Kummer and Kronecker: two results in algebraic number theory

Hugo Trebše (hugo.trebse@gmail.com)

5. avgust 2024

Theorem 0.1

Let $\alpha \in \mathbb{A}$ and $|\alpha| = 1$. If all Galois conjugates of α have absolute value 1, then α is a root of unity.

Proof. Set $\alpha = \alpha_1$ and denote the algebraic conjugates of α as $\alpha_2, \ldots, \alpha_n$.

Observe the polynomial

$$p_k(X) = \prod_{i=1}^{n}(X - \alpha_i^k).$$

The coefficients of p_k are symmetric polynomials over $\mathbb{Z}$ in $\alpha_1^k, \alpha_2^k, \ldots, \alpha_n^k$ and hence symmetric polynomials in $\alpha_1, \alpha_2, \ldots, \alpha_n$. By the fundamental theorem of symmetric polynomials, the coefficients of p_k can be expressed as a polynomial over $\mathbb{Z}$ in the elementary symmetric polynomials of variables $\alpha_1, \alpha_2, \ldots, \alpha_n$. However, by the Vieta formulas on the minimal polynomial of α, we may conclude that the elementary symmetric polynomials in variables $\alpha_1, \alpha_2, \ldots, \alpha_n$ evaluate to rationals. It hence follows that the coefficients of p_k must be rational. But since the coefficients of p_k are also algebraic integers it follows that $p_k \in \mathbb{Z}[X]$

The m-th coefficient of p_k is, however, bounded from above by $\binom{n}{m}$ by the triangle inequality and the assumption that the α_i have absolute value at most 1. It hence follows that there are only finitely many distinct polynomials in the sequence $\{p_i\}_{i \in \mathbb{N}}$. It follows that there exists an infinite set of positive integers S, such that for all $a, b \in S$: $p_a = p_b$

By the definition of p_j it follows that $\{\alpha_1^a, \alpha_2^a, \ldots, \alpha_n^a\}$ is a permutation of $\{\alpha_1^b, \alpha_2^b, \ldots, \alpha_n^b\}$. Since S is infinite, it must be that for some distinct $c, d \in S$:

$$(\alpha_1^c, \alpha_2^c, \ldots, \alpha_n^c) = (\alpha_1^d, \alpha_2^d, \ldots, \alpha_n^d)$$

which proves that all α_i are roots of unity. □

Theorem 0.2

Let $p \in \mathbb{P}$ and $\zeta_p = e^{\frac{2\pi i}{p}}$. If $u \in \mathbb{Q}(\zeta)^\times$, then for some integer r

$$\frac{u}{\overline{u}} = \zeta_p^r.$$

Proof. If $u \in \mathbb{Q}(\zeta)$ is a unit, then $\overline{u}$ must be a unit. Indeed, there exists $u' \in \mathbb{Q}(\zeta)$, such that $u \cdot u' = 1$, from which it follows that $\overline{u} \cdot \overline{u'} = \overline{1} = 1$. Such a manipulation is indeed legal as u must be a $\mathbb{Q}$-linear combination of $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$, hence $\overline{u}$ is a $\mathbb{Q}$-linear combination of $1, \overline{\zeta_p}, \overline{\zeta_p^2}, \ldots, \overline{\zeta_p^{p-1}}$, which means $\overline{u} \in \mathbb{Q}(\zeta_p)$ since $\overline{\zeta_p} \in \mathbb{Q}(\zeta)$.

It follows that $\frac{u}{\overline{u}} \in \mathbb{Q}(\zeta_p)^\times$ and $\left|\frac{u}{\overline{u}}\right| = 1$. We would now like to apply the result proven above, which requires that all Galois conjugates of $\frac{u}{\overline{u}}$ to have absolute value 1.

Since $\mathbb{Q}$ is a field of characterstic zero, we know that $\mathbb{Q}(\zeta_p)$ is a Galois extension and since $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is an extension of degree $p-1$, a well-known result implies

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}_{p-1}.$$

We know from Galois theory that for any Galois conjugate v of $\frac{u}{\overline{u}}$, there must exist a $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, such that

$$\sigma(v) = \frac{u}{\overline{u}}.$$

Since any automorphism in $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is uniquely determined by the image of ζ_p and since $\overline{\zeta_p} \in \mathbb{Q}(\zeta_p)$, it is clear that complex conjugation $\overline{\cdot}$ is a field automorphism of $\mathbb{Q}(\zeta_p)$.

As $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$ is an Abelian group, all automorphisms of $\mathbb{Q}(\zeta_p)$ commute. It follows that:

$$|v|^2 = v \cdot \overline{v} = \sigma(\frac{u}{\overline{u}}) \cdot \overline{\sigma(\frac{u}{\overline{u}})} = \sigma(\frac{u}{\overline{u}}) \cdot \sigma(\frac{\overline{u}}{u}) = \sigma(\frac{u}{\overline{u}} \cdot \frac{\overline{u}}{u}) = \sigma(1) = 1$$

This demonstrates that all Galois conjugates of $\frac{u}{\overline{u}}$ have absolute value 1, hence $\frac{u}{\overline{u}} = \zeta_p^r$ $\square$