Note Title 11/4/2022

Lecture 33, 34, and 35 — Oct 31, Nov 1 and Nov 4.

Theorem: Let F be a finite field. Then, $|F| = p^n$ for some prime p and $n \geq 1$.

Proof: Since F is a finite field, so $\text{char}(F)$ is prime, say, $\text{char}(F) = p$.

Then $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\} \subseteq F$ (or you can say that F contains a subfield isomorphic to $\mathbb{Z}_p$).

Now, we have two fields $\mathbb{Z}_p$ and F such that $\mathbb{Z}_p \subseteq F$. Hence, F is a vector space over $\mathbb{Z}_p$.
Since F is finite, so dimension of F over $\mathbb{Z}_p$ is finite, say, $\dim(F) = n$.

Let $\{v_1, v_2, \dots, v_n\}$ be a basis of F over $\mathbb{Z}_p$.

We know that every $v \in F$ can be written uniquely as

$$v = a_1 v_1 + \dots + a_n v_n, \quad a_i \in \mathbb{Z}_p.$$

$$\Rightarrow |F| = p^n.$$

This completes the proof.

—————x—————

- Let $f(x) \in R[x]$. Then, $f(x)$ determines a function $f : R \to R$, $a \mapsto f(a)$.

Two different polynomials may determine the same function.

For example, let $f(x) = 1 + x$, $g(x) = 1 + x^2 \in \mathbb{Z}_2[x]$.

As polynomials, clearly $f(x)$ and $g(x)$ are two different elements in $\mathbb{Z}_2[x]$.

But as functions $f: \mathbb{Z}_2 \to \mathbb{Z}_2$ & $g: \mathbb{Z}_2 \to \mathbb{Z}_2$ are the same. This is because,

$$f(0) = 1 = g(0)$$
$$f(1) = 1+1 = 0 = 1+1 = g(1).$$

$$\therefore\ f(a) = g(a) \quad \forall\, a \in \mathbb{Z}_2$$

$\Rightarrow$ f and g are the same functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$

Remark: This is not the case for polynomials over infinite fields. (See the next theorem).

<u>Theorem:</u> Let F be an <u>infinite</u> field. Let $f(x), g(x) \in F[x]$. Then, $f(x)$ and $g(x)$ are equal as polynomials

$\iff$ f and g are equal as functions from F to F.

<u>Proof:</u> If $f(x)$ and $g(x)$ are equal as polynomials, then they determine same function from F to F and this is obvious.

Conversely, suppose that $f(x), g(x) \in F[x]$ are such that $f, g : F \to F$ satisfy $f(a) = g(a)$ $\forall\, a \in F$.

We need to prove that $f(x)$ and $g(x)$ are equal as polynomials.

Let $\psi(x) = f(x) - g(x)$ and we have $\psi(x) \in F[x]$.

Now, since for every $a \in F$, $f(a) = g(a)$, so

$$\psi(a) = f(a) - g(a) = 0.$$

$\Rightarrow$ every element of F is a zero of the polynomial $\psi(x)$.

But F is an infinite field, so $\psi(x)$ must be the zero polynomial.

Hence, $f(x) = g(x)$ as polynomials in $F[x]$.

This completes the proof.

—x—

§ Field of fractions:

Let D be an integral domain.

Let: $R = D \times (D - \{0\}) = \{(a, b) \mid a, b \in D,\ b \neq 0\}$

We now define a relation $\sim$ in R:

$$(a, b) \sim (c, d) \text{ if } ad - bc = 0.$$

Easy to prove that this relation is an equivalence relation.

Let $\frac{a}{b} :=$ the equivalence class containing the element $(a, b) \in R$.

Let $F(D) =$ set of all the equivalence class of the above relation
$= \{\frac{a}{b} \mid a, b \in D,\ b \neq 0\}$.

We now define two binary operations in $F(D)$:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$

The sum of equivalence class containing (a,b) and the equivalence class containing (c,d) is the equivalence class containing $(ad+bc,\ bd)$.

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

The multiplicative identity is $\frac{1}{1} = \frac{a}{a}$, $a \neq 0$.

A nonzero element of $F(D)$ is $\frac{a}{b}$, where $a \neq 0$, $b \neq 0$.

Clearly, every nonzero element has inverse, namely, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

This proves that $F(D)$ is a field.

Theorem: $F(D)$ is the smallest field containing D.

Proof: • We have already seen that $F(D)$ is a field.

• The map $\psi: D \longrightarrow F(D)$, $a \longmapsto \frac{a}{1}$ is a ring homomorphism and ψ is injective.

$\therefore D \cong \psi(D) \subseteq F(D)$.

Hence, $F(D)$ contains D (or we can say that $F(D)$ contains a field isomorphic to D)

• To prove that $F(D)$ is the smallest field containing D, we let K be a field containing D.

Claim: K contains (an isomorphic copy) $F(D)$.

We have $D \subseteq K$. So, if $b \neq 0$ in D, then b^{-1} exists in K ($\because K$ is a field).

Define $\phi : F(D) \longrightarrow K$

$$\frac{a}{b} \longmapsto ab^{-1}.$$

Easy to prove that ϕ is a ring homomorphism and ϕ is injective. Hence, $F(D) \cong \phi(F(D)) \subseteq K$.

This completes the proof of the theorem.

<u>Definition</u>: $F(D)$ is called the field of fractions of the integral domain D.

<u>Ex:</u> consider $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p$ is an integral domain,
so $\mathbb{Z}_p[x]$ is also an integral domain.

The field of fraction of $\mathbb{Z}_p[x]$

$$= \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{Z}_p[x],\ g(x) \neq 0 \right\}.$$

This field is called the field of rational functions over $\mathbb{Z}_p$.

This is an infinite field whose characteristic is p (finite).

——— x ———

<u>Lecture 34</u>   <u>Nov 1, 2022</u>

§ <u>Arithmetical Functions:</u> Let $\mathbb{N}$ denote the set of positive integers.

An arithmetical function is a function $f : \mathbb{N} \longrightarrow \mathbb{C}$.

<u>Ex</u>: <u>Möbius function</u>: $\mu : \mathbb{N} \longrightarrow \mathbb{C}$ is defined by

$\mu(1) = 1$, and if $n > 1$, write $n = p_1^{a_1} \cdots p_k^{a_k}$ ($p_1, \dots, p_k$ are distinct primes)

Then, $$\mu(n) = \begin{cases} (-1)^k & \text{if } a_1 = a_2 = \cdots = a_k = 1 \\ 0 & \text{otherwise.} \end{cases}$$

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

<u>Theorem:</u> If $n \geq 1$, we have

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$$

<u>Proof.</u> The formula is true if $n=1$. Assume that $n>1$. Write $n = p_1^{a_1} \cdots p_k^{a_k}$. In the sum $\sum_{d|n} \mu(d)$, the only nonzero terms come from $d=1$ and from those divisors of n which are product of distinct primes.

Thus,

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1 p_2) + \cdots + \mu(p_{k-1} p_k) + \cdots + \mu(p_1 p_2 \cdots p_k).$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k$$

$$= (1-1)^k$$

$$= 0.$$

This completes the proof.

Ex: The Euler totient function $\varphi(n)$: $\varphi(n) = \#\{k \mid 1 \le k \le n, \underbrace{\gcd(k,n)}_{=1}\}$

We can also write

$$\varphi(n) = \sum_{k=1}^{n}{}' \, 1$$

where the $'$ indicates that the sum in extended over those k relatively prime to n.

<u>Theorem:</u> If $n \geq 1$, we have $\displaystyle\sum_{d \mid n} \varphi(d) = n$.

<u>Proof:</u> Let $S = \{1, 2, \ldots, n\}$. We distribute the integers of S into disjoint sets as follows: For each divisor d of n, let

$$A(d) = \{k \mid \gcd(k, n) = d, \ 1 \leq k \leq n\}.$$

Clearly, the sets $A(d)$, where d runs over all the divisors of n, form a disjoint collection whose union is S.

$$\therefore \sum_{d \mid n} \# A(d) = \# S = n.$$

<u>Claim:</u> $\# A(d) = \varphi(d)$.

We have $\gcd(k, n) = d \iff \gcd\left(\frac{k}{d}, \frac{n}{d}\right) = 1$,

and $1 \leq k \leq n$ if and only if $1 \leq \frac{k}{d} \leq \frac{n}{d}$.

Therefore, if we let $q = k/d$, there is a one-to-one correspondence between the elements in $A(d)$ and those integers q

satisfying $1 \leq q \leq \frac{n}{d}$ and $\gcd(q, \frac{n}{d}) = 1$

The number of such q is $\varphi(n/d)$.

$\therefore \ \# A(d) = \varphi(n/d)$.

This proves that $\displaystyle\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n.$

When d runs through all divisors of n, so does $\frac{n}{d}$.

$\therefore \displaystyle\sum_{d|n} \varphi(d) = n.$

This completes the proof.

#

§ A relation connecting φ and μ:

<u>Theorem:</u> If $n \geq 1$, then we have $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

<u>Proof:</u> We have $\varphi(n) = \sum_{k=1}^{n}{}' \, 1 = \sum_{k=1}^{n} \left[\frac{1}{\gcd(k,n)} \right]$

Since $\sum_{d|n} \mu(d) = \left[\frac{1}{n} \right]$, so

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d | \gcd(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

For a fixed divisor d of n, we must sum over all those k in the range $1 \leq k \leq n$ which are multiple of d. If we write $k = qd$, $1 \leq k \leq n$ if and only if $1 \leq q \leq \frac{n}{d}$.

$$\therefore \quad \varphi(n) = \sum_{d \mid n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d \mid n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d \mid n} \mu(d) \cdot \frac{n}{d}$$

Thus, $\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}$, and this completes the proof.

—— x ——

Let $\mathcal{A}$ = set of all the arithmetical functions
$= \{ f \mid f : \mathbb{N} \to \mathbb{C} \}$

We now define a binary operation $*$ in $\mathcal{A}$.

<u>Dirichlet product (Dirichlet convolution):</u>

For $f, g \in \mathcal{A}$, Dirichlet product $f * g : \mathbb{N} \to \mathbb{C}$ is defined by
$$(f*g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right).$$

<u>Properties:</u> (i) $f * g = g * f$ $\quad\forall f, g, h \in \mathcal{A}$.

(ii) $f * (g * h) = (f * g) * h$

Definition: Define $I : \mathbb{N} \to \mathbb{C}$ by

$$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

$$= \left[\frac{1}{n} \right]$$

Theorem: $f * I = f = I * f \quad \forall f \in \mathcal{A}$.

Proof: We have $(f * I)(n) = \sum_{d|n} f(d)\, I\left(\frac{n}{d}\right)$

$I\left(\frac{n}{d}\right) \neq 0$ only if $\frac{n}{d} = 1$, that is, if $n = d$.

$\therefore (f * I)(n) = f(n) \Rightarrow f * I = f$. #

Result: $\mathcal{A}$ is a monoid w.r.t. Dirichlet product.

Lecture 35

4th Nov, 2022.

Theorem: If $f \in \mathcal{A}$ with $f(1) \neq 0$, then there is a unique arithmetical function f^{-1}, called the Dirichlet inverse of f, such that

$$f * f^{-1} = f^{-1} * f = I.$$

Moreover, f^{-1} is given by the recursion formula:

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d \mid n \\ d < n}} f\left(\frac{n}{d}\right) f^{-1}(d) \text{ if } n > 1.$$

Proof: Given f, we shall show that the equation $(f * f^{-1})(n) = I(n)$ has a unique solution for the function values $f^{-1}(n)$.

For $n=1$, we solve $$(f * f^{-1})(1) = I(1)$$

$$\Rightarrow f(1)\, f^{-1}(1) = 1 \Rightarrow f^{-1}(1) = \frac{1}{f(1)}.$$

Assume now that the function values $f^{-1}(k)$ have been uniquely determined for all $k < n$. Then, we solve

$$(f * f^{-1})(n) = I(n) \quad \text{for } n > 1.$$

$$\Rightarrow \sum_{d \mid n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

$$\Rightarrow f(1)\, f^{-1}(n) + \sum_{\substack{d \mid n \\ d < n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0$$

If the values $f^{-1}(d)$ are known for all divisors $d < n$, there is a uniquely determined value for $f^{-1}(n)$, namely

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d \mid n \\ d < n}} f\left(\frac{n}{d}\right) f^{-1}(d).$$

This completes the proof. #

---x---

<u>Definition:</u> We define $u : \mathbb{N} \longrightarrow \mathbb{C}$ by

$$u(n) = 1 \quad \forall\, n \in \mathbb{N}.$$

We have, $\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = I(n)$.

$$\Rightarrow \sum_{d|n} \mu(d) \cdot u\left(\frac{n}{d}\right) = I(n) \Rightarrow \mu * u = I$$

$\therefore \mu^{-1} = u$ and $u^{-1} = \mu$ in $\mathcal{A}$.

<u>Theorem (Möbius inversion formula):</u> For $f, g \in \mathcal{A}$, the equation

$$f(n) = \sum_{d|n} g(d) \text{ implies } g(n) = \sum_{d|n} f(d)\,\mu\left(\frac{n}{d}\right).$$

Conversely, $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$ implies $f(n) = \sum_{d|n} g(d)$.

__Proof:__ $f(n) = \sum_{d|n} g(d) = \sum_{d|n} g(d)\, u\left(\frac{n}{d}\right)$

$\therefore f = \sum_{d|n} g(d) \Rightarrow f = g * u$

$\Rightarrow f * u^{-1} = g \Rightarrow f * \mu = g$

$\Rightarrow g(n) = (f * \mu)(n) = \sum_{d|n} f(d)\, \mu\left(\frac{n}{d}\right)$.

Conversely, if $g(n) = \sum_{d|n} f(d)\, \mu\left(\frac{n}{d}\right)$, then $g = f * \mu$

$\Rightarrow g * \mu^{-1} = f \Rightarrow f = g * u \Rightarrow f(n) = \sum_{d|n} g(d)$. #

§ Application of the identity $\sum_{d \mid n} \varphi(d) = n$:

<u>Theorem:</u> Let F be a field. If G is a finite subgroup of $F^* = F \setminus \{0\}$, then G is cyclic.

<u>Proof:</u> Let $|G| = n$. Then, $a^n = 1 \quad \forall\, a \in G$

Hence, the polynomial $x^n - 1 \in F[x]$ has n distinct zeros and the zeros are the elements of G.

Let $d_1, d_2, \ldots, d_k$ be the divisors of n such that G has an element of order d_i for each $i = 1, 2, \ldots, k$

Let $d_1, d_2, \ldots, d_k, d_{k+1}, \ldots, d_m$ be the all divisors of n.

Then, $\sum_{d|n} \varphi(d) = n$ is equivalent to $\sum_{i=1}^{m} \varphi(d_i) = n$. $\longrightarrow$ (1)

Now, let α_i be an element of G s.t. $o(\alpha_i) = d_i$, $1 \leq i \leq k$.

Consider the subgroup $\langle \alpha_i \rangle$ and since $o(\alpha_i) = d_i$ so $|\langle \alpha_i \rangle| = d_i$.

Now, the elements of $\langle \alpha_i \rangle$ satisfy $x^{d_i} - 1 = 0$.

But there are atmost d_i many zeros of $x^{d_i} - 1$.

That is, the zeros of $x^{d_i}-1$ are the elements of $\langle \alpha_i \rangle$.

Hence, there is exactly one subgroup of order d_i in G for each $i = 1, 2, \ldots, k$.

The number of elements of order d_i in G

$= $ the number of elements of order d_i in $\langle \alpha_i \rangle$

$= \phi(d_i)$

$$\therefore\ n = |G| = \sum_{i=1}^{k} \phi(d_i). \longrightarrow (2)$$

From (1) and (2), we must have $k = m$.

This proves that G has $\varphi(n)$ number of elements of order n ($\because d \mid n$, we take $d_m = d_k = n$).

This proves that G is cyclic.

#