① 5/1/2020

Let F be a field. For $f(x)$ and $g(x)$ in $F[x]$ there exist unique $q(x)$ and $r(x)$ with $\deg r(x) < \deg g(x)$ or $r(x)=0$

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

<u>Ex</u> $f(x) = x^4+x^3+x-1 \quad g(x) = x^2+1$ in $\mathbb{Q}[x]$

$$
\begin{array}{r|l}
 & x^2+x-1 \\
\hline
x^2+1 & x^4+x^3+x-1 \\
 & x^4+x^2 \\
\hline
 & x^3-x^2+x-1 \\
 & x^3+x \\
\hline
 & -x^2 \cancel{+x} - 1 \\
 & -x^2-1 \\
\hline
 & \cancel{2x}\ 0
\end{array}
$$

same thing in $\mathbb{F}_5[x]$

$$
\begin{array}{r|l}
 & x^2+x-1 \\
\hline
x^2+1 & x^4+x^3+x-1 \\
 & x^4+x^2 \\
\hline
 & x^3-x^2+x-1 \\
 & x^3+x \\
\hline
 & -x^2-1 \\
 & -x^2-1 \\
\hline
 & 0
\end{array}
$$

② $(x^2+1)(x^2+x-1) = x^4+x^3+x-1$ in $\mathbb{Z}[x]$

$$\varphi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$$
$$x \mapsto x+5\mathbb{Z} = [x]_5$$

$$\Phi : \mathbb{Z}[x] \to \mathbb{Z}_5[x]$$
$$f(x) = \sum a_i x^i \longmapsto \sum (a_i + 5\mathbb{Z}) x^i$$
$$\sum [a_i]_5 x^i$$

is a ring homo'sm.

$$\Phi((x^2+1)(x^2+x-1)) = \Phi(x^2+1)\,\Phi(x^2+x-1)$$

$$\boxed{-a_n b_m^{-1} x^{n-m}}$$

In $\mathbb{Z}_5[x]$

$$\begin{array}{r|l}
 & x^3 - x^2 + 2x + 2 \\
x+2 & x^4 + x^3 + x - 1 \\
 & x^4 + 2x^3 \\ \hline
 & -x^3 + x - 1 \\
 & -x^3 - 2x^2 \\ \hline
 & 2x^2 + x - 1 \\
 & 2x^2 + 4x \\ \hline
 & -3x - 1 = 2x+4 \\
 & 2x - 4 \\ \hline
 & -5x - 5 = 0
\end{array}$$

(3) In $\mathbb{Q}[x]$

$$
\begin{array}{r|l}
 & x^3 - x^2 + 2x - 3 \\
\hline
x+2 & x^4 + x^3 + x - 1 \\
 & x^4 + 2x^3 \\
\hline
 & -x^3 + x - 1 \\
 & -x^3 - 2x^2 \\
\hline
 & 2x^2 + x - 1 \\
 & 2x^2 + 4x \\
\hline
 & -3x - 1 \\
 & -3x - 6 \\
\hline
 & 5
\end{array}
$$

$$x^4 + x^3 + x - 1 = (x+2)(x^3 - x^2 + 2x - 3) + 5$$

$$\Phi(x^4 + x^3 + x - 1) = \Phi(x+2)(x^3 - x^2 + 2x - 3) + \underset{0}{\underset{\shortparallel}{\Phi(5)}}$$

(4)

Thm Let F be a field and $f(x), g(x)$ in $F[x]$. Repeated application of division algorithm yields:

$$
\begin{aligned}
&(1) \quad f(x) = q_1(x) g(x) + r_1(x) \\
&(2) \quad g(x) = q_2(x) r_1(x) + r_2(x) \\
&(3) \quad r_1(x) = q_3(x) r_2(x) + r_3(x) \\
&\qquad \vdots \\
&(n) \quad r_{n-2}(x) = q_n r_{n-1}(x) + r_n(x) \\
&(n+1) \quad r_{n-1}(x) = q_{n+1}(x) r_n(x) + 0
\end{aligned}
$$

and $r_n(x)$ is a gcd of $f(x)$ and $g(x)$

pf: $\deg g > \deg r_1 > \deg r_2 > \ldots$ means that the process stops.

		$d \mid f$ and $d \mid g$
$(n+1)$:	$r_n \mid r_{n-1}$	(1) $d \mid r_1$
(n)	$r_n \mid r_{n-2}$	(2) $d \mid r_2$
$(n-1)$	$r_n \mid r_{n-3}$	(3) $d \mid r_3$
$\vdots$	$\vdots$	$\vdots$
(3)	$r_n \mid r_1$	(n) $d \mid r_n$
(2)	$r_n \mid g$ } a common divisor	
(1)	$r_n \mid f$ }	$\square$

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

Ex $\gcd(\underset{f}{x^5+1},\ \underset{g}{x^3+1})$ in $\mathbb{Q}[x]$

(1) $f = \underset{q_1}{x^2}(x^3+1) \underset{r_1}{- x^2+1}$

$g = \underset{q_2}{(-x)}(\underset{r_1}{-x^2+1}) + \underset{r_2}{(x+1)}$

$$
\begin{array}{r}
x^2 \\
x^3+1 \,\big)\, \overline{x^5+1} \\
x^5+x^2 \\
\hline
-x^2+1
\end{array}
\qquad
\begin{array}{r}
-x \\
-x^2+1 \,\big)\, \overline{x^3+1} \\
x^3-x \\
\hline
x+1
\end{array}
$$

$r_1 = -(x-1)(x+1) + 0$

$\therefore \gcd(f,g) = r_2 = x+1$

Ex $f = x^3+4x^2+x-1$ in $\mathbb{Z}_5[x]$

$g = x^3-x^2-x+1$

$f = \underset{q_1}{1}\cdot g + (\underset{r_1}{2x+3})$

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

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

$\gcd(f,g) = r_1$

$= 2x+3$

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

(6)

Def A $a \in F$ is a zero for $f(x)$ in $F[x]$ if $f(a) = 0$.

Thm In $F[x]$ one has $(x-a) \mid f(x)$ if and only if $f(a) = 0$.

Pf If: $f(x) = q(x)(x-a)$

then $f(a) = q(a)(a-a) = 0$

Only if:

$$f(x) = q(x)(x-a) + r(x),$$

with $r(x) = 0$ or $\deg r(x) = 0$

$$0 = f(a) = q(a)(a-a) + r(a)$$

$$= r(a)$$

$\therefore \quad r = 0$