Math 5251 Polynomials (Chap. 10)

ACTIVE LEARNING

(1) Compute $\overline{20}^{-1}$ in $\mathbb{Z}/108$

(2) Can you compute

$$\mathrm{GCD}(x^5+x^3,\ x^4+1) \text{ in } \mathbb{F}_2[x] \text{ ?}$$

(Try Euclid's Algorithm!)

In fact, the same things we proved about division & Euclidean algorithm in $\mathbb{Z}$

also work in $\mathbb{F}[x]$ where $\mathbb{F}$ is any field,

like $\mathbb{F} = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{F}_2, \underset{p \text{ prime}}{\mathbb{F}_p}$

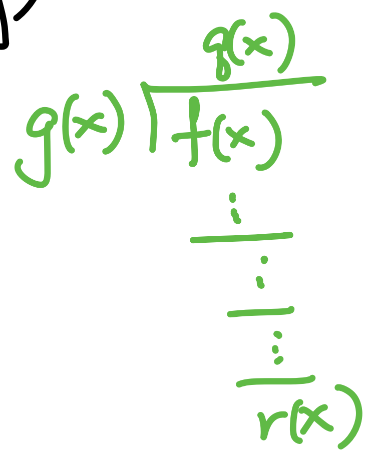
and for essentially the same reasons...

PROPOSITION Given $f(x), g(x) \in \mathbb{F}[x]$ for a field $\mathbb{F}$, there is a unique $q(x), r(x)$ with

$$f(x) = q(x) \cdot g(x) + r(x)$$

and $\quad 0 \le \deg(r) < \deg(g)$

proof: Use division algorithm



to find at least one such $q(x), r(x)$.

To see uniqueness, suppose

$$f(x) = q_1(x) \cdot g(x) + r_1(x)$$
$$= q_2(x) \cdot g(x) + r_2(x)$$

with $\quad 0 \le \deg(r_1), \deg(r_2) < \deg(g)$

Then subtracting gives

$$\underbrace{(q_1(x) - q_2(x)) \cdot g(x)}_{\substack{\text{degree} \ge \deg(g) \\ \text{if } q_1 \neq q_2}} = \underbrace{r_1(x) - r_2(x)}_{\text{degree} < \deg(g)}$$

$$\Rightarrow \quad q_1 - q_2 = 0 = r_1 - r_2 \quad \text{i.e. } q_1 = q_2,\ r_1 = r_2 \quad \blacksquare$$

PROPOSITION For any $f(x), g(x) \in \mathbb{F}[x]$ with $\mathbb{F}$ any field, there exists $d(x) \in \mathbb{F}[x]$ with

$$\underbrace{\mathbb{F}[x]\, f(x) + \mathbb{F}[x]\, g(x)}_{=\{a(x)f(x)+b(x)g(x):\ a,b\in\mathbb{F}[x]\}} = \underbrace{\mathbb{F}[x]\, d(x)}_{\text{multiples of } d(x)}$$

and $d(x)$ is unique if we further insist that it is monic, meaning $d(x) = x^r + d_{r-1}x^{r-1} + \dots + d_1 x + d_0$ for some $d_0, d_1, \dots, d_{r-1} \in \mathbb{F}$

Then we say $d(x) = GCD(f(x), g(x))$, since

- $d(x)$ is a common divisor of both $f(x), g(x)$
- any other common divisor $e(x)$ of $f(x), g(x)$ has $e(x) \mid d(x)$.

Also $\exists\ a(x), b(x) \in \mathbb{F}[x]$ with

$$a(x)f(x) + b(x)g(x) = d(x)$$

and one can compute $d(x)$ via Euclid's algorithm and compute $a(x), b(x)$ via extended Euclid's algorithm.

EXAMPLE What is $\mathrm{GCD}(x^5+x^3, x^4+1)$ in $\mathbb{F}_2[x]$?

$$
\begin{array}{r}
x \\
x^4+1 \overline{\big)\, x^5+x^3} \\
\underline{x^5+x} \\
x^3+x
\end{array}
$$

$$= \mathrm{GCD}(x^4+1, x^3+x)$$

$$= \mathrm{GCD}(x^2+1, x^3+x)$$

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

$$= x^2+1 \qquad \Big[= (x+1)^2$$

since

$$(x+1)^2 = x^2+\overset{0}{\cancel{2x}}+1 = x^2+1 \Big]$$

$$
\begin{array}{r}
x \\
x^2+1 \overline{\big)\, x^3+x} \\
\underline{x^3+x} \\
0
\end{array}
$$

Compare this with these **factorizations** in $\mathbb{F}_2[x]$:

$$x^5+x^3 = x^3(x^2+1) = x^3(x+1)^2$$

$$x^4+1 = (x+1)^4$$

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

We'll come back to factorization later!

(sketch) proof of PROP: Very similar to proof that $m\mathbb{Z}+n\mathbb{Z} = d\mathbb{Z}$ for $d=$ smallest nonnegative integer in $m\mathbb{Z}+n\mathbb{Z}$

Now we let $d(x)$ be the smallest degree monic polynomial in $\mathbb{F}[x]\cdot f(x) + \mathbb{F}[x]\cdot g(x)$.

Then similarly show

$$\mathbb{F}[x]\, d(x) = \mathbb{F}[x]\, f(x) + \mathbb{F}[x]\, g(x)$$

and $d(x)$ has the other properties. $\blacksquare$

REMARK $\mathbb{F}$ being a field does play a role here.

For example, $\mathbb{Z}$ is not a field and in $\mathbb{Z}[x]$, one can check that

$$\mathbb{Z}[x]\cdot \underset{f(x)}{x} + \mathbb{Z}[x]\cdot \underset{g(x)}{2} \neq \mathbb{Z}[x]\cdot d(x)$$

for any polynomial $d(x)$.

Euler's and Fermat's Theorems (§§6.10, 6.9)

= some amazing features of our finite rings $\mathbb{Z}/m$

DEF'N: In a ring R, the set of units is
$$R^\times := \{u \in R : u \text{ has a mult. inverse } u^{-1}\}$$
i.e. $u \cdot u^{-1} = 1$

EXAMPLES

(1) Fields $\mathbb{F}$ are exactly the rings for which $\mathbb{F}^\times = \mathbb{F} - \{0\}$

so $\mathbb{R}^\times = \mathbb{R} - \{0\}$
$\mathbb{C}^\times = \mathbb{C} - \{0\}$
$\mathbb{Q}^\times = \mathbb{Q} - \{0\}$
$\mathbb{F}_p^\times = \mathbb{F}_p - \{0\}$ if p is prime

(2) $\mathbb{Z}^\times = \{\pm 1\} \neq \mathbb{Z} - \{0\}$

(3) $(\mathbb{Z}/12)^\times = \{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11\}$
$= \{1, 5, 7, 11\}$

so $\varphi(12) := |(\mathbb{Z}/12)^\times| = 4$
Euler phi function

DEF'N: The power table for $(\mathbb{Z}/m)^\times$ lists $\bar{x}^i$ for $i = 1, 2, \ldots, \varphi(m)$

EXAMPLE $m = 12$ $\quad (\mathbb{Z}/12)^\times = \{1, 5, 7, 11\}$

x \ power	1	2	3	$4 = \varphi(12)$
1	1	1	1	1
5	5	1	5	1
7	7	1	7	1
11	11	1	11	1

ACTIVE LEARNING

(1) Write down $(\mathbb{Z}/m)^\times$ and its power table for $m = 5, 6, 7$. Make a conjecture based on this.

(2) Try to factor these polynomials as far as possible:

$x^2 - x$ in $\mathbb{F}_2[x]$

$x^3 - x$ in $\mathbb{F}_3[x]$

$x^5 - x$ in $\mathbb{F}_5[x]$

THEOREM: In a ring R where $R^\times$ is finite, say of cardinality $N := |R^\times|$, one has
$$u^N = 1 \quad \forall\, u \in R^\times.$$

$\Downarrow$ Take $R = \mathbb{Z}/m$, so $N = \varphi(m) = |(\mathbb{Z}/m)^\times|$

COROLLARY 1: (Euler's Thm) Every $\alpha \in (\mathbb{Z}/m)^\times$ has $\alpha^{\varphi(m)} = 1$ in $\mathbb{Z}/m$

$\Downarrow$ Let $m = p$ a prime, so $N = \varphi(p) = |(\mathbb{Z}/p)^\times|$
$= |\mathbb{Z}/p - \{0\}| = p-1$

COROLLARY 2: ("Fermat's "Little" Thm) Every $\alpha \in \mathbb{F}_p^\times = (\mathbb{Z}/p)^\times = \mathbb{F}_p - \{0\}$ satisfies $\alpha^{p-1} = 1$.

Consequently, every $\alpha \in \mathbb{F}_p$ satisfies $\alpha^p = \alpha$ is therefore a root of $f(x) = x^p - x$.

proof of THEOREM

A clever idea: list the elements of $R^\times$ as $r_1, r_2, \ldots, r_N$

e.g. $R = \mathbb{Z}/12$, $R^\times = (\mathbb{Z}/12)^\times = \{\underset{r_1}{\bar{1}}, \underset{r_2}{\bar{5}}, \underset{r_3}{\bar{7}}, \underset{r_4}{\overline{11}}\}$ $N=4$

Fix some $u \in R^\times$, for which we want to show $u^N = 1$.
Note that multiplication by u is a bijection $R^\times \to R^\times$
(Why - What is the inverse bijection?)

e.g. $u=5$, $R^\times = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$

$$\begin{array}{c} \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\} \\ \text{mult. by } u=5 \big\downarrow \quad \big\uparrow \text{mult. by } u^{-1} = 5^{-1} \\ \{\underset{ur_1}{\bar{5}}, \underset{ur_2}{\overline{25} = \bar{1}}, \underset{ur_3}{\overline{35} = \overline{11}}, \underset{ur_4}{\overline{55} = \bar{7}}\} \end{array}$$

Therefore, we should have

$$r_1 r_2 \cdots r_N = \prod_{\alpha \in R^\times} \alpha = (ur_1)(ur_2)\cdots(ur_N) = u^N \cdot r_1 r_2 \cdots r_N$$

$\Big\downarrow$ mult. by $r_1^{-1} r_2^{-1} \cdots r_N^{-1}$

$$1 = u^N \qquad \blacksquare$$

So since $f(x) = x^p - x$ has every $\alpha \in \mathbb{F}_p$ as a root for p prime, we'd like to conclude we can factor

$$x^p - x = \prod_{\alpha \in \mathbb{F}_p} (x-\alpha) \quad \text{in } \mathbb{F}_p[x]$$

e.g. $x^5 - x = x(x-1)(x-2)(x-3)(x-4)$

and that this factorization is unique, since each factor $x-\alpha$ is irreducible

can't be factored further

Does this work in $\mathbb{F}_p[x]$??

(Disturbing/Cautionary) EXAMPLE

Let $f(x) = x^2 - \bar{5}x = x(x-\bar{5})$ in $\mathbb{Z}/6[x]$

But also $f(x) = (x-\bar{2})(x-\bar{3})$

$$= x^2 - (\bar{2}+\bar{3})x + \bar{6} = x^2 - \bar{5}x$$

So $x(x-\bar{5}) = (x-\bar{2})(x-\bar{3})$ in $\mathbb{Z}/6[x]$

No unique factorization!

Also, $f(x)$ has $\bar{0}, \bar{5}, \bar{2}, \bar{3}$ as distinct roots, but is not divisible by $(x-\bar{0})(x-\bar{5})(x-\bar{2})(x-\bar{3}) = (x^2 - \bar{5}x)^2$

Not to worry: $\mathbb{F}_p$ being a field fixes both problems...

PROPOSITION: When $\mathbb{F}$ is a field, and $f(x) \in \mathbb{F}[x]$ that has ℓ distinct roots $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}$ will have
$f(x) = (x-\alpha_1)\cdots(x-\alpha_\ell)\,g(x)$ for some $g(x) \in \mathbb{F}[x]$
with $\deg(g) = \deg(f) - \ell$. In particular $\ell \leq \deg(f)$
so $f(x)$ can't have more than $\deg(f)$ distinct roots.

proof: Induction on ℓ.

BASE CASE: $\ell = 1$

If $\alpha_1 \in \mathbb{F}$ is a root of $f(x)$, use division algorithm to write $f(x) = (x-\alpha_1)\,q(x) + r$

with $0 \leq \deg(r) < 1 = \deg(x-\alpha_1)$

so $r \in \mathbb{F}$

$$x-\alpha_1 \overline{\big)\, f(x)}^{\,q(x)}$$
$\vdots$
r ← $\deg(r) < 1 \Rightarrow r$ constant

But then $0 = f(\alpha_1) = (\alpha_1 - \alpha_1)\,q(\alpha_1) + r$

$\Rightarrow \quad 0 = r$

$\Rightarrow \; f(x) = (x-\alpha_1)\,q(x)$

with $\deg(q) = \deg(f) - 1$ ✓

INDUCTIVE STEP: Assume $\ell \geq 2$.

Since $\alpha_1, \ldots, \alpha_{\ell-1}$ are distinct roots of $f(x)$, we know by induction $f(x) = (x-\alpha_1)\cdots(x-\alpha_{\ell-1})\,\hat{g}(x)$ where $\deg(\hat{g}) = \deg(f) - (\ell-1)$.

But since α_ℓ is also a root of $f(x)$,

$$0 = f(\alpha_\ell) = \underbrace{(\alpha_\ell - \alpha_1)}_{\neq 0} \cdots \underbrace{(\alpha_\ell - \alpha_{\ell-1})}_{\neq 0}\,\hat{g}(\alpha_\ell)$$

mult. by $(\alpha_\ell - \alpha_1)^{-1} \cdots (\alpha_\ell - \alpha_{\ell-1})^{-1}$ (using $\mathbb{F}$ a field)

$$0 = \hat{g}(\alpha_\ell)$$

, i.e. α_ℓ is a root of $\hat{g}(x)$.

Hence $\hat{g}(x) = (x - \alpha_\ell)\,g(x)$

and
$$\begin{aligned} f(x) &= (x-\alpha_1)\cdots(x-\alpha_{\ell-1})\,\hat{g}(x) \\ &= (x-\alpha_1)\cdots(x-\alpha_{\ell-1})(x-\alpha_\ell)\,g(x) \end{aligned}$$

where
$$\begin{aligned} \deg(g) = \deg(\hat{g}) - 1 &= \deg(f) - (\ell-1) - 1 \\ &= \deg(f) - \ell \end{aligned}$$

$\blacksquare$

What about unique factorization in $\mathbb{F}[x]$?

First, what should it mean...

DEF'N: Say $f(x) \in \mathbb{F}[x] - \{0\}$ is irreducible if the only factorizations $f(x) = g(x)h(x)$ have either $g(x)$ or $h(x)$ of degree 0, meaning a scalar in $\mathbb{F}^\times$.

EXAMPLE

$$x^3 - 1 = (x-1)(x^2+x+1) \text{ in } \mathbb{R}[x]$$

is not irreducible,

but $\left.\begin{array}{l} x-1 \\ x^2+x+1 \end{array}\right\}$ are both irreducible

$$\left(\text{even though } \begin{array}{l} x-1 = \frac{1}{2}\cdot(2x-2) \\ x^2+x+1 = 3\cdot\left(\frac{1}{3}x^2+\frac{1}{3}x+\frac{1}{3}\right) \end{array}\right)$$

Unique factorization into irreducibles in $\mathbb{F}[x]$

means one can write

$$f(x) = f_1(x) f_2(x) \cdots f_r(x) \text{ with } f_i \text{ irreducible,}$$

uniquely up to re-indexing or factoring out scalars in $\mathbb{F}^\times$

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

does not contradict unique factorization in $\mathbb{R}[x]$; they are all considered the same factorization.

The key here is a property of irreducibles in $\mathbb{F}[x]$ similar to primes p in $\mathbb{Z}$:

if a prime $p \mid ab$, then $p \mid a$ or $p \mid b$

EXAMPLES

(1) $\underset{\text{not prime}}{12} \mid 8\cdot 15 = 120$ but $12 \nmid 8$, $12 \nmid 15$

while $\underset{\text{prime}}{3} \mid 8\cdot 15 = 120$ forcing $\underset{\text{NO}}{\cancel{3 \mid 8}}$ or $\underset{\text{YES}}{3 \mid 15}$

(2) In $\mathbb{Z}/6[x]$, $x-\bar{2}$ is irreducible

and $x \mid x^2-\bar{5}x = (x-\bar{2})(x-\bar{3})$, but $x \nmid x-\bar{2}$, $x \nmid x-\bar{3}$

PROPOSITION: If $\mathbb{F}$ is a field and $f(x) \in \mathbb{F}[x]$ is irreducible, then $f(x) \mid g(x)h(x)$

$$\Rightarrow f(x) \mid g(x) \text{ or } f(x) \mid h(x).$$

proof:

Suppose $f \mid g \cdot h$, but $f \nmid g$. We'll show $f \mid h$.

Let $d(x) = GCD(f(x), g(x))$.

Then since $d \mid f$ and f is irreducible,

either $d(x) = 1$ or $\cancel{d(x) = f(x)}$.

Can't happen, else $f(x) = d(x) \mid g(x)$ (but $f \nmid g$)

So $1 = d(x) = GCD(f(x), g(x))$

$\Rightarrow 1 = a(x)f(x) + b(x)g(x)$ for some $a, b \in \mathbb{F}[x]$

{ mult. by $h(x)$

$$h(x) = \underbrace{\underbrace{a(x)f(x)h(x)}_{\text{div. by } f} + \underbrace{b(x)g(x)h(x)}_{\text{div. by } f}}_{\Rightarrow \text{ div. by } f}$$

, so $f \mid h$. ∎

COROLLARY For $\mathbb{F}$ a field, every $f(x) \in \mathbb{F}[x]$ can be written $f(x) = f_1(x) \cdots f_r(x)$ with each f_i irreducible, uniquely up to reindexing and multiplying f_i by scalars in $\mathbb{F}^\times$.

proof: Existence of some irreducible factorization is pretty easy by induction on $\deg(f)$: either f is irreducible, or factor it $f = g \cdot h$ with $\deg(g), \deg(h) > 0$

$$\Downarrow$$

$$\deg(g), \deg(h) < \deg(f)$$

$$\Downarrow \text{ induction}$$

$$g = g_1 \cdots g_\ell, \quad h = h_1 \cdots h_m$$

each g_i, h_j irreducible

$$\Downarrow$$

$$f = g_1 \cdots g_\ell h_1 \cdots h_m$$

For uniqueness, also induct on $\deg(f)$.

Assume $f = f_1 f_2 \cdots f_r = g_1 g_2 \cdots g_s$ with all f_i, g_j irreducible.

Since $f_1 \mid f = g_1 \cdot g_2 \cdots g_s$, either

$$f_1 \mid g_1 \quad \text{or} \quad f_1 \mid g_2 \cdots g_s$$

$\Downarrow$ $f_1 = c g_1$ for some $c \in \mathbb{F}^\times$

$\Downarrow$ keep going!

Eventually you conclude $f_1 = c g_j$ for some $c \in \mathbb{F}^\times$ and index j, so re-index to make $j=1$, and rescale the g_1, g_2 to make $f_1 = g_1$. Then

$$f = f_1 f_2 \cdots f_r = f_1 g_2 \cdots g_s$$

so

$$0 = f_1 f_2 \cdots f_r - f_1 g_2 \cdots g_s = \underbrace{f_1}_{\text{a nonzero polynomial in } \mathbb{F}[x]} \big(\underbrace{f_2 \cdots f_r - g_2 \cdots g_s}_{\text{this must be the zero polynomial}} \big)$$

$\Rightarrow$ $f_2 \cdots f_r = g_2 \cdots g_s$ and by induction on degree, can re-index and rescale to make $r=s$, $f_i = g_i$ ∎