Some slides for 20th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

30-11-2010

$\xi \in \mathbb{C}$ is called an *n*th root of unity for a positive integer n if $\xi^n = 1$.

Remember polar coordinates: $\xi = re^{i\theta} = r(\cos(\theta) + i\sin(\theta))$

$\xi \in \mathbb{C}$ is called a primitive *n*th root of unity for a positive integer n if $\xi^n = 1$ and $\xi, \xi^2, \ldots, \xi^{n-1} \neq 1$.

Lemma 4.4.1

$\xi \in \mathbb{C}$ is a primitive *n*th root of unity if and only if

$$\xi = e^{(k2\pi i)/n}$$

where $1 \leq k \leq n$ and $\gcd(k, n) = 1$. If ξ is a primitive *n*th root of unity and $\xi^m = 1$ then $n|m$.

Let $n \in \mathbb{N}$ with $n \geq 1$. The *nth cyclotomic polynomial* is

$$\Phi_n(X) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} (X - e^{2\pi i k/n}) \in \mathbb{C}[X]$$

Degree of $\Phi_n(X)$?

Proposition 4.4.3

Let $n \geq 1$. Then

- $X^n - 1 = \prod_{d|n} \Phi_d(X)$
- $\Phi_n(X) \in \mathbb{Z}[X]$

We may consider the unique ring homomorphism $\kappa : \mathbb{Z} \to R$, for a ring R. And therefore

$$\kappa' : \mathbb{Z}[X] \to R$$

Hence, we can see $X^n - 1 = \prod_{d|n} \Phi_d(X)$ in $R[X]$

Let R be a ring and n a positive natural number. An element $\alpha \in R$ is called a primitive nth root of unity in R if $\alpha^n = 1$ and $\alpha, \alpha^2, \ldots, \alpha^{n-1} \neq 1$.

Lemma 4.5.2

Let α be an element in a domain R. If $\Phi_n(\alpha) = 0$ and α is not a multiple root of $X^n - 1 \in R[X]$ then α is a primitive nth root of unity in R

Theorem 4.5.3 (Gauss)

Let F be a field and $G \subset F^*$ a finite subgroup of the group of units in F. Then G is cyclic.

In particular, $\mathbb{F}_p^*$ is a cyclic group, for p prime. How to find a primitive root?
Probability of choosing (randomly) a primitive root in $\mathbb{F}_p^*$

$$\frac{\varphi(\varphi(p))}{\varphi(p)} = \frac{\varphi(p-1)}{p-1}$$

Theorem (Gauss)

Cyclotomic polynomials are irreducible as polynomials in $\mathbb{Q}[X]$.

$\Phi_8 = X^4 + 1$ is reducible in $\mathbb{F}_p[X]$ for any prime p.

Φ_n is irreducible in $\mathbb{F}_p[X]$ if and only if $[p]$ generates the group $(\mathbb{Z}/n\mathbb{Z})^*$.