Math 3032 Lecture 8 (Feb 9, 2021)

OH today 12-2pm.

No class next week: Winter Study Break.

Following week (Feb 22-26) OH by appointment/email.

Today: long division + factorization (of polynomial(s))

Long division.

To warm up: division in $\mathbb{Z}$.
eventually: division in $\mathbb{Q}[x]$.

$$
\begin{array}{r}
189 \\
65 \overline{)\,12345} \\
-\,65 \\
\hline
584 \\
-\,520 \\
\hline
645 \\
-\,585 \\
\hline
60
\end{array}
$$

$9 \times 65 = 585$

learned:

$$12345 = \underbrace{189}_{q} \times 65 + \underbrace{60}_{r}$$

This process was algorithmic: guaranteed to terminate.

The numbers $q = 189$ and $r = 60$ are uniquely determined by

- $12345 = q \times 65 + r$ and
- $0 \leq r < 65$

$65 = 6 \cdot 10 + 5$

$\rightsquigarrow 6 \cdot x + 5$

$1x^4 + 2x^3 + 3x^2 + 4x + 5$

More generally, Euclid showed that

for any positive $m, n \in \mathbb{Z}$, there are unique

$q, r \in \mathbb{Z}$ w/ $0 \le r \le n$ and

$$m = q \cdot n + r.$$

This is also true for polynomials.

Thm (Long division): For any field $\mathbb{F}$,

and any $f, g \in \mathbb{F}[x]$, there are unique

$q, r \in \mathbb{F}[x]$ s.t. $f(x) = q(x)g(x) + r(x)$ and $\deg r < \deg g$.

Eg (Long Division)

$$6x+5 \;\overline{)\; x^4+2x^3+3x^2+4x+5 \;}\;\; \frac{1}{6}x^3+\frac{7}{36}x^2+\frac{73}{216}x+\frac{a}{6}$$

$$-\left(x^4+\frac{5}{6}x^3\right)$$

$$\frac{7}{6}x^3+3x^2$$

$$-\left(\frac{7}{6}x^3+\frac{35}{36}x^2\right)$$

$$\frac{73}{36}x^2+4x$$

$$\frac{73}{36}x^2+\frac{365}{216}x$$

$$\left(4-\frac{365}{216}\right)x+5$$

a

and

Some remainder

Thm: Given $f, g \in \mathbb{F}[x]$, there are unique $q, r \in \mathbb{F}[x]$ s.t.

$$f = gq + r \quad \text{and} \quad \deg r < \deg g.$$

Pf: **Uniqueness:** Suppose $f = gq_1 + r_1$, $\deg r_1 < \deg g$

and $f = gq_2 + r_2$. $\deg r_2 < \deg g$.

(Want to show $r_1 = r_2$ and $q_1 = q_2$)

Then $r_1 - r_2 = g \cdot (q_2 - q_1)$

$\deg(r_1 - r_2) \leq \max(\deg(r_1), \deg(r_2)) < \deg g.$

Remark: $\forall d$ $\mathbb{F}_{\leq d}[x]$ = {polys of deg $\leq d$} is an gp under $+$.

$\deg(r_1 - r_2) < \deg(g)$ and $r_1 - r_2 = g \cdot (f_1 - f_2)$ ★

Since F is a field, in particular a domain,

and so ★ implies

$$\deg(r_1 - r_2) = \deg(g) + \deg(f_1 - f_2).$$

$\deg(f_1 - f_2) \in \mathbb{N} \cup \{-\infty\}$ $\geq \deg(g)$ if $\deg(f_1 - f_2) \in \mathbb{N}$.

$\{0, 1, 2, \ldots\}$

So only option is $\deg(f_1 - f_2) = -\infty$.

This only happens when $f_1 - f_2 = 0$.

Then $r_1 - r_2 = g \cdot (f_1 - f_2) = 0$.

Existence:

Suppose $f = f_0 = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0.$

If $n < m$, done: set $q = 0$ $r = f$.

Otherwise

$$f = g \cdot \left(\frac{a_n}{b_m} x^{n-m}\right) + \underbrace{\text{lower order}}_{f_1}$$

$\deg < \deg f = n$

Define $f_1 = f_0 - g \cdot \left(\frac{a_n}{b_m} x^{n-m}\right)$.

Now repeat with f_1 in place of f_0.

Existence: We will define a sequence $f_0, f_1, \ldots, f_k$

$f_0 := f$ and

Suppose $f_i = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$

$g = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0.$

If $n < m$, stop.

Otherwise

$$f_i = g \cdot \left(\frac{a_n}{b_m} x^{n-m} \right) + \underbrace{\underbrace{\text{lower order}}_{\deg < \deg f = n}}_{f_{i+1}}$$

Define $f_{i+1} = f_i - g \cdot \left(\frac{a_n}{b_m} x^{n-m} \right)$.

This algorithm will terminate because $\deg f_{i+1} < \deg f_i$.

When it does, we will have $f = f_0 = g \cdot (\,) + f_1 = g \cdot (\,) + g(\,) + f_2 = \ldots$

When the algorithm terminates, we will have found

$$f = f_0 = g \times (\dots) + f_1 = g \times (\dots) + g \times (\dots) + f_2$$
$$= \dots = g \times (\text{something}) + f_k.$$

termination was when $\deg f_k < \deg g$.

So we set

$$r := f_k$$

$$q := (\text{something}). \qquad \square$$

Remark: Inspecting the existence algorithm, we see that the only divisions that occur in coefs are by leading coef of g.

For uniqueness, we needed ring of coefs to be a domain.

In other words, the same proof shows:

Thm: If R is a domain and $g \in R[x]$ is monic, then for any $f \in R[x]$ there are unique $q, r \in R[x]$ s.t. $f = qg + r$ and $\deg r < \deg g$.

Defn: A monic poly has leading coef $= 1$.

E.g.:

$$x^2+x+1 \;\big|\; x^4-2x^3+x^2+2x+1 \;=\; x^2+2x-2 =: q$$

$$x^4+x^3+x^2$$

$$-3x^3+0x^2+2x+1$$

$$-3x^3-3x^2-3x$$

$$3x^2+5x+1$$

$$3x^2+3x+3$$

$$2x-2 =: r$$

$f = f_0$

f_1

f_2

f_3

$\mathbb{F}_5[x]$

$\mathbb{F}_5 = \mathbb{Z}/5$

The basic question of alg geo is to find the zeros of polynomials.

Cor of Long division thm:

Let $\mathbb{F}$ a field, $f \in \mathbb{F}[x]$.

Then $a \in \mathbb{F}$ is a zero of f iff $x-a$ divides f.

Remark: Also works over any Domain.

Defn: g divides f if there exists z s.t. $f = z \cdot g$.

Pf: Write $f \overset{\star}{=} (x-a)\cdot q + r$.

$\deg r < \deg(x-a) = 1$ so $r \in \mathbb{F}$.

But now evaluate $\star$ at $x=a$, and

$f(a) = (a-a)\,q(a) + r(a) = r$. So $r = 0 \iff f(a) = 0$.

Corollary of the corollary:

A degree-n polynomial in $\mathbb{F}[x]$ (where $\mathbb{F}$ is a field (or domain)) has at most n distinct zeros. ($n \neq -\infty$)

Pf: Suppose $a_1, \dots, a_n$ are distinct zeros of $f \in \mathbb{F}[x]$. $=: f_0$

Then $f_0 = (x - a_1) \cdot f_1$ for some f_1, $\deg f_1 = \deg f - 1 = n - 1$.

$0 = f_0(a_2) = \underbrace{(a_2 - a_1)}_{\neq 0} f_1(a_2)$

Since $\mathbb{F}$ is a domain, a_2 is a zero of f_1

So $f_1 = (x - a_2) f_2$. By repeating, you eventually get

to f_N of degree $n-N$.

so $n-N \in \mathbb{N}$ so $n \geq N$. $\square$.

Recall Fermat's little theorem

$\forall\, a \not\equiv 0 \bmod p$, $a^{p-1} \equiv 1 \bmod p$.

this was simply the statement that

$\mathbb{F}_p := \mathbb{Z}/p$ was a field of order p and so

$(\mathbb{Z}/p)^\times = \mathbb{Z}/p \setminus \{0\}$ is a gp of order $p-1$.

Thm: $(\mathbb{Z}/p)^\times = (\mathbb{F}_p)^\times$ is a cyclic gp.

In fact: If $\mathbb{F}$ is any finite field, then $\mathbb{F}^\times$ is cyclic.

Pf: Let n be the exponent of $\mathbb{F}^\times$.

From the classification of finite ab gps, $\mathbb{F}^\times$ is cyclic $\Leftrightarrow$ $n = \#\mathbb{F}^\times$.

The poly $x^n - 1$ has $\#\mathbb{F}^\times$ many zeros. So $n \geq \#\mathbb{F}^\times$. □

Defn: If G is a gp, then the exponent of G is the smallest $n > 0$ s.t. $g^n = 1 \ \forall g \in G$.

N.B: exponent divides order.

Remarks:

- Finding a generator of $(\mathbb{Z}/p)^\times$ is not trivial.
- if you do have a generator

$$(\mathbb{Z}/5)^\times = \{2, \underset{\shortparallel}{2^2}, \underset{\shortparallel}{2^3}, \underset{\shortparallel}{2^4}\}.$$
$$\begin{matrix} \shortparallel & \shortparallel & \shortparallel \\ 4 & 3 & 1 \\ \shortparallel & & \\ -1 & & \end{matrix}$$

then you can talk about "finite log"

$$\log_2 : \mathbb{Z}/5 \to \mathbb{Z}/4 \cup \{-\infty\}$$
$$\log_2(0) = -\infty. \qquad \log_2(3) = 3.$$

Examples of finite fields:

$\mathbb{F}_p = \mathbb{Z}/p$. p a prime.

$\bar{\omega} = \omega^2 = \omega + 1$.

$\mathbb{F}_2 \subseteq \mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$.

$\mathbb{F}_4^\times = \{1, \omega, \bar{\omega}\} \simeq C_3$.

$\mathbb{F}_9 = \mathbb{F}_3[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{F}_3\}$

$(a + b\sqrt{-1})(c + d\sqrt{-1})$

$= (ac - bd)1 + (ad + bc)\sqrt{-1}$.