GTLA Lecture 22.10.2020

Principal ideal domains PIDs

(have good gcd's: gcd(a,b) is well defined).

Let A be a commutative ring.

<u>Example</u> $\mathbb{Z}$.

<u>Nonexample</u> $M_n(\mathbb{C})$ for $n > 1$.

<u>A satisfies the cancellation law</u> if it satisfies

(CL) if $a, b, c \in A$ and $c \neq 0$ and $ac = bc$ then $a = b$.

<u>A has no zero divisors</u> if A satisfies

(NZD) if $a, b \in A$ and $ab = 0$ then $a = 0$ or $b = 0$.

HW: A satisfies (CL) if and only if A satisfies (NZD)

Let A be a commutative ring. A is an integral domain if A satisfies (CL).

Example $\mathbb{Z}$, or a field $\mathbb{F}$. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Nonexample $\mathbb{Z}/12\mathbb{Z}$.

In $\mathbb{Z}/12\mathbb{Z}$, $3 \cdot 4 = 0$.

Ideals

An ideal, or submodule, of A is a subset $M \subseteq A$ such that

(a) If $m_1, m_2 \in M$ then $m_1 + m_2 \in M$.

(b) If $m \in M$ and $a \in A$ then $am \in M$.

(i.e. M is closed under addition and scalar multiplication).

(same as a subspace except $\mathbb{A}$ doesn't have to be a field).

A principal ideal domain (or PID.) is a commutative ring $\mathbb{A}$ such that

(a) $\mathbb{A}$ satisfies (CL),

(b) If M is an ideal of $\mathbb{A}$ then there exists $\ell \in \mathbb{A}$ such that $M = \ell\mathbb{A}$

(multiples work well in a PID).

((b) i.e. is every ideal is generated by one element).

(analogy: A cyclic subgroup is a subgroup generated by one element)

Example $\mathbb{Z}$ $\qquad$ $3\mathbb{Z} \subseteq \mathbb{Z}$.

or $\mathbb{F}$ a field, or $\mathbb{F}[x]$.

Nonexample An integral domain

but is not a PID.

$\mathbb{C}[x,y]$ or $\mathbb{Z}[x]$.

In $\mathbb{Z}[x]$ then M gen by $2, x$

is $2 \cdot \mathbb{Z}[x] + x\,\mathbb{Z}[x]$ is an ideal that can't be generated by one element.

In $\mathbb{C}[x,y]$ then

$$x\,\mathbb{C}[x,y] + y\,\mathbb{C}[x,y]$$

is an ideal that can't be generated by one element.

Let $\mathbb{F}$ be a field and let M be an ideal in $\mathbb{F}$.

So $M \subseteq \mathbb{F}$, closed under addition and under scalar multiplication.

If $M \neq 0$ let $a \in M$ with $a \neq 0$.
Then scalar mult. by $a^{-1} \in \mathbb{F}$ gives $a^{-1} \cdot a \in M$.

So $1 \in M$.

So $c \cdot 1 \in M$ for $c \in \mathbb{F}$.

So $M = \mathbb{F}$.

So if M is an ideal in $\mathbb{F}$

then $M = 0$ or $M = \mathbb{F}$.

(i.e. $\mathbb{F}$ "has no ideals")

A ring with no ideals is a <u>simple ring</u>.

A group with <u>no normal subgroups</u> is a <u>simple group</u>

A module with no submodules is a <u>simple module</u>.

("simple" and "irreducible" are synonyms)

So $\mathbb{F}$ has only the ideals $0 \cdot \mathbb{F}$ and $1 \cdot \mathbb{F}$

So $\mathbb{F}$ is a PID.

Goal: If $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a PID.

(consequence is that for polynomials you work with $\gcd(p(x), q(x))$ and $\mathrm{lcm}(p(x), q(x))$.

Proposition (Euclidean algorithm for $\mathbb{F}[x]$). Let $\mathbb{F}$ be a field. Let $a(x), b(x) \in \mathbb{F}[x]$ with $b(x)$ monic. Then there exist $q(x), r(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)b(x) + r(x) \quad \text{and}$$

$$\deg(r(x)) < \deg(b(x)).$$

Example $a = 2x^4 + 3x^2$
$b = x^2 + 2$.

$$\underbrace{2x^4+3x^2}_{a} \underset{=}{=} \underbrace{(2x^2-1)}_{q}\underbrace{(x^2+2)}_{b} \underbrace{+2}_{+\ r}$$

$$\begin{array}{r} 2x^2 - 1 \\ x^2+2 \overline{) 2x^4 + 3x^2} \\ \underline{2x^4 + 4x^2} \\ -x^2 \\ \underline{-x^2 + 2} \\ -2 \end{array}$$

POINT: Just figure out what $q(x)$ has to be.

Proof Let $a(x), b(x) \in \mathbb{F}[x]$ with $b(x)$ monic. Let

$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

$b(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} + x^m.$

To show: There exist $q(x)$ and $r(x)$ such that $a = qb + r$ and $\deg r < \deg b$.

Let $q(x) = q_0 + q_1 x + \cdots + q_{n-m} x^{n-m}$ given by

$q_{n-m} = a_n$

$$q_{n-m-1} + q_{n-m} b_{m-1} = a_{n-1}$$

$$\vdots$$

$$q_{n-m-j} + q_{n-m-(j-1)} b_{m-1} + \cdots + q_{n-m-1} b_{m-j+1} + q_{n-m} b_{m-j} = a_{n-j}$$

$$\vdots$$

$$q_0 + q_1 b_{m-1} + \cdots + q_{n-m-1} b_{m-(n-m)+1} + q_{n-m} b_{m-(n-m)} = a_m.$$

For convenience let $b_{-k} = 0$ for $k \in \mathbb{Z}_{>0}$

This system of linear equations is triangular and so $q_0, q_1, \ldots, q_{n-m}$ are determined.

Then define (the remainder)

$$r(x) = a(x) - q(x) b(x)$$

<u>Uniqueness:</u> Assume

$$a(x) = q_1(x) b(x) + r_1(x)$$

$$a(x) = q_2(x) b(x) + r_2(x)$$

with $\deg(r_1(x)) < \deg(b(x))$

$\deg(r_2(x)) < \deg(b(x))$

To show: $q_1(x) = q_2(x)$ and

$r_1(x) = r_2(x)$.

Since

$$0 = a(x) - a(x)$$

$$= (q_1(x) - q_2(x))b(x) + (r_1(x) - r_2(x))$$

Solve for $q_1(x) - q_2(x)$ to get

$$q_1(x) - q_2(x) = 0.$$

(using the equations above).

Then $q_1(x) = q_2(x)$.

and $r_1(x) - r_2(x) = 0$.

So $r_1(x) = r_2(x)$. //