LN XIIIa

§6.3)

Definition a non-constant poly f is **irreducible**:

$f = gh \implies g = \text{constant}$ or $h = \text{constant}$

Ex) 1, $x-3$

Definition a non-constant poly f is **prime**:

f divides $rs \implies f$ divides r or f divides s.

For $f \in \mathbb{C}[x], \mathbb{R}[x]$ these notion are equivalent as they are for numbers. There are ~~fields~~ Rings for which these notions are not equivalent, $F[x]$.

Prop) $f \in \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_p[x]$

If f is irreducible then f is prime.

Pf) f is irreducible and

f divides rs

The $\gcd(f,r) = c$ or f.

$\quad\quad\quad\quad\quad\uparrow$ constant

If $\gcd(f,r) = f$ the f divides r. Done.

Suppose $\gcd(f,r) = c$. Then f does not divide r.

The Division algorithm gives poly u, v. s.t.

$$c = fu + rv.$$

So

$$\left.\begin{array}{l} cs = fus + rsv \\ f \text{ divides } rs \end{array}\right\} \Longrightarrow f \text{ divides } s.$$

$\square$.

<u>Corollary</u> If f is irreducible and

f divides $f_1 f_2 \cdots f_r$

then $\exists\, i$ s.t.

f divides f_r.

Prop If f is prime then f is irreducible. ($f \in \mathbb{R}[x], \mathbb{C}[x]$, $\mathbb{Z}_p[x]$)

Pf Suppose f is prime and

$$f = gh$$

Then f divides either g or h. (because f is prime).

Suppose

$$\deg(f) = n \quad \deg(g) = m \quad \deg(h) = k$$

then $n = m + k$.

f divides either g or h. So $n \leq m$ or ~~m~~ $n \leq k$. $\Longrightarrow$

either $m = 0$ or $k = 0$. This means either g or h is a constant. So f is irreducible

$\square$.

$f \in \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_p[x]$

f is prime $\iff$ f is irreducible.

The same as for numbers.

What about factorization of poly.?

<u>Thm</u> $\forall f \in \mathbb{R}[x]$ or $\mathbb{C}[x]$

$$f = f_1 \cdots f_r$$

where each f_i is irreducible. This factorization is unique. (

$$f_1 f_2 \cdots f_r = g_1 g_2 \cdots g_s \implies r = s \text{ and}$$

$$f_i = c_i g_i \;)$$

<u>Pf</u> <u>Part I</u>: there exists a factorization.

The proof is by induction in the degree of f.

If $\deg(f) = 1$ then $f = c(x-\alpha)$. Hence f is irreducible.

Suppose the existence has been shown for all degrees $\leq n$.

let f with $\deg(f) = n+1$

If f is irreducible then $f_1 = f$. Done

If f is not irreducible then

$$f = g \cdot h$$

~~with~~ with $\deg(g), \deg(h) \leq n$. So by Induction

$$g = g_1 \cdots g_r \quad g_i \text{ irreducible}$$
$$h = h_1 \cdots h_s \quad h_j \text{ irreducible}$$

So $\quad f = g_1 g_2 \cdots g_r h_1 h_2 \cdots h_s$

f has a factorization in irreducible factors

<u>Part II</u> Uniqueness.

Proof by induction in r, the number of factors.

<u>$r=1$</u>: f is irreducible.

If $f = g_1 g_2 \cdots g_s$ then $s = 1$ <u>Done</u>

Suppose the uniqueness has been shown for poly with r factors.

Suppose

$$f = f_1 \cdots f_{r+1} = g_1 g_2 \cdots g_s.$$

where f_i and g_j are irreducible.

f_1 divides f. Hence f_1 divides $g_1 g_2 \cdots g_s$.

So f_1 divides some g_j (say f_1 divides g_1).

f_1 g_1 are both irreducible: $g_1 = c_1 f_1$

c_1 a constant.

So

$$\underbrace{f_2 \cdots f_{r+1}}_{r} = g_2 \cdots g_s$$

The Induction hypothesis says. $s = r+1$

$f_i = g_i$ (up to a constant).

$\square$.

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

$f(1) = 0 \quad f(-1) = 0 \quad f(-2) = 0$

$$f(x) = (x-1)(x+1)(x+2).$$

irreducible.

-

- ## Fundamental Theorem of Algebra

$f \in \mathbb{C}[x]$ $\deg(f) = n$ then

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

$\alpha_i \in \mathbb{C}$.

- Every $f \in \mathbb{C}[x]$ can be factorized into linear factors.

-

Lets consider x^2+1

$x^2+1 \in \mathbb{C}[x]$: $x^2+1 = (x+i)(x-i)$

$x^2+1 \in \mathbb{R}[x]$: irreducible

$x^2+1 \in \mathbb{Z}_2[x]$: $(x^2+1) = (x+1)^2$.

$x^2+1 \in \mathbb{Z}_3[x]$: No zero, No linear factor So x^2+1 is irreducible.

§6.2 continued,

Recall: * a poly f is irreducible.

$f = gh \Rightarrow g$ or h constant

* a poly f is a prime

$f \mid rs \Rightarrow f \mid r$ or $f \mid s$.

* Factorization Thm $\forall f$.

$f = f_1 f_2 \cdots f_r$

where each f_i is irreducible. The factorization is unique.

* Fund. Thm. of Alg. $f \in \mathbb{C}[x]$

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

Cor: over $\mathbb{C}$ only the linear poly are irreducible.

Let $f \in \mathbb{R}[x]$

If $\alpha \in \mathbb{C}$ is a root then $\bar{\alpha}$ is also a root.

factorize f over $\mathbb{C}$

$$f = c\,\underbrace{(x-\alpha)(x-\bar{\alpha})}\cdots$$

$$= c\left(x^2 - \underset{\mathbb{R}}{\underset{\uparrow}{(\alpha+\bar{\alpha})}}x + \underset{\mathbb{R}.}{\underset{\uparrow}{\alpha\bar{\alpha}}}\right)\cdots$$

<u>Cor</u>: irreducible real poly are either linear or quadratic.

$\forall f \in \mathbb{R}[x]$

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)\cdot$$
$$(x^2+b_1x+c_1)(x^2+b_2x+c_2)\cdots(x^2+b_sx+c_s)$$

where $\alpha_i, b_j, c_j \in \mathbb{R}$.

<u>Rmk</u>: To classify irreducibles over $\mathbb{Z}_p$ is not so easy. In particular

$\forall p\, \forall n\ \exists$ irreducible poly over $\mathbb{Z}_p$ with degree n.

Ex) Factorize

$$f = x^4 + x^3 + x^2 + x + 1 \quad \text{over } \mathbb{Z}_2$$

First: check for roots.

$f(0) = 1 \qquad f(1) = 1$: no roots

No roots means no linear factors.
So if f has irreducible factors
they have to be quadratic. Say
Assume

$$f = (ax^2 + bx + c)(dx^2 + ex + f).$$

write the product

$$x^4 + x^3 + x^2 + x + 1 =$$
$$ad\,x^4 + (ae + bd)x^3 + (be + af + cd)x^2 + (ce + bf)x + cf.$$

x^4: $ad = 1 \implies a = d = 1$

1: $cf = 1 \implies c = f = 1$

$$\left.\begin{array}{ll} x^3: & e+b=1 \\ x^2: & be+1+1=1 \end{array}\right\} \Longrightarrow$$

$$\left.\begin{array}{l} e+b=1 \\ be=1 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} e+b=1 \\ e=b=1 \end{array}\right\} \lightning$$

So f can <u>not</u> be factorized in linear and quadratic factors:

f is irreducible.

Ex] Factorize

$f = x^4+1$ over $\mathbb{Z}_3$.

First check roots.

$f(0)=1 \quad f(1)=2 \quad f(2)=2$

So no linear factors.

Assume f can be factorizes with quadratics.

$x^4+1 = (ax^2+bx+c)(dx^2+ex+f)$

$$x^4+1 = adx^4 + (ae+bd)x^3 + (be+af+cd)x^2 + (ce+bf)x + cf.$$

x^4: $ad = 1 \implies a=d=1$ or $a=d=2$.
(observe 1, 2 are there own inverses).

you may assume $a=d=1$ (otherwise divide by 2)

1: $cf = 1 \implies c=f=1$ or $c=f=2$.
So $\boxed{c=f.}$

x^3: $0 = \cancel{\text{and}}\ e+b$ $\quad\boxed{e=-b}$

x^2: $0 = -b^2+f+c = -b^2+2c.$

$$\boxed{2c=b^2}$$

$a=1 \quad b=1 \quad c=2 \quad d=1 \quad e=-1=2 \quad f=2$
is a solution. So

$$x^4+1 = (x^2+x+2)(x^2+2x+2)$$

Ex] factorize
x^3+x+1 over $\mathbb{Z}_2$

roots? $f(0)=1$ $f(1)=1$

No roots
So no linear factors.
If f is reducible it has two
quad factors. but then the
degree $=4$ $\lightning$
So f is irreducible.