Math 5402

4/20/20

Week 13

Finite fields continued... (13.5)

Theorem: $\mathbb{F}_{p^n}^{\times} = \mathbb{F}_{p^n} - \{0\}$ is a cyclic group under multiplication.

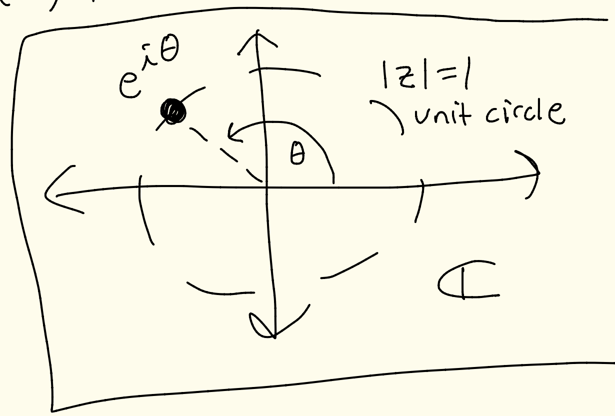
Theorem: For each divisor m of n, $\mathbb{F}_{p^n}$ has a unique subfield of size p^m. Moreover, these are the only subfields of $\mathbb{F}_{p^n}$.

Ex: Subfields of $\mathbb{F}_{5^3}$

$$\begin{array}{c} \mathbb{F}_{5^3} \\ | \\ \mathbb{F}_{5^2} \\ | \\ \mathbb{F}_5 = \mathbb{Z}_5 \end{array}$$

13.6 - Cyclotomic polynomials and Extensions

Recall if θ is a real number then $e^{i\theta} = \cos(\theta) + i\sin(\theta)$



Let $n \in \mathbb{Z}$, $n \geq 1$.

Let

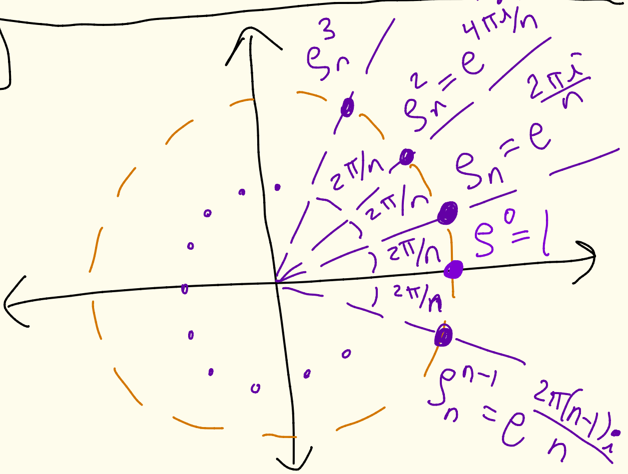
$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

Note that if $0 \leq a \leq n-1$, then

$$(\zeta_n^a)^n = \left(e^{\frac{2\pi i}{n}a}\right)^n = e^{2\pi i a} = \underbrace{\cos(2\pi a)}_{1} + i\underbrace{\sin(2\pi a)}_{0}$$

$$= 1$$

So, $1, \rho_n, \rho_n^2, \ldots, \rho_n^{n-1}$ are distinct and they each solve $x^n - 1 = 0$.



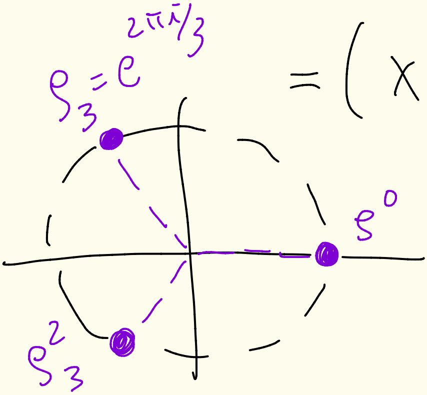
These elements subdivide the unit circle into n slices.

Therefore,

$$x^n - 1 = \prod_{a=0}^{n-1} (x - \rho_n^a).$$

Ex: $x^3 - 1 = (x - \rho_3^0)(x - \rho_3^1)(x - \rho_3^2)$

$$= (x-1)(x-\rho_3)(x-\rho_3^2)$$



The field $\mathbb{Q}(\zeta_n)$ is the splitting field for $x^n - 1$ over $\mathbb{Q}$, where $\zeta_n = e^{2\pi i/n}$.

The field $\mathbb{Q}(\zeta_n)$ is called the <u>cyclotomic field of n-th roots of unity</u>.

Let

$$\begin{aligned} \mu_n &= \{ z \in \mathbb{C} \mid z^n - 1 = 0 \} \\ &= \{ \zeta_n^a \mid 0 \leq a \leq n-1 \} \\ &= \{ 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1} \} \end{aligned}$$

μ_n is a cyclic group under multiplication. μ_n is called the <u>group of nth roots of unity over $\mathbb{Q}$</u>.

The generators of the cyclic group $\mathbb{Z}_n$ under addition are the elements $\bar{a} \in \mathbb{Z}_n$ where $\gcd(a,n) = 1$.

Since $\varphi : \mathbb{Z}_n \to \mu_n$ given by $\varphi(\bar{k}) = \rho_n^k$ is an isomorphism of groups (you can check this) we have that the generators of μ_n are the elements

$\rho_n^a = \varphi(\bar{a})$ where $1 \leq a \leq n-1$ and $\gcd(a,n) = 1$.

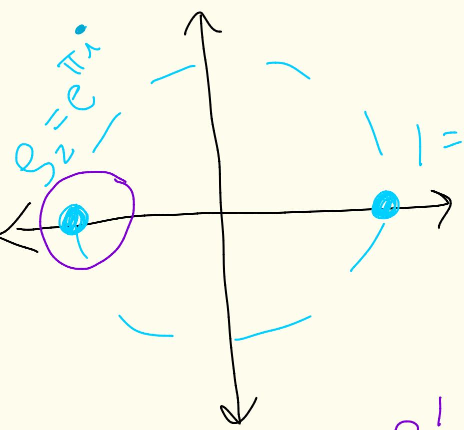
[An isomorphism of cyclic groups maps generators to generators.]

Def: If ζ generates μ_n as a group under multiplication, then ζ is called a primitive nth root of unity.

So, the primitive nth roots of unity are $\{\zeta_n^a \mid \gcd(a,n)=1,\ 1 \leq a \leq n-1\}$

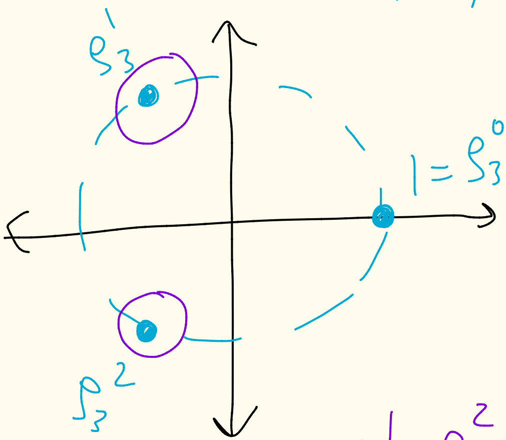
---

n = 2 $\mu_2 = \{1, \zeta_2\}$



primitive roots: ζ_2^1

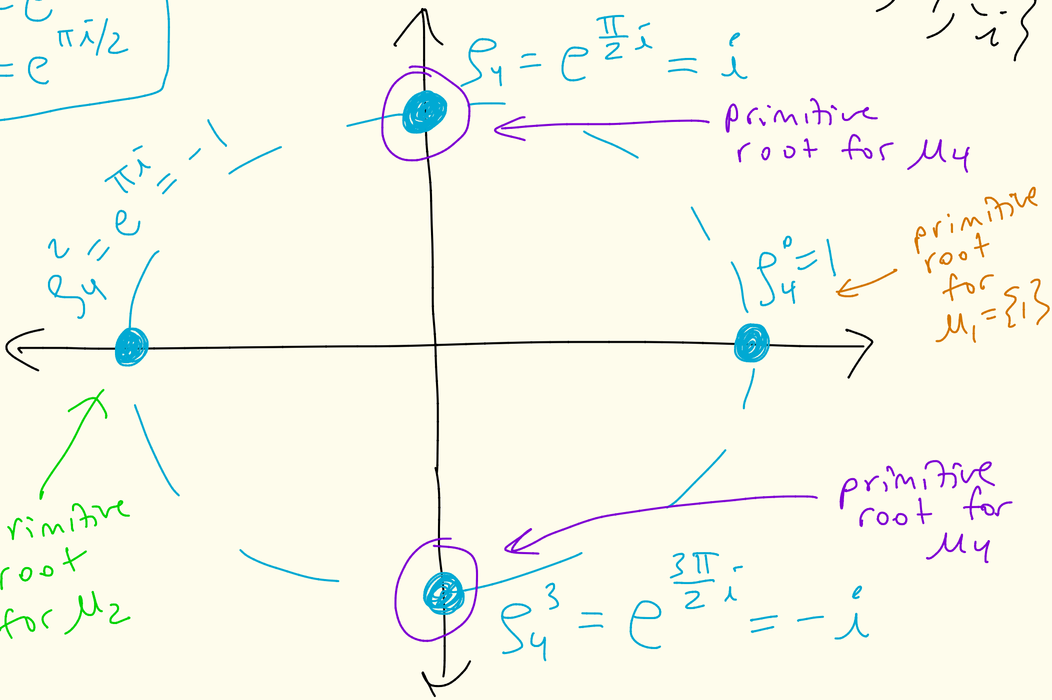
n = 3 $\mu_3 = \{1, \zeta_3, \zeta_3^2\}$



primitive roots: ζ_3^1, ζ_3^2

$\boxed{n=4}$: $\mu_4 = \{1, \rho_4, \rho_4^2, \rho_4^3\} = \{1, i, -1, -i\}$

$$\boxed{\rho_4 = e^{2\pi i/4} = e^{\pi i/2}}$$



primitive roots in μ_4:

$$\rho_4 = i, \quad \rho_4^3 = -i$$

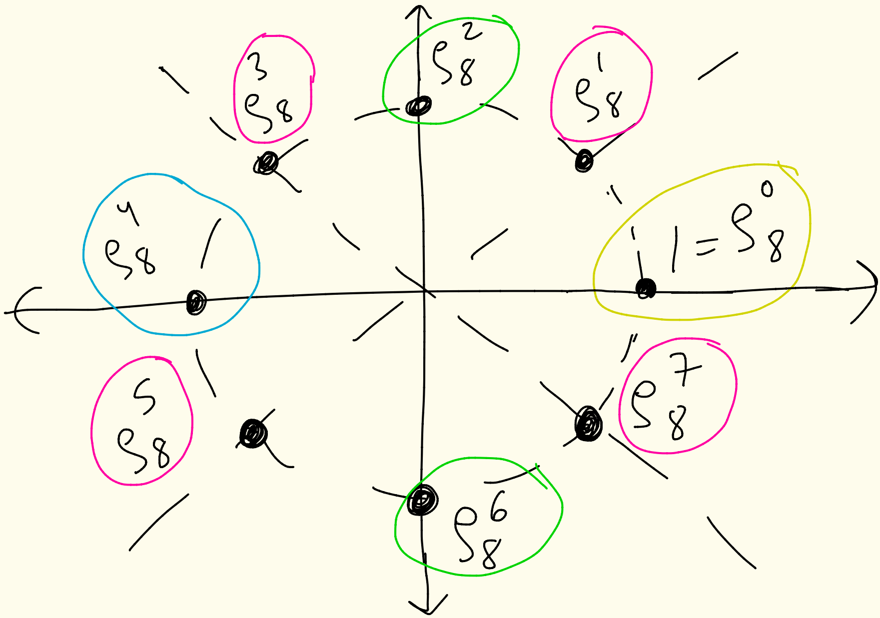
Note
$\mu_2 = \{1, -1\} \subseteq \mu_4$
-1 is a primitive root for μ_2

$$\rho_4 = e^{\pi/2\, i} = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right) = 0 + i \cdot 1 = i$$

And
$\mu_1 = \{1\} \subseteq \mu_4$

$\underline{n=8}$

$$\mu_8 = \{1, \zeta_8, \zeta_8^2, \zeta_8^3, \zeta_8^4, \zeta_8^5, \zeta_8^6, \zeta_8^7\}$$



$\mu_1 = \{1\} \subseteq \mu_8$

$\mu_2 = \{1, -1\} \subseteq \mu_8$

$\mu_4 = \{1, i, -1, -i\}$

$\subseteq \mu_8$

primitive roots of μ_8 are $\zeta_8^1, \zeta_8^3, \zeta_8^5, \zeta_8^7$

primitive roots of μ_4 are $\zeta_8^2 = i, \zeta_8^6 = -i$

primitive root of μ_2 is $\zeta_8^4 = -1$

primitive root of μ_1 is $\zeta_8^0 = 1$.

Proposition: $\mu_d \subseteq \mu_n$ iff $d \mid n$.

proof:

($\Rightarrow$) Suppose $\mu_d \subseteq \mu_n$.

Note that $|\mu_d| = d$ and $|\mu_n| = n$.

So, by Lagrange's thm, $d \mid n$.

($\Leftarrow$) Suppose $d \mid n$. So, $n = dk$, where $k \in \mathbb{Z}$.

Let $\rho \in \mu_d$. So, $\rho^d = 1$.

Then,

$$\rho^n = \rho^{dk} = (\rho^d)^k = 1^k = 1,$$

So, $\rho \in \mu_n$. $\blacksquare$

Def: Define the nth cyclotomic polynomial $\Phi_n(x)$ to be

pg 10

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ is primitive}}} (x - \zeta) = \prod_{\substack{1 \le a \le n \\ \gcd(a,n)=1}} (x - \zeta_n^a)$$

Note that $\text{degree}(\Phi_n) = \underbrace{\varphi(n)}_{\text{Euler phi function}} = \#\text{ generators of } \mu_n$

$= |\mathbb{Z}_n^\times|$

Thm: $$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

proof: We have that $x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta)$

If we group the elements together based on their orders in the group we get

$$x^n - 1 = \prod_{d \mid n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ is primitive} \\ \text{in } \mu_d}} (x - \zeta) = \prod_{d \mid n} \Phi_d(x)$$

$\blacksquare$