Lecture 36: 11th Nov 2022

Note Title 11/11/2022

<u>Theorem 1</u>: Let G be a finite group. If for every divisor d of $|G|$, there is exactly one subgroup of order d, then G is cyclic.

<u>Proof</u>: Let $|G| = n$.

Let $d_1, d_2, \ldots, d_m$ be the divisors of n.

Let $d_1, d_2, \ldots, d_k$ $(k \leq m)$ be the divisors of n such that there exists an element x_i of order d_i $(1 \leq i \leq k)$.

Let l_i = number of elements in G of order d_i $(1 \leq i \leq k)$.

Then, we have $\sum_{i=1}^{k} l_i = |G| = n$.

Let x_i be an element of order d_i $(1 \leq i \leq k)$. Then, $|\langle x_i \rangle| = d_i$

Since G has exactly one subgroup of order d for each divisor d of n, so $\langle x_i \rangle$ is the only subgroup of order d_i

$\therefore \; l_i = \varphi(d_i) \quad \forall\, i = 1, 2, \dots, k$

$$\Rightarrow \sum_{i=1}^{k} \varphi(d_i) = n.$$

Again, we know that $\displaystyle\sum_{i=1}^{m} \varphi(d_i) = \sum_{d|n} \phi(d) = n.$

Hence, $k = m$.

$\Rightarrow$ For each divisor d of n, G has an element of order d.

$\Rightarrow$ G has an element of order n. $\Rightarrow$ G is cyclic.

This completes the proof. #

Let p be a prime. Let $q = p^k$, where $k \in \mathbb{N}$.

We denote by $\mathbb{F}_q$ the finite field with q elements.

<u>Theorem 2</u>: For every finite field $\mathbb{F}_q$ and every $n \in \mathbb{N}$, the product of all the monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$.

This is,
$$x^{q^n} - x = \prod_{d \mid n} f_d(x),$$
where $f_d(x)$ is the product of all the monic irreducible polynomials over $\mathbb{F}_q$ of degree d.

<u>Ex</u>: Let $q = p = 2$ and $n = 2$. Then,
$$x^{q^2} - x = x^4 - x = x(x+1)(x^2+x+1) \quad \text{over } \mathbb{F}_2$$

Here, x and $1+x$ are the (monic) irreducible polynomials over $\mathbb{F}_2$ of degree 1; and x^2+x+1 is the degree 2 irreducible polynomial over $\mathbb{F}_2$.

Ex: $q=2$, $n=3$.

$$x^{2^3}-x = x^8 - x = x(x+1)\underbrace{(x^3+x+1)(x^3+x^2+1)}_{\text{are the only irreducible polynomials of degree 3 over } \mathbb{F}_2}$$

Note that any non-constant polynomial over $\mathbb{F}_2$ is monic

Ex: $q=2$, $n=4$

$$x^{16}-x = x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1).$$

<u>Theorem 3</u>: The number of monic irreducible polynomials over a finite field $\mathbb{F}_q$ of degree n is equal to

$$\frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{n/d},$$ where μ is the Möbius function.

<u>Proof</u>. Let $N_{\mathbb{F}_q}(d)$ = number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d.

By Theorem 2, we have

$$q^n = \sum_{d \mid n} d \cdot N_{\mathbb{F}_q}(d). \longrightarrow (1)$$

Let $F, f : \mathbb{N} \longrightarrow \mathbb{C}$ be defined by

$$F(m) = q^m \quad \text{and} \quad f(m) = m \cdot N_{\mathbb{F}_q}(m), \qquad m \in \mathbb{N}.$$

Then (1) $\Rightarrow$

$$F(n) = \sum_{d|n} f(d).$$

By Möbius inversion formula, we have

$$f(n) = \sum_{d|n} \mu(d) \, F(n/d) \Rightarrow n \cdot N_{\mathbb{F}_q}(n) = \sum_{d|n} \mu(d) \, q^{n/d}$$

$$\Rightarrow N_{\mathbb{F}_q}(n) = \frac{1}{n} \sum_{d|n} \mu(d) \, q^{n/d}.$$

This is the required formula. #

Ex: Number of (monic) irreducible polynomials of degree 2 over $\mathbb{F}_2$

$$= \frac{1}{2} \sum_{d|2} \mu(d)\, 2^{2/d}$$

$$= \frac{1}{2} \left[\mu(1) \cdot 2^2 + \mu(2) \cdot 2^1 \right] = \frac{1}{2} [4 - 2] = 1.$$

$N_{\mathbb{F}_2}(4) = \#$ (monic) irreducible polynomials of degree 4 over $\mathbb{F}_2$

$$= \frac{1}{4} \sum_{d|4} \mu(d)\, 2^{4/d} = \frac{1}{4} \left[\mu(1) \cdot 2^4 + \mu(2) \cdot 2^2 + \mu(4) \cdot 2 \right]$$

$$= \frac{1}{4} [16 - 4 + 0] = \frac{1}{4} \times 12 = 3$$

#

Subfields of a finite field:

Let F be a finite field. Then, we know that $|F| = p^n$, where p is a prime and $n \in \mathbb{N}$.

Note that $p = \mathrm{char}(F)$ and $\dim F/\mathbb{F}_p = n$.

Let K be a subfield of F. Clearly, $|K| = p^k$ for some $k \in \mathbb{N}$.

We know that F is a vector space over K.

Let $m = \dim F/K$. Then, $|F| = |K|^m$

$\Rightarrow p^n = (p^k)^m = p^{km} \Rightarrow km = n \Rightarrow k \mid n.$

__Theorem 4:__ If a finite field of order p^n contains a subfield of order p^k, then $k \mid n$. Conversely, if $k \mid n$ then a finite field of order p^n contains a __unique__ subfield of order p^k.

Thus, a finite field of order p^n contains a subfield of order $p^k \Leftrightarrow k \mid n$. Also, the subfields are unique.

__Ex:__ $|\mathbb{F}_4| = 4 = 2^2$. Since 1 and 2 are the only divisors of 2, so there is no field lying between $\mathbb{F}_2$ and $\mathbb{F}_4$.

__Ex:__ $|\mathbb{F}_{16}| = 16 = 2^4$. In this case, we have a field K of order $2^2 = 4$ lying between $\mathbb{F}_2$ and $\mathbb{F}_{16}$.

#

We have $\mathbb{F}_{16} = \mathbb{F}_2[x] / \langle x^4+x+1 \rangle$.

$$= \{ a + bx + cx^2 + dx^3 + \langle x^4+x+1 \rangle \mid a,b,c,d \in \mathbb{F}_2 \}.$$

We have $\mathbb{F}_2 \subsetneq K \subsetneq \mathbb{F}_{16}$, where K is a field of order 4.

Determine K.

Clearly, $0, 1 \in K$. What are the other two elements of K?

—— x ——