1]$ is an ideal.

$(x^{1/2}) \subset C[0,1]$ is an ideal

and $(x) \subset (x^{1/2}) \subset (x^{1/4}) \subset (x^{1/8}) \subset \cdots$

Notice that we can't do this in $F[x]$.

There is also a descending chain condition (DCC

The DCC is much stronger. Not symmetric.

In fact DCC $\Rightarrow$ ACC, but this is not obvious

ACC $\not\Rightarrow$ DCC.

Why is the DCC stronger?

In any rng R using any $x \notin R^\times$,

we can write down a descending chain:

$$(x) \supset (x^2) \supset (x^3) \supset (x^4) \supset \cdots$$

If this can't happen, many familiar examples are eliminated.

$\mathbb{Z}$ and $F[x]$ do not satisfy the DCC.

If G is a finite group, then $F[G]$ satisfies the DCC since it is a FDVS over F.

Why does a PID satisfy the ACC?

Suppose $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ in a PID R.

Then $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal.

By PID condition $I = (a)$ for some $a \in R$. And $a \in I_n$ for some n.

Then $a \in I_n$ so $I_n = I_{n+1} = I_{n+2} = \cdots$

Note also an equivalent form of the ACC: finite generation of ideals.

Thus PID $\Rightarrow$ 1-generation $\Rightarrow$ finite generation

Euclidean Algorithm for computing gcd.

- very fast.
- not obvious.
- much better than: compute prime factorizations and check for common primes.

Common phenomenon in algorithms: the "obvious" way to do something is very slow relative to an indirect method.

Example: integer factorization.

Obvious algorithm: divide by 2, 3, 5, ...

Indirect: Pollard Rho, Quadratic Sieve, etc.

In a PID ~~the Euclidean algorithm~~ (Prop. 6) a gcd of a, b can be written as a linear combination of a and b.

$\gcd(a, b) = xa + yb$ for some $x, y \in R$.

Prop. 7: Every nonzero prime ideal in a PID is maximal.

Idea of proof: if $(a) \subset (b)$ then $b = xa$ and so we have "factored" b.

Corollary: 8: If R is a commutative ring such that. $R[x]$ is a PID, then R is a field.

Idea of proof: In $\mathbb{Z}[x]$ we have

$$(x) \subset (2, x).$$

Definition: (Dedekind - Hasse Norm)
(Generalizes Euclidean condition)
For every nonzero $a, b \in R$ either $a \in (b)$ or there is a nonzero element of (a, b) with norm less than the $N(b)$.

Rephrase. Either $a = xb$ or.

$\exists\ s, t$ such that $N(sa - tb) < N(b)$.

Proposition 9: R is a PID $\Leftrightarrow$ R has a DH norm.

Idea of Proof: (DH norm $\Rightarrow$ PID)

Generalize the proof for Euclidean case.

(Extreme Principle + Proof By Contradiction.)

Other direction: PID $\Rightarrow$ DH norm.

Use PID $\Rightarrow$ UFD, and then show that there is a DH norm:

$N(a) = 2^{\#\text{ irreducibles in factorization.}}$