§6.1)

polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

a_k coefficient.

n degree.

$$= \sum_{k=0}^{n} a_k x^k$$

coefficients can be from $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$,

....

The set of polynomial with coef. in $\mathbb{R}$

$\mathbb{R}[x]$

(The set of polynomials with coef $\mathbb{Z}_p$

$\mathbb{Z}_p[x]$.)

A root of a polynomial f is x with

$f(x) = 0$.

In general not so easy to find roots.

deg $= 2$: $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

deg $= 3$: $x = \cdots\cdots$

deg $= 4$: $x = \cdots\cdots$

deg ≥ 5 : there is not such a formula (Abel, Galois)

Thm Every polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Addition of polynomials:

add coef of the same exponent.

Ex) $(3x^5 + 7x^3 - 10x^2) + (-7x^3 + 4x^2 - 3x + 1) =$

$3x^5 + (7-7)x^3 + (-10+4)x^2 - 3x + 1 =$

$3x^5 - 6x^2 - 3x + 1$

Lem $(\mathbb{R}[x], +)$ Abelian group.

Multiplication of polynomials

Just write out the product collecting coef of the same exponet

$$(3x^{5}+7x^3)(-3x^{4}+x^3-9x^2+1) =$$

$$\cancel{-9x^9} + \cancel{3x^8} - \cancel{27x^7} + \cancel{3x^5} +$$
$$-\cancel{21x^7} + \cancel{7x^6} - \cancel{63x^5} + \cancel{7x^3} =$$

$$-9x^9 + 3x^8 - 48x^7 + 7x^6 - 60x^5 + 7x^3$$

Lem $\deg(fg) = \deg(f) + \deg(g)$.

$(\mathbb{R}[x], +, \cdot)$ cummutative Ring.

Rmk: Every polynomial has an additive inverse $f + (-f) = 0$

Not every polynomial has a multiplicative inverse

$$x \cdot \boxed{\frac{1}{x}} = 1$$ Not a polynomial.

Examples in $\mathbb{Z}_p[x]$.

$p=2$: $(x^2+x+1)+(x^2+1) = 2x^2+x+2 = x$

$p=3$: $(x+2)^2 = x^2+4x+4 = x^2+x+1$

you have to calculate as usual

and take mod p.

Roots of $f \in \mathbb{Z}_p[x]$

If p is small just check each x.

$\boxed{p=2}$ $\quad x^2+1 = \begin{cases} 1 & x=0 \\ 2=0 & \underline{x=1} \end{cases}$

$x=1$ is a root.

$x^2+x+1 = \begin{cases} 1 & x=0 \\ 1 & x=1 \end{cases}$

No roots

§6.2

Thm (Division Thm for polynomials).

$f, g \in \mathbb{R}[x]$ $\quad \deg g \geq 0$

Then $\exists$ $q \in \mathbb{R}[x]$ and $r \in \mathbb{R}[x]$

$$f = qg + r$$

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

Before the proof let's use "Long Division" to find q and r.

Ex) $f = x^4 - 3x^2 + 2x - 4$

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

$$
\begin{array}{r|l|l}
\overbrace{x^2-3x+2}^{g} & \overbrace{\boxed{x^4} - 3x^2 + 2x - 4}^{f} & \overbrace{x^2 + 3x + 4}^{q} \\
 & \underline{\boxed{x^4} - 3x^3 + 2x^2} \quad - & \\
 & \boxed{3x^3} - 5x^2 + 2x - 4 & \\
 & \underline{\boxed{3x^3} - 9x^2 + 6x} \quad - & \\
 & \quad \boxed{4x^2} - 4x - 4 & \\
 & \quad \underline{\boxed{4x^2} - 12x + 8} \quad - & \\
 & \quad \quad \underbrace{8x - 12}_{r} &
\end{array}
$$

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

$$\underbrace{(x^2+3x+4)}_{q}\underbrace{(x^2+3x+2)}_{g}+\underbrace{8x-12}_{r}$$

<u>Check!</u>

$\boxed{\text{Ex}}$ $f=3x^4-7x^3+5x^2-x+3$

$g=x^2-3x+8$

$$
\begin{array}{l|l|l}
x^2-3x+8 & \boxed{3x^4}-7x^3+5x^2-x+3 & 3x^2+2x-13 \\
 & \underline{\boxed{3x^4}-9x^3+24x^2} \quad - & \\
 & \boxed{2x^3}-19x^2-x+3 & \\
 & \underline{\boxed{2x^3}-6x^2+16x} \quad - & \\
 & \boxed{-13x^2}-17x+3 & \\
 & \underline{\boxed{-13x^2}+39x-104} \quad - & \\
 & -56x+107 &
\end{array}
$$

$$3x^3-7x^3+5x^2-x+3=$$

$$(3x^2+2x-13)(x^2-3x+8)+(-56x+107)$$

Proof Division Thm

Let $S = \{ f - gt \mid t \in \mathbb{R}[x] \}$.

(Assume $\deg(f) \geq \deg(g)$
otherwise let $q = 0$ and $r = f$)

$S \neq \phi$

Let $D = \{ \deg(s) \mid s \in S \}$.

$D \neq \phi$

Take a minimal degree in D. Say $r \in S$

$$\deg(r) = \min D = k.$$

So $f = qg + r$.

We need to show $\deg(r) < \deg(g)$.

Let $g = b_0 + b_1 x + \cdots + b_m x^m \qquad b_m \neq 0$

$\quad r = c_0 + c_1 x + \cdots + c_k x^k \qquad c_k \neq 0.$

Assume $k \geq m$.

Consider.

$$r' = \underbrace{r - \frac{c_k}{b_m} x^{k-m} g}_{\deg < \deg r} = f - qg - \frac{c_k}{b_m} x^{k-m} g$$

$$= f - \left(q + \frac{c_k}{b_m} x^{k-m}\right) g \in S.$$

but $\deg(r') < \deg(r)$. Contradiction because $\deg(r)$ is minimal degree among poly in S $\square$.

<u>Definition</u>: The poly g divides f if $\exists$ a poly q s.t.

$$f = q \cdot g.$$

<u>Lemma</u>: α zero of $f \Longleftrightarrow$ $x - \alpha$ divides f.

So if $\alpha_1 \cdots \alpha_n$ are the roots of the poly g. then

$$g(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

The roots help to factorize a poly.

Ex) Factorize $x^3+6x^2+11x+6 = f$

Try some integer $x = -2, -1, 0, 1, 2$.

$x=-1$ is a root. So $x+1$ divides f.

$$f = (x+1)(x^2+5x+6)$$ Long division

$x=-2$ is a root of x^2+5x+6

$$f = (x+1)(x+2)(x+3)$$ long division.

Ex) Factorize x^3+2x^2+x+2 over $\mathbb{Z}_3$

Try $0, 1, 2$ for the roots.

$x=1$ is a root.

Use Long division

$$\begin{array}{r|l|l} x-1 & x^3+2x^2+x+2 & x^2+1 \\ & \underline{x^3-x^2} & \\ & \quad 3x^2+x+2 & \\ & \quad \underline{\quad x-1} & \\ & \qquad 3 = 0 & \end{array}$$

$0 \xrightarrow[\mathbb{Z}_3]{}$

$3 \underset{\mathbb{Z}_3}{=} 0$

So $x^3+2x^2+x+2 = (x-1)(x^2+1)$

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

Maybe x^2+1 has a root? Try

$x=0,1,2$ are all no roots.

So x^2+1 can not be factorized.

<u>Prop</u> $f, g \in \mathbb{R}[x]$ then

1) $\exists\, d \in \mathbb{R}[x]$ d divides f and g.

2) If c divides f and g then

c divides d.

The proof is the same as for the similar proposition for $\gcd(a,b)$.

d is called the g.c.d.

d is unique up to a scalar

<u>Prop</u>: $f, g \in \mathbb{R}[x]$

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

$$\gcd(f,g) = \gcd(g,r)$$

Hence we can also apply the Euclidean Algorithm for poly's.

<u>Ex</u> determine the gcd of

$$\begin{cases} f(x) = x^4 - 5x^3 + 7x^2 - 5x + 6 \\ g(x) = x^3 - 6x^2 + 11x - 6 \end{cases}$$

Find q, r s.t. $f = qg + r$.

$$
\begin{array}{r|l|l}
x^3-6x^2+11x-6 & x^4-5x^3+7x^2-5x+6 & x+1 \\
 & x^4-6x^3+11x^2-6x & - \\
\hline
 & x^3-4x^2+x+6 & \\
 & x^3-6x^2+11x-6 & - \\
\hline
 & 2x^2-10x+12 &
\end{array}
$$

Let $q = x+1$ $\quad r = 2x^2-10x+12$.

So $\gcd(f,g) = \gcd(g,r)$.

Find q_2, r_2 s.t. $g = q_2 r + r_2$.

$$
\begin{array}{r|l|l}
2x^2-10x+12 & x^3-6x^2+11x-6 & \frac{1}{2}x-\frac{1}{2} \\
 & x^3-5x^2+6x & \\
\hline
 & -x^2+5x-6 & \\
 & -x^2+5x-6 & \\
\hline
 & 0 &
\end{array}
$$

So

$$g = \left(\tfrac{1}{2}x-\tfrac{1}{2}\right)\underbrace{(2x^2-10x+12)}_{r}$$

so $\gcd(f,g) = \gcd(g,r) = r = 2x^2-10x+12$.

You can also use x^2-5x+6 as gcd.

Ex) What is the gcd of

$g = x^3 + x + 1$

$f = x^4 + x^3 + x + 1$

over $\mathbb{Z}_2$.

Use division alg. $f = qg + r$.

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

So $q = x+1$ and $r = -x^2 - x$.

So $\gcd(f,g) = \gcd(g, -x^2-x)$

$= \gcd(g, x^2+x)$

$$
\begin{array}{r|l|l}
x^2+x & x^3+x+1 & x-1 \\
 & \underline{x^3+x^2} \; - & \\
 & -x^2+x+1 & \\
 & \underline{-x^2-x} & \\
 & 2x+1 &
\end{array}
$$

$$\underset{\mathbb{Z}_2}{=} 1$$

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

$$\gcd(g, x^2+x) = \gcd((x^2+x), 1) = 1.$$