Some slides for 13th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

28-03-2014

$\xi \in \mathbb{C}$ is called an nth root of unity (enhedsrod) 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 nth root of unity (primitiv n'te enhedsrod) 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 nth 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 nth root of unity and $\xi^m = 1$ then $n|m$.

Let $n \in \mathbb{N}$ with $n \geq 1$. The *n*th cyclotomic polynomial (cyklotomiske polynomium) 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 4.5.4

There are infinitely many prime numbers $\equiv 1 \pmod{n}$ for a natural number $n \geq 2$.

Gauss:

If R is a unique factorization domain then $R[X]$ is a unique factorization domain.

But we prove:

Proposition 4.6.1

The polynomial ring $F[X]$ is a Euclidean domain (and therefore a principal ideal domain and a unique factorization domain).

Proof:

- $\deg : F[X] \setminus \{0\} \to \mathbb{N}$ is a Euclidean function on $F[X]$
- For $f \in F[X]$ and $d \in F[X] \setminus \{0\}$ then there exists $q, r \in F[X]$ s.t.
$$f = qd + r$$
where $r = 0$ or $\deg(r) < \deg(d)$.

Hence, we can use the Euclidean algorithm to compute the GCD of two polynomials.

If $f \in F[X]$ is not an irreducible polynomial there is a factorization $f = f_1 f_2$ s.t.

$$0 < \deg(f_1), \deg(f_2) < \deg(f)$$

Proposition 4.6.3

Let $f \in F[X]$

1. $\langle f \rangle$ is a maximal ideal if and only if f is irreducible. In this case the quotient ring $F[X]/\langle f \rangle$ is a field
2. If $f \neq 0$ then f is a unit if and only if $\deg(f) = 0$
3. If $\deg(f) = 1$ then f is irreducible.
4. If f is irreducible and $\deg(f) > 1$ then f does not have any roots.
5. If $\deg(f)$ is 2 or 3 then f is irreducible if and only if f has no roots.

$X^4 + X^2 + 1 \in \mathbb{F}_2$ does not have any roots but it is not irreducible.