proof: The existence of $q(x), r(x)$ given $f(x), g(x)$ comes from the usual division algorithm.

For uniqueness, if $g(x) = f(x)\,q_1(x) + r_1(x)$ with $\deg(r_1)$,
$= f(x)\,q_2(x) + r_2(x)$ $\quad \deg(r_2) < \deg(f)$,

then $\underbrace{f(x)}_{\text{monic of some degree } d}(q_1(x) - q_2(x)) = \underbrace{r_2(x) - r_1(x)}_{\text{degree strictly less than } d}$

$$\Rightarrow \begin{Bmatrix} q_1(x) - q_2(x) = 0 \\ r_2(x) - r_1(x) = 0 \end{Bmatrix} \quad \text{i.e.} \begin{Bmatrix} q_1 = q_2 \\ r_1 = r_2 \end{Bmatrix}$$ ∎

COROLLARY (11.2.10): The same holds when the leading coefficient of $f(x)$ lies in $R^\times$, and in particular for any $f(x) \neq 0$ when R is a field.

proof: If $f(x) = a_0 + a_1 x + \dots + a_n x^n$ and $a_n \in R^\times$

replace it by $a_n^{-1} f(x) = \frac{a_0}{a_n} + \frac{a_1}{a_n}x + \dots + \frac{a_{n-1}}{a_n}x^{n-1} + x^n$ which is monic,

then do $a_n^{-1}f(x) \overline{)\,g(x)}$ (quotient $q(x)$, remainder $r(x)$), and divide by a_n after. (q, r) ∎

NON-EXAMPLE: Can't divide everyone in $\mathbb{Z}[x]$ by $f(x) = 2x+1$ e.g. $g(x) = x^2$

The special case where $f(x) = x - \alpha$ relates to the substitution map $R[x] \to R$: $x \mapsto \alpha$

COROLLARY (11.2.11): The remainder when dividing $g(x) \in R[x]$ by $f(x) = x - \alpha$ for $\alpha \in R$ is the substitution $g(\alpha) \in R$

In particular,
- $g(\alpha) = 0 \iff x - \alpha$ divides $g(x)$
- when R is a domain, $g(x) \neq 0$ can have at most $\deg(g)$ distinct roots $r_i \in R$ ($g(r_i) = 0$)

NOTE: False, for R not a domain e.g. $g(x) = \bar{2}x \in \mathbb{Z}/4\mathbb{Z}[x]$ has 2 distinct roots $x = \bar{0}$, $x = \bar{2}$ but $\deg(g) = 1$

(and $g(x) = \bar{2}\cdot(x - \bar{0}) = \bar{2}(x - \bar{2})$)

(13)

2/4/2019

proof: Dividing $g(x)$ by $f(x) = x - \alpha$ gives

$$g(x) = (x-\alpha)\,q(x) + \underbrace{r(x)}_{\deg(r) < \deg(x-\alpha) = 1 \text{ i.e. } \deg(r) = 0 \text{ so } r(x) = r_0}$$

$$= (x-\alpha)\,q(x) + r_0$$

Apply the substitution homom. $R[x] \xrightarrow{\text{"}x=\alpha\text{"}} R$

gives $g(\alpha) = \underbrace{(\alpha-\alpha)}_{0}\,q(\alpha) + r_0 = r_0$.

Hence $g(\alpha) = 0 \iff r_0 = 0 \iff g(x) = (x-\alpha)q(x) \iff x-\alpha$ divides $g(x)$.

(uniqueness of q, r)

When R is a domain, show $g(x)$ has $\le \deg(g)$ distinct roots $r_i \in R$

by induction on $\deg(g)$. Base case $\deg(g) = 0$ is easy since $g \neq 0$,

so $g(x) = a_0 \neq 0$ has no roots.

In inductive step, if $g(x)$ has no roots, we're done.

If α_1 is a root, so $g(\alpha_1) = 0$, then division gives

$$g(x) = (x-\alpha_1)\underbrace{q(x)}_{\deg(q) = \deg(g)-1}$$

But every root $\alpha_2, \alpha_3, \ldots$ of $g(x)$ with $\alpha_i \neq \alpha_1$ is also a root of $q(x)$

because $0 = g(\alpha_i) = \underbrace{(\alpha_i - \alpha_1)}_{\neq 0}\,q(\alpha_i) \underset{\text{R a domain}}{\Rightarrow} q(\alpha_i) = 0$.

for $i \ge 2$

Hence there are at most $\deg(q) = \deg(g) - 1$ such $\alpha_2, \alpha_3, \ldots$

and so $\alpha_1, \alpha_2, \alpha_3, \ldots$ are at most $\deg(g)$ ∎

(14) Lets use this to deduce...

THEOREM: Every finite field $\mathbb{F}$ has $\mathbb{F}^\times$ cyclic,

i.e. if $|\mathbb{F}| = p^d$ then $\mathbb{F}^\times = \{1, \alpha, \alpha^2, \dots, \alpha^{p^d-2}\} = \langle \alpha \rangle$ for some $\alpha \in \mathbb{F}^\times$

$$\cong (\mathbb{Z}/(p^d-1)\mathbb{Z})^+$$

(EXAMPLES: ① $\mathbb{F}_7^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \{\bar{1}, \bar{3}, \bar{3}^2, \bar{3}^3, \bar{3}^4, \bar{3}^5\}$ $\quad \bar{2} = \bar{3}^2,\ \bar{6} = \bar{3}^3,\ \bar{4} = \bar{3}^4,\ \bar{5} = \bar{3}^5$

② $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, $\quad 1 = \alpha^3,\ \alpha+1 = \alpha^2$, $\quad \mathbb{F}_4^\times = \{1, \alpha, \alpha^2\} \cong (\mathbb{Z}/3\mathbb{Z})^+$)

proof: We claim that it follows easily from this

(group theory) LEMMA: In a finite abelian group G, there always exists some $g \in G$ whose order is $\operatorname{lcm}(\{\operatorname{ord}(h) : h \in G\}) =: \ell$

FALSE for nonabelian G e.g. $G = G_3$ has ord((12)) = 2, ord((123)) = 3, but no elements of order $6 = \operatorname{lcm}(2,3)$

Why? (the claim) Apply this lemma to $G = \mathbb{F}^\times$ (a finite abelian group) to find such an $\alpha \in \mathbb{F}^\times$ of order ℓ, and we'll show $\ell = |\mathbb{F}^\times|$, so $\langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{\ell-1}\} = \mathbb{F}^\times$.

Certainly ℓ divides $|\mathbb{F}^\times|$ since $\alpha^{|\mathbb{F}^\times|} = 1$ ($g^{|G|} = e$ in any finite group).

But since every $\beta \in \mathbb{F}^\times$ has $\operatorname{ord}(\beta)$ dividing ℓ $(= \operatorname{lcm}(\{\operatorname{ord}(\beta)\}_{\beta \in \mathbb{F}^\times})$,

they all have $\beta^\ell = 1$

$\Rightarrow \beta^\ell - 1 = 0$

i.e. β is a root of $x^\ell - 1$, a polynomial of degree ℓ

Thus $x^\ell - 1$ has $|\mathbb{F}^\times|$ distinct roots β, hence $|\mathbb{F}^\times| \le \ell$

$\Rightarrow |\mathbb{F}^\times| = \ell$.

---

proof of LEMMA: Write $\ell = \operatorname{lcm}\{\operatorname{ord}(h) : h \in G\} = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, p_i prime.

There must exist $h_1, \dots, h_r \in G$ with $\operatorname{ord}(h_i)$ divisible by $p_i^{e_i}$

hence also $\exists\ g_1, \dots, g_r \in G$ with $\operatorname{ord}(g_i) = p_i^{e_i}$ (why?)

We claim $g := g_1 g_2 \cdots g_r$ has order ℓ.

Certainly $g^\ell = (g_1 g_2 \cdots g_r)^\ell \overset{G \text{ abelian}}{=} g_1^\ell g_2^\ell \cdots g_r^\ell = 1 \cdot 1 \cdot \cdots \cdot 1 = 1$

and hence $\operatorname{ord}(g)$ divides ℓ.

On the other hand, if $\mathrm{ord}(g)$ strictly divides ℓ, we'll get a contradiction.

Pick one of the primes, say p_1 with $\mathrm{ord}(g)$ divisible only by $p_1^{d_1} < p_1^{e_1}$, not by $p_1^{e_1}$.

Writing $m := p_2^{e_2} \cdots p_r^{e_r}$, then

$$1 = g^{p_1^{d_1} m} = g_1^{p_1^{d_1} m} \, g_2^{p_1^{d_1} m} \cdots g_r^{p_1^{d_1} m}$$

Why?

$$= g_1^{p_1^{d_1} m} \cdot (g_2^m)^{p_1^{d_1}} \cdots (g_r^m)^{p_1^{d_1}}$$

$$= g_1^{p_1^{d_1} m} \cdot 1 \cdots 1$$

$$\Rightarrow 1 = g_1^{p_1^{d_1} m}$$

Now pick $n := m^{-1} \bmod p_1^{e_1}$, using $\gcd(p_1^{e_1}, \underbrace{p_2^{e_2} \cdots p_r^{e_r}}_{= m}) = 1$

so $nm = k \cdot p_1^{e_1} + 1$ for some $k \in \mathbb{Z}$

and $1 = 1^n = (g_1^{p_1^{d_1} m})^n = (g_1^{nm})^{p_1^{d_1}}$

$$= \left(g_1^{k p_1^{e_1} + 1}\right)^{p_1^{d_1}}$$

$$= \left((g_1^{p_1^{e_1}})^k \cdot g_1^1\right)^{p_1^{d_1}} = g_1^{p_1^{d_1}} \neq 1. \text{ Contradiction } \blacksquare$$