Last week

Cor 30 F : a field

$\alpha \in F$

Then the remainder of $f \in F[x]$ when divided by $x - \alpha$ is $f(\alpha)$
$\;\; = f(x)$

In particular,

$$f(\alpha) = 0 \Leftrightarrow x - \alpha \text{ divides } f(x).$$

<u>Example</u> $F = \mathbb{F}_7 = \{ [0], [1], \ldots$

$\ldots [6] \}$

$f(x) = x^2 + 3$

in $\mathbb{F}_7[x]$

<u>Claim</u>

$x - [2]$ divides $x^2 + [3]$

<u>Pf</u> $\alpha = [2]$

Need to check that

$f([2]) = [2]_7^2 + [3]_7 \overset{?}{=} [0]_7$

$= [4]_7 + [3]_7 = [7]_7$

By Corollary 30,

$x - [2]$ divides

$f(x) = x^2 + [3]$

similarly $x + [2]$ divides $x^2 + [3]$

In fact

$$x^2 + [3] = (x - [2])(x + [2])$$

$$[3] = [-4] = -[4]$$

$$x^2 + [3] = x^2 - [4]$$

$$= x^2 - [2]^2$$

$$= (x + [2])(x - [2])$$

- Let's consider $F = \mathbb{F}_5$

$$\mathbb{F}_5 = \{[0], \cdots, [4]\}$$

$f(x) = x^2 + 2$ is irreducible, i.e.

no non-trivial polynomial in $\mathbb{F}_5[x]$

divides $f(x)$.

In this set-up, this means that no polynomial of degree 1 divides $f(x)$

, i.e. x^2+2 is <u>NOT</u> of the form

$$(x+[a])(x+[b]) \quad [a],[b] \in \mathbb{F}_5$$

To do this, we use Cor 30.

By Cor 30, if $f(\alpha) \neq [0]$

for any $\alpha \in \mathbb{F}_5$,

then $f(x)$ is NOT divisible by

$x - \alpha$ for any α.

α	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$f(\alpha)$	$[2]$	$[3]$	$[6]$	$[11]$	$[18]$
$\parallel$			$\parallel$	$\parallel$	$\parallel$
α^2+2			$[1]_5$	$[1]_5$	$[3]$

Therefore $f(x)$ can not be

divided by a polynomial of the form

$x - \alpha$

Theorem 31 (The fundamental theorem of Algebra)

If $f = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$

$c_n \neq 0 \qquad c_i \in \mathbb{C}$.

then f has a root in $\mathbb{C}$,

i.e. $\exists\, \alpha \in \mathbb{C}$ s.t. $f(\alpha) = 0$

Theorem 32 f as above.

Then there exist $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$

$$f(x) = c_n (x-\alpha_1) \cdots (x-\alpha_n)$$

i.e. $\quad f(\alpha_i) = 0 \quad 1 \le i \le n.$

Rk Some of the α_i's might be equal.

Pf "Complex analysis"

Recall that x^2+1 does not have a root in $\mathbb{Q}[x]$

but it has a root in $\mathbb{C}[x]$.

Def We say that a polynomial

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in F[x]$$

is **monic** if the leading coefficient

c_n is $1 = 1_F$

(the identity w.r.t. $\times$ in $(F, +, \times)$)

__Rk__ The zero polynomial is defined to be monic.

__Rk__ The degree 0 monic polynomial is 1

(__NOT__ any element $c \in F^\times$)

__Def__ F : a field

(e.g. $F = \mathbb{Q}$

$= \mathbb{F}_p$

$= \mathbb{C}$)

Given $f, g \in F[x]$,

the gcd of f & g is

a polynomial $h \in F[x]$

- h divides f

  & h divides g

- if h' is a polynomial in $F[x]$

  that divides both f and g

then h' divides h.

- h is $\boxed{\text{monic}}$

(Rk Without this condition, h that satisfies the first two and ch can both be gcds of f and g, $c \in F^\times = F - \{0\}$.)

Rk Recall $a, b \in \mathbb{Z}$

the gcd of a & b is defined to be an integer $g \in \mathbb{Z}$

- g divides a

  & divides b

- if g' divides a and b,

  then g' divides g

- $g \geq 0$

Theorem 33 Let $f, g \in F[x]$

- There is a gcd of f and g.

  in $F[x]$.

- The gcd of f and g can be computed by Euclid's algorithm.

(based on Theorem 28)

- There exist p and q in $F[x]$

$$f \cdot p + g \cdot q = \gcd(f, g).$$

(as in Bezout's identity in Week 1).

Theorem 28

$f \in F[x]$

$g \neq 0$

$$f = g \cdot q + r$$

for some $q, r \in F[x]$

where $r = 0$

or

$\deg(r) < \deg(g)$

Example $f(x) = x^4 + 2x^3 + x^2 - 4$

$g(x) = x^3 - 1$, in $\mathbb{Q}[x]$.

- $x^4 + 2x^3 + x^2 - 4 = (x^3 - 1)\underbrace{(x+2)}_{= q}$

$+ x^2 + x - 2$

r

$$x^3 - 1 = \underbrace{(x-1)}_{q}(x^2 + x - 2) + \underbrace{(3x-3)}_{r}$$

$$x^2 + x - 2 = \frac{1}{3}(x+2)(3x-3) + \underline{0}$$

$\Rightarrow$ $3x - 3$ is a common divisor.

Since this is <u>not</u> monic,

the $\gcd(f, g) = x - 1$.

Exercise Find $p, q \in \mathbb{Q}[x]$

s.t.

$$(x^4+2x^3+x^2-4)\cdot p$$

$$+ (x^3-1)\cdot q = x-1$$

From the second line of E.A's.

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

Substituting the relation

$$x^2+x-2 = f(x) - (x+2)g(x)$$

from the 1st line into

$$3x-3=\underbrace{(x^3-1)}_{g(x)}-(x-1)\big(f(x)-(x+2)g(x)\big)$$

$$=-(x-1)f(x)+\big(1+(x-1)(x+2)\big)g(x)$$

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

Therefore

$$x-1=-\frac{1}{3}(x-1)f(x)$$

$$+ \frac{1}{3}(x^2 - x - 1)\, g(x). \quad \square$$

<u>Example</u>

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

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

in $\mathbb{F}_2[x]$

$$\mathbb{F}_2 = \{[0], [1]\}.$$

$$[1] + [1] = [2] = [0]$$

Instead of x^4+1,

use $(x+1)^4$

$$\text{because} \quad (x+1)^4 = x^4 + \underset{\substack{\shortparallel \\ 4}}{\binom{4}{1}} x^3 + \underset{\substack{\shortparallel \\ 6}}{\binom{4}{2}} x^2 + \underset{\substack{\shortparallel \\ 4}}{\binom{4}{3}} x + 1$$

$$= x^4 + [4]x^3 + [6]x^2 + [4]x + [1]$$

$$= x^4 + [1] \quad \text{because} \quad [4]_2 = [0]_2$$

$$[6]_2 = [0]_2$$

- $$(x+1)^4 = \underbrace{\left(\begin{matrix}(x+1)^2 \\ + \\ (x+1)+1\end{matrix}\right)}_{\substack{\shortparallel \\ q}}(x^2+x) + \underbrace{x+1}_{\substack{\shortparallel \\ r}}$$

- $$x^2+x = x\ (x+1) + 0$$

$\Rightarrow$ $x+1$ is the gcd.

Furthermore,

$$x+1 = 1\cdot(x+1)^4$$
$$- \left((x+1)^2 + (x+1) + 1 \right)(x^2+x)$$

Example

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

$$g(x) = x^2 + x \quad \text{in } \mathbb{Q}[x]$$

What is gcd? What are "p"s "q"

- $\underbrace{x^4 + 1}_{f} = \underbrace{(x^2 - x + 1)}_{q}\underbrace{(x^2 + x)}_{g} + \underbrace{(-x + 1)}_{\text{"}r\text{"}}$

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

- $-x + 1 = \frac{1}{2}(-x + 1)2 + 0$

Since 2 is NOT monic,

the gcd is 1.

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

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

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

$$= (x+2)f(x) + (-x^3-x^2+x$$

$$-1)g(x)$$

Therefore

$$\underline{1} = \gcd(f, g)$$

$$= (x+2)f + (-x^3 - x^2 + x - 1)g$$