① 5/4/2020

F - a field

$f(x) \in F[x]$, $a \in F$

Division Alg.

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

$$\deg r(x) < \deg(x-a) = 1$$

$$\therefore \quad r(x) = r_a \in F$$

<u>Thm</u> For $f(x) \in F[x]$ and $a \in F$ one has $f(a)=0$ if and only if $(x-a)$ divides $f(x)$

<u>Thm</u> For $f(x) \in F[x]$ and $a \in F$ $f(a)$ is the remainder after div by $x-a$.

Thm. Let $f(x) \in F[x]$ be of degree n. It then has at most n zeros in F.

(2)

Proof: By induction on n.

If $n=0$, then $f(x) = a \neq 0$ is constant so it has no zeros.

Let $n>0$ and assume that a poly of deg. $n-1$ has at most $n-1$ zeros.

Let $a \in F$ be a zero for $f(x)$:

$$f(x) = g(x)(x-a)$$

$\deg g(x) = n-1$, so has at most $n-1$ zeros, so $f(x)$ has ~~degree~~ at most n zeros.

Ex In $\mathbb{Z}_6[x]$ the polynomial $f(x)=x^2-x = x(x-1)$ has 3 zeros

$$f(0) = 0$$
$$f(1) = 0$$
$$f(3) = 3(2) = 6 = 0$$

Def Let $f(x) \in F[x]$ and $f(a)=0$. The multiplicity of a is s if

$$(x-a)^s g(x) = f(x) \text{ and } g(a) \neq 0$$

③

Ex $f(x) = x^2 - 1$

In $\mathbb{Q}[x]$: $f(x) = (x-1)(x+1)$
$\therefore$ 1 is zero with mult. 1

In $\mathbb{Z}_2[x]$ $f(x) = (x-1)^2$
$\therefore$ 1 is zero will mult 2.

In $\mathbb{Q}[x]$ $f(x) = x^2+1$ has no zeros
$\mathbb{C}[x]$ $f(x) = (x-i)(x+i)$

Thm Let $f(x) \in \mathbb{R}[x]$. If $z = a+bi$ is a zero, then $\bar{z} = a - ib$ is a zero.

Pf: $f(z) = 0$
$f(\bar{z}) = \overline{f(z)} = \bar{0} = 0$

Recall: $U(5)$ is the group of units in $\mathbb{Z}_5$. $U(5) \cong \mathbb{Z}_4$

$U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

④

I.e. For prime p $\mathbb{Z}_5^* = \langle \mathbb{Z}_5 \setminus \{0\}, \cdot \rangle$ is isomorphic to $\mathbb{Z}_{p-1}$.

<u>Thm</u> Let F be a finite field and F^* the mult. group of non-zero elts. Every subgroup G of F^* is cyclic.

<u>Pf</u> By Fundamental thm for abelian groups

$$G \cong C_{d_1} \times \dots \times C_{d_n}$$

where $d_i = p_i^{\alpha_i}$

Note $|G| = d_1 \cdots d_n$

set $n = \mathrm{lcm}(d_1, \dots, d_n)$

For $x \in C_{d_i}$: $x^n = x^{d_i n_i} = (x^{d_i})^{n_i} = 1$

For $x \in G \leftrightarrow (x_1, \dots, x_n) \in C_{d_1} \times \dots \times C_{d_n}$

$$x^n = 1$$

$\therefore$ $x^n - 1 \in F[x]$ has $|G|$ zeros in F

$\therefore$ $n \geq |G| \geq n$

$\therefore$ $n = |G|$. $\therefore$ $\mathrm{lcm}(d_1, \dots, d_n) = d_1 \cdots d_n$

$\therefore$ p_i's distinct primes $G \cong \mathbb{Z}_{|G|}$ $\square$