MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 21

Let us prove the $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. We will assume without proof the *Gauss Lemma*, which tells that irreducibility of polynomials over $\mathbb{Z}$ is the same as over $\mathbb{Q}$. Suppose that ζ is a primitive root of $x^n - 1$. Then ζ^k is a root of $x^n - 1$, and if k and n are coprime, then ζ^k is a primitive root. Let $f(x)$ be the irreducible monic polynomial of ζ over $\mathbb{Q}$. It has integer coefficients by Gauss Lemma. Then $f(x)g(x) = \Phi_n(x)$, where g and f are coprime. Let p be a prime not dividing n. Then $x - \zeta^p$ also divides $\Phi_n(z)$. We want to prove that $x - \zeta^p$ divides $f(x)$. Suppose that it is not true. Then $x - \zeta^p$ divides $g(x)$, i.e., ζ^p is a root of $g(x)$. It follows that ζ is a root of $g(x^p)$. But $f(x)$ is the minimal polynomial of ζ, so $f(x)|g(x^p)$.Let us reduce everything modulo p, i.e., look at the coefficients of the polynomials as at elements of the field $\mathbb{Z}_p$. Then we still have that $f(x)|g(x^p)$ in $\mathbb{Z}_p[x]$. But we have $g(x^p) = (g(x))^p$ over $\mathbb{Z}_p$, so $f(x)|(g(x))^p$. Hence $f(x)$ and $g(x)$ have a common divisor. This implies that $x^n - 1$ has a multiple root in the algebraic extension of $\mathbb{Z}_p$. But we have shown before that $x^n - 1$ is separable over $\mathbb{Z}_p$ if p does not divide n.

We proved that if a prime p does not divide n, and ζ is a primitive root of $x^n - 1$, then ζ and ζ^p belong to the same irreducible factor of $\Phi_n(x)$. But every root of $\Phi_n(x)$ is of the form ζ^m for some m coprime with n. We can write then $m = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$, where p_i are primes. Since m and n are coprime, the primes p_i do not divide n, and step by step we prove that ζ^m divides the same irreducible factor of $\Phi_n(x)$. This shows that $\Phi_n(x)$ has only one irreducible factor.

We have shown that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. Fix a primitive root ζ. Recall that the nth cyclotomic extension is equal to the splitting field of $x^n - 1$ and is equal to $\mathbb{Q}(\zeta)$, since every root of $x^n - 1$ is of the form ζ^m. Every element σ of $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ is uniquely determined by its value $\sigma(\zeta)$. We know that $\sigma(\zeta)$ must generate the multiplicative group of roots of $x^n - 1$, i.e., that $\sigma(\zeta)$ is a root of $\Phi_n(x)$ and we have $\sigma(\zeta) = \zeta^m$ for some m coprime with n. Then for every root ζ^k we have $\sigma(\zeta^k) = \sigma(\zeta)^k = \zeta^{mk}$. If $\sigma(\zeta^k) = \zeta^{m_1 k}$ and $\tau(\zeta^k) = \zeta^{m_2 k}$, then $\sigma\tau(\zeta^k) = \zeta^{m_1 m_2 k}$. Conversely, for every primitive root ζ^m (where m and n are coprime) there exists an element of the Galois group such that $\zeta \mapsto \zeta^m$, since $\Phi_n(x)$ is irreducible.

It follows that the Galois group of the cyclotomic extension is isomorphic to the multiplicative group of the ring $\mathbb{Z}_n$. In particular, it is an abelian group of order $\phi(n)$. For example, if $n = p$ is prime, then it is isomorphic to the multiplicative group of the field $\mathbb{Z}_p$, hence cyclic of order $p - 1$. For some non-prime values of n it is not cyclic.

Constructing a regular n-gon by compass and a straightedge is equivalent to constructing a tower of quadratic extensions $\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_m$ such that F_m contains all complex roots of $x^n - 1$. If such an extension exists, then $[F_m : \mathbb{Q}] = 2^k$, and if K is the nth cyclotomic field, then $\mathbb{Q} \subseteq K \subseteq F_m$, so $[K : \mathbb{Q}]$ divides 2^k, hence $[K : \mathbb{Q}]$ is a power of two. But the degree of the cyclotomic extension is equal to $\phi(n) = \deg \Phi_n(x)$. The formula for $\phi(n)$ is

$$\phi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1).$$

We see that it is a power of 2 if and only if all odd primes p_i are raised to power $a_i = 1$ and are of the form $2^m + 1$. For any such a prime m must have no odd divisor, i.e., be a power of two. Hence all odd prime divisors of n must be *Fermat primes*: primes of the form $2^{2^k} + 1$. For example, such are $2 + 1, 4 + 1, 16 + 1, \ldots$. Fermat conjectured that all numbers $2^{2^k} + 1$ are primes. In fact, the only known Fermat primes are $2 + 1, 2^2 + 1, 2^{2^2} + 1, 2^{2^3} + 1, 2^{2^4} + 1$. For example, $2^{2^5} + 1 = 641 \times 6700417$.

Conversely, suppose that $\phi(n)$ is a power of 2. Then the Galois group $G(K/\mathbb{Q})$ of the nth cyclotomic extension over $\mathbb{Q}$ is of order $\phi(n)$, hence a power of two. Every group of order 2^m has a subgroup of index 2 (one of Sylow's theorems). The corresponding intermediate field E will satisfy $[E : \mathbb{Q}] = 2$, the extension $[K : E]$ is normal with the Galois group of order 2^{m-1}. Continuing like this we will get a sequence of degree two extension all the way from $\mathbb{Q}$ to the cyclotomic field. This will show that the regular n-gon is constructible.

Fundamental Theorem of Algebra

Theorem 1

$\mathbb{C}$ *is algebraically closed.*

We want to prove that every polynomial in $\mathbb{C}[x]$ has a root. It is equivalent to proving that $\mathbb{C}$ has no non-trivial finite extensions. Suppose that, on the contrary, $\mathbb{C} \subset K$ is a finite extension. Then $\mathbb{R} \subset K$ is also a finite extension. We can find a finite normal extension $\mathbb{R} \subset E$ such that $K \subset E$. (Take the irreducible polynomials of the generators of K over $\mathbb{R}$, and then adjoin all their roots.) Consider the Galois group $G = G(E/\mathbb{R})$.

Proof of the Fundamental Theorem of Algebra

Consider the Sylow 2-subgroup $H_1 \leq G$. Then $[G : H_1]$ is odd. Let $\mathbb{R} \subset F_1 \subset E$ be the corresponding field. We have then $[F_1 : \mathbb{R}] = [G : H_1]$. Hence for any $\alpha \in F_1$ the degree of the irreducible polynomial $f(x) \in \mathbb{R}[x]$ of α is odd. But every polynomial over $\mathbb{R}$ of odd degree has a root (since its signs at ∞ and $-\infty$ are opposite). Therefore, $F_1 = \mathbb{R}$, i.e., $H_1 = \{1\}$ and the Galois group G has order 2^n for some n. Consequently, the subgroup $G(E/\mathbb{C})$ of $G(E/\mathbb{R})$ is of order 2^{n-1}. By one of the Sylow Theorems, $G(E/\mathbb{C})$ has a subgroup H_2 of order 2^{n-2}. The corresponding field $\mathbb{C} \subset F_2 \subset E$ will have $[F_2 : \mathbb{C}] = [G : H_2] = 2$. but every *quadratic polynomial* in $\mathbb{C}[x]$ has a root in $\mathbb{C}$. Contradiction.