GTLA Lecture 27.10.2020

Let $\mathbb{A}$ be a commutative ring.

An <u>ideal</u>, or <u>$\mathbb{A}$-submodule</u>, of $\mathbb{A}$ is a subset $M \subseteq \mathbb{A}$ such that

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

(2) If $m \in M$ and $a \in \mathbb{A}$ then
$$am \in M$$

$\mathbb{A}$ is a <u>PID</u>, or <u>principal ideal domain</u>, if $\mathbb{A}$ satisfies

(1) If $a, b, c \in \mathbb{A}$ and $c \neq 0$ and $ac = bc$ then $a = b$

(cancellation law)

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

<u>Example</u> $\mathbb{Z}$, and $\ell\mathbb{Z}$ is multiples of ℓ.

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

Proposition (Euclidean algorithm for $\mathbb{F}[x]$) Let $a(x), b(x) \in \mathbb{F}[x]$ and $b(x)$ is monic then there exist unique $q(x), r(x) \in \mathbb{F}[x]$ such that

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

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

Partial fractions

Backwards of common denominator.

For example:

$$\frac{5x+22}{(x+2)(x+6)} = \frac{3}{x+2} + \frac{2}{x+6}.$$

Another example:

$$\frac{31}{33} = \frac{3}{11} + \frac{2}{3}$$

Steps for partial fractions

Splitting Let $\mathbb{A}$ be a PID.

Let $p, q \in \mathbb{A}$ with

$$\boxed{p\mathbb{A} + q\mathbb{A} = \mathbb{A}}$$

(i.e. p, q are relatively prime, i.e. $\gcd(p,q) = 1$)

There exist $r, s \in \mathbb{A}$ such that

$$pr + qs = 1$$

Then $$\frac{1}{pq} = \frac{pr+qs}{pq} = \frac{r}{q} + \frac{s}{p}.$$

and $$\frac{a}{pq} = \frac{a \cdot 1}{pq} = \frac{apr + aqs}{pq} = \frac{ar}{q} + \frac{as}{p}$$

Prime powers

$$\frac{a_1}{p} + \frac{a_2}{p^2} + \frac{a_3}{p^3} = \frac{a_1 p^2 + a_2 p + a_3}{p^3}$$

with $a_1, a_2, a_3 \in \mathbb{A}/p\mathbb{A}$

This is decimal expansion in the case $p=10$

$$a_1 10^{-1}+a_2 10^{-2}+a_3 10^{-3}=\frac{a_1\cdot 10^2+a_2 10+a_3}{10^3}$$

$$2\frac{1}{10}+\frac{6}{100}+\frac{5}{1000}=\frac{265}{1000}$$

The "digit" $a_1, a_2, a_3 \in \{0, 1, \dots, 9\}$.

Representatives of A/qA.

If $a=bq+r$ then $\frac{a}{q}=b+\frac{r}{q}$.

Partial fractions for

$$\frac{2x^4+3x^2}{(x^2+1)^2(x^2+2)}$$

Note: Using Euclidean algorithm

$$(x^2+1)^2 = x^2(x^2+2)+1$$

So $1=(-x^2)(x^2+2)+(x^2+1)^2$.

So

$$\frac{2x^4+3x^2}{(x^2+1)^2(x^2+2)} = \frac{(2x^2-1)(x^2+2)+2}{(x^2+1)^2(x^2+2)}$$

$$= \frac{2x^2-1}{(x^2+1)^2} + \frac{2}{(x^2+1)^2(x^2+2)}$$

$$= \frac{2(x^2+1)-3}{(x^2+1)^2} + \frac{2\left((-x^2)(x^2+2)+(x^2+1)^2\right)}{(x^2+1)^2(x^2+2)}$$

$$= \frac{2(x^2+1)-3+(-2x^2)}{(x^2+1)^2} + \frac{2}{x^2+2}$$

$$= \frac{-1}{(x^2+1)^2} + \frac{2}{x^2+2}$$

<u>Proposition</u> Let $\mathbb{F}$ be a field. If M is an ideal of $\mathbb{F}[x]$ then there exists $\ell(x) \in \mathbb{F}[x]$ such that $M = \ell(x)\mathbb{F}[x]$.

(From the depths:
Let $A \in M_n(\mathbb{F})$. Then

$$ev_A : \mathbb{F}[x] \longrightarrow M_n(\mathbb{F})$$
$$p_0 + p_1 x + \cdots + p_k x^k \longmapsto p_0 + p_1 A + \cdots + p_k A^k$$

$\ker(ev_A) = \{ p(x) \in \mathbb{F}[x] \mid p(A) = 0 \}$.

The <u>minimal polynomial</u> of A is the polynomial $m_A(x)$ of lowest degree such that $m_A(A) = 0$

And $m_A(x)$ divides $\det(x - A)$.

i.e. $\det(x-A)$ is a multiple of $m_A(x)$.

REALLY

$$\ker(ev_A) = m_A(x)\,\mathbb{F}[x]$$

<u>Proof</u> Let M be an ideal of $\mathbb{F}[x]$.

To show: There exists $\ell(x) \in \mathbb{F}[x]$ such $M = \ell(x)\,\mathbb{F}[x]$.

Let $m(x) \in M$ be such that

if $p(x) \in M$ then $\deg(p(x)) \geq \deg(m(x))$.

Let $m(x) = m_0 + m_1 x + \cdots + m_d x^d$ with $m_d \neq 0$.

Let $\ell(x) = \frac{1}{m_d}(m(x))$
$= m_0 m_d^{-1} + m_1 m_d^{-1} x + \cdots + m_{d-1} m_d^{-1} x^{d-1} + x^d.$

To show: $\ell(x)\mathbb{F}[x] = M$.

To show: (a) $\ell(x)\mathbb{F}[x] \subseteq M$

(b) $M \subseteq \ell(x)\mathbb{F}[x]$.

(a) To show: If $p(x) \in \mathbb{F}[x]$ then $\ell(x)p(x) \in M$.

Assume $p(x) \in \mathbb{F}[x]$.

To show: $p(x)\ell(x) \in M$.

Since M is closed under scalar multiplication by elements of $\mathbb{F}[x]$ then $p(x)\ell(x) \in M$.

So $\ell(x)\mathbb{F}[x] \subseteq M$

(b) To show: $M \subseteq \ell(x)\mathbb{F}[x]$.

To show: If $a(x) \in M$ then $a(x) \in \ell(x)\mathbb{F}[x]$

Assume $a(x) \in M$.

By the Euclidean algorithm, there exist $q(x), r(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)\ell(x) + r(x)$$

and $\deg(r(x)) < \deg(\ell(x))$.

Since $a(x) \in M$ and $\ell(x) \in M$ and M is closed under scalar multiplication and addition then

$$r(x) = a(x) - q(x)\ell(x) \in M.$$

By construction $\ell(x)$ has minimal degree among elements of M so

$\deg(r(x)) < \deg(\ell(x))$ forces

$$r(x) = 0.$$

So $a(x) = q(x)\ell(x) \in \ell(x)\mathbb{F}[x]$.

So $M \subseteq \ell(x)\mathbb{F}[x]$.

So $M = \ell(x)\mathbb{F}[x]$. //

$\deg(a_0 + a_1x + a_2x^2 + \cdots)$ is the maximal $d \in \mathbb{Z}_{\geq 0}$ such that $a_d \neq 0$.