Lecture 18:

Last time:

Thm: Any non-const $p(z) \in \mathbb{C}[z]$ has a root.

Follows from 

Lemma: Suppose $p(z) = z + b_2 z^2 + b_3 z^3 + \cdots + b_n z^n$ with $|b_n| < \frac{1}{n^2 (n!) 10^{10}}$. Then $p(\mathbb{C}) \supseteq B_{1/2}(0)$

Proof: Will use Newton's Method. Fix $w_0 \in B_{1/2}(0)$.

Claim: Suppose $z \in B_1(0)$ with $|p(z) - w_0| < \varepsilon < 1/10$.
Then $\exists z'$ with $|p(z') - w_0| < \varepsilon^2$ and

$$|z' - z| < 10\varepsilon$$

Assuming this, take $z_0 = w_0$. Then $|p(z_0) - w_0| < 10^{-10}$

So $\exists z_1$ within 10^{-9} of z_0 with $|p(z_1) - w_0| < 10^{-20}$

Repeating, get z_n with $|p(z_n) - w_0| < 10^{-2^n \cdot 10}$

and $|z_n| \leq |z_0| + (10^{-9} + 10^{-19} + 10^{-39} + \cdots) < \frac{1}{2} + 10^{-8} < 1$.

Let $z = \lim_{n \to \infty} z_n$. Then by cont, $p(z) = w_0$

Proof of Claim: Take $z' = z - \frac{p(z)-w_0}{p'(z)}$. First observe

$$|p'(z)| = |1 + 2b_2 z + 3b_3 z^2 + \cdots + n b_n z^{n-1}|$$

↑ at most 1

$$> |-\frac{1}{n! 10^{10}}| > 1/10$$

So $$|z - z'| = \frac{|p(z)-w_0|}{|p'(z)|} < 10\varepsilon.$$

Second, $a = -\frac{p(z)-w_0}{p'(z)}$

$$p(z') = p(z+a)$$

If you want, this is just a comb. statement about polys

$$= p(z) + p'(z)a + \underbrace{\frac{p''(z)}{2}}_{\frac{1}{n^2 10^{10}} < 100\varepsilon^2} a^2 + \cdots + \underbrace{\frac{p^{(n)}(z)}{n!}}_{< \frac{1}{n^2 10^{10}}} \underbrace{a^n}_{< 100\varepsilon^2}$$

$$= p(z) + p'(z)a + E$$

where $|E| < \varepsilon^2$

So

$$p(z') = p(z) + p'(z)a + E = w_0 + E. \quad \blacksquare$$

This completes the proof of the Fund. Thm of Algebra.

Change of perspective is a very powerful tool...

Cyclotomic Fields: [Key example.]

$$\mathbb{Q}(\zeta_n) \text{ for } \zeta_n = e^{2\pi i/n}$$

When n is prime, $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$. What is $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$?

$$\mu_n = \left\{ \begin{matrix} \text{all roots of} \\ x^n - 1 \text{ in } \mathbb{C} \end{matrix} \right\} = \begin{matrix} \text{group of} \\ n\text{th roots of one, under mult.} \end{matrix}$$

Note: $|\mu_n| = n$ and is cyclic, generated by ζ_n.

Primitive n^{th} root: generator of μ_n, i.e. $\zeta^k \neq 1$ for $k < n$.

Which ζ_n^k are primitive? Those with $\gcd(k,n) = 1$

since

$$\mu_n \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z}. \quad \text{Thus there are}$$

$$\zeta_n^k \longrightarrow k \qquad \varphi(n) = \#\, 1 \le k < n \text{ with } \gcd(k,n) = 1$$

[Query: familiar with $\varphi(n)$? What is

$\varphi(p_1^{k_1} \cdots p_m^{k_m})$? A. $p_1^{k_1-1}(p_1-1) \cdots p_m^{k_m}(p_m-1)$]

Cyclotomic poly:

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

Now any $\zeta \in \mu_n$ is a primitive d^{th} root in μ_d for some $d \mid n$. Hence

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

$$= \prod_{d \mid n} \Phi_n(x)$$

Ex: $\Phi_1 = x - 1$

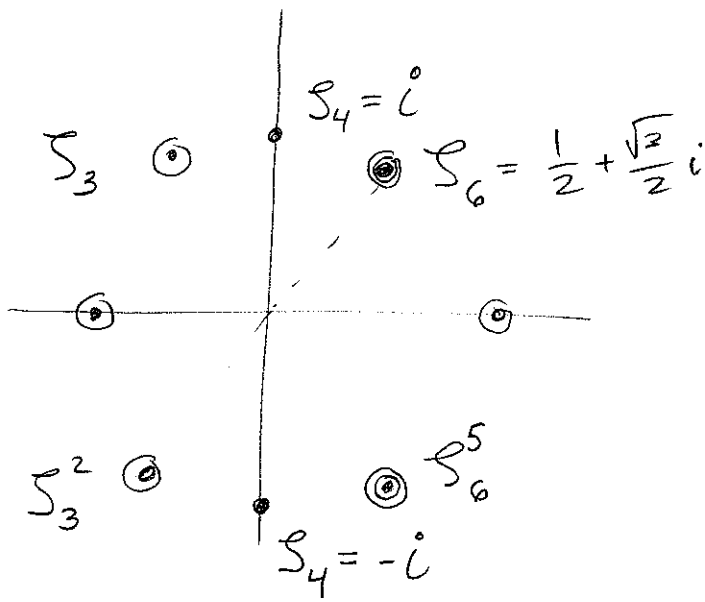
$\Phi_2 = x + 1$

$\Phi_3 = x^2 + x + 1$

$\Phi_4 = x^2 - 1$

$\Phi_5 = x^4 + x^3 + x^2 + 1$

$\Phi_6 = (x - \zeta_6)(x - \bar{\zeta}_6) = x^2 - x + 1$



Ex: $X^6 - 1 = (X^2 - X + 1)(X^2 + X + 1)(X + 1)(X - 1)$

Note: $\mathbb{Q}(S_6) = \mathbb{Q}(S_3)$.

Thm: $\Phi_n \in \mathbb{Z}[X]$ and is irreducible.
Hence $[\mathbb{Q}(S_n) : \mathbb{Q}] = \varphi(n)$.

Pf: To show $\Phi_n \in \mathbb{Z}[X]$, induct on n.
Let $f(X) = \prod_{\substack{d \mid n \\ d < n}} \Phi_d(X)$. Then $X^n - 1 = f(X)\Phi_n(X)$

Now since $X^n - 1$ and $f(X) \in \mathbb{Q}[X]$ it follows that so is $\Phi_n(X)$. (Have $X^n - 1 = q(X)f(X) + r(X)$ with $\deg r(X) < \deg f(X)$. Then in $\mathbb{Q}(S_n)[X]$ we have

$$f(X)\Phi_n(X) = q(X)f(X) + r(X) \Rightarrow (\Phi_n(X) - q(X))f(X) = r(X)$$

$$\Rightarrow q(X) = \Phi_n(X).$$

Cont: Next time.