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

$\mathbb{A}$ satisfies the cancellation law if $\mathbb{A}$ satisfies

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

The ring $\mathbb{A}$ has no zero divisors if $\mathbb{A}$ satisfies

(NZD) If $b, c \in \mathbb{A}$ and $bc = 0$ then $b = 0$ or $c = 0$.

HW: Show that $\mathbb{A}$ satisfies CL
if and only if $\mathbb{A}$ satisfies NZD.

An integral domain is a commutative ring $\mathbb{A}$ which satisfies the cancellation law.

Note: $\mathbb{Z}$ is an integral domain (also a field $\mathbb{F}$ is, and $\mathbb{F}[x]$, and $\mathbb{Q}$ and $\mathbb{R}$ and $\mathbb{C}$).

Note $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain

Ideals

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

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

(b) if $m \in M$ and $a \in \mathbb{A}$ then $am \in M$.

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

(a) $\mathbb{A}$ satisfies the cancellation law,

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

i.e. $\mathbb{A}$ is an integral domain
and every ideal is generated by one element.

Analogy, a cyclic group is a group generated by one element.

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

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 unique $q(x), r(x) \in \mathbb{F}[x]$ such that

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

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

Proof Let

$a(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ and

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

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

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

by the conditions

$$q_{n-m} = a_n,$$

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

$$\vdots$$

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

$$\vdots$$

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

(Note: $n-(n-m) = m$). Define

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

The definition of $q_0, \ldots, q_{n-m}$ is precisely what is required to ensure that

$$b(x) q(x) = c_0 + c_1 x + \cdots + c_{m-1} x^{m-1} + a_m x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n.$$

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

$$= (a_0 - c_0) + (a_1 - c_1)x + \cdots + (a_{m-1} - c_{m-1})x^{m-1}$$

and $\deg(r(x)) < m = \deg(b(x))$.

<u>Uniqueness</u>: Assume $a(x) = q_1(x)b(x) + r_1(x)$
and $a(x) = q_2(x)b(x) + r_2(x)$
and $\deg(r_1(x)) < \deg(b(x))$
and $\deg(r_2(x)) < \deg(b(x))$.

Then $0 = a(x) - a(x) = (q_1(x) - q_2(x))b(x) + (r_1(x) - r_2(x))$
$$= c_0' + c_1'x + \cdots + c_{m-1}'x^{m-1} + 0x^m + \cdots + 0x^n$$
and this forces $q_1(x) - q_2(x) = 0$ (by multiplying out $(q_1(x) - q_2(x))b(x)$ and using $\deg(r_1(x) - r_2(x)) < \deg(b(x))$.).

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

So $r_1(x) = r_2(x)$, since $r_1(x) - r_2(x)$. //.

<u>Theorem</u> $\mathbb{F}[x]$ is a PID

<u>Proof</u> To show: (a) $\mathbb{F}[x]$ is an integral domain.

(b) If M is an ideal then there exists $l(x) \in \mathbb{F}[x]$ such that $M = l(x)\mathbb{F}[x]$.

(b) Let M be an ideal of $\mathbb{F}[x]$.

Let $m(x) \in M$ of minimal degree among all elements of M, i.e.

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

Let $m(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_d x^d$ with $m_d \neq 0$

Let $\ell(x) = \frac{1}{m_d} m(x) \in \mathbb{F}[x]$.

Since $\frac{1}{m_d} \in \mathbb{F}[x]$ and $m(x) \in M$ then $\ell(x) \in M$.

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

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 $a(x) \in M$.

Then there exists $r(x), q(x) \in \mathbb{F}[x]$ such that

$$a(x) = q(x)\ell(x) + r(x) \quad \text{with } \deg(r(x)) < \deg(\ell(x))$$

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

Since $\deg(r(x)) < \ell(x)$ and $\ell(x)$ has minimal degree among elements of M then $r(x) = 0$.

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

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

14.10.2020 ①
Partial Fractions
A. Ran

Partial fractions for $\dfrac{2x^4+3x^2}{(x^2+1)^2(x^2+2)}$

Note that (say, by the Euclidean algorithm computation of the gcd$((x^2+1)^2, x^2+2)$),

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

So

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

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

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

Partial fractions for $\dfrac{3x^2-2x+1}{(x+1)(x^2+2x+2)}$

Note that (say, by the Euclidean algorithm computation of $\gcd(x+1, x^2+2x+2)$)

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

so

$$\frac{3x^2-2x+1}{(x+1)(x^2+2x+2)} = \frac{3(x^2+2x+2)-8x-5}{(x+1)(x^2+2x+2)}$$

$$= \frac{3}{x+1} + \frac{-8(x+1)+3}{(x+1)(x^2+2x+2)}$$

$$= \frac{3}{x+1} - \frac{8}{x^2+2x+2} + 3\frac{((x^2+2x+2)-(x+1)(x+1))}{(x+1)(x^2+2x+2)}$$

$$= \frac{3}{x+1} - \frac{8}{x^2+2x+2} + \frac{3}{x+1} - \frac{3(x+1)}{x^2+2x+2}$$

$$= \frac{6}{x+1} + \frac{-3x-11}{x^2+2x+2} = \frac{6}{x+1} - \frac{3(x+1)}{(x+1)^2+1} - \frac{8}{(x+1)^2+1}.$$

Partial fractions for $\dfrac{4x+1}{(x-3)(x+1)}$

Note that (say, by the Euclidean algorithm computation of $\gcd(x-3, x+1)$)

$x+1 = (x-3)+4$, so $4 = (x+1)-(x-3)$

and $1 = \frac{1}{4}(x+1) - \frac{1}{4}(x-3)$.

So

$$\frac{4x+1}{(x-3)(x+1)} = \frac{4(x+1)-8}{(x-3)(x+1)} = \frac{4}{x-3} - \frac{8}{(x-3)(x+1)}$$

$$= \frac{4}{x-3} - \frac{8\left(\frac{1}{4}(x+1) - \frac{1}{4}(x-3)\right)}{(x-3)(x+1)}$$

$$= \frac{4}{x-3} - \frac{2}{x-3} + \frac{2}{x+1} = \frac{7}{x-3} + \frac{2}{x+1}.$$