NAP 2019, MODULE II, CLASS #6, MAY 30, 2019

Michel Waldschmidt

- Answer to questions:
  Cayley – Hamilton Theorem.
  α transcendental over K, $f \in K[x]$ not constant, then $K(\alpha)$ is a finite extension of $K(f(\alpha))$.

- Reduction modulo p of a polynomial of $\mathbb{Z}[x]$. If the polynomial is reducible, its reduction (modulo a prime p which does not divide the leading term) is reducible. Hence if one of the reductions is irreducible, the polynomial is irreducible.

- The converse is not true. The polynomial $x^4 + 1$ is reducible modulo p for all p but irreducible over $\mathbb{Z}$ (no proof).

- Eisenstein criterion. Proof for $\mathbb{Z}[x]$ using reduction modulo p.

- For any $n \geq 1$, there exists an irreducible polynomial over $\mathbb{Z}$ of degree n (for instance $x^n - 2$), hence there exists a finite extension of $\mathbb{Q}$ of degree n.

- $x^n + px + p^2$ is irreducible over $\mathbb{Z}$. Same proof as for Eisenstein criterion.

- Last chapter: **construction with ruler and compass.**

- Definition: constructible point in $\mathbb{R}^2$, constructible number in $\mathbb{R}$.

- Theorems:
  The set of constructible numbers is a subfield of $\mathbb{R}$.
  A number α is constructible if and only if there exists a set $\{\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n\}$ of real numbers with $\alpha_0 = 1$ and $\alpha_n = \alpha$ such that
  $$\alpha_j^2 \in \mathbb{Q}(\alpha_0, \alpha_1, \dots, \alpha_{j-1}) \quad (1 \leq j \leq n).$$
  Consequence: a constructible number is algebraic over $\mathbb{Q}$ of degree a power of 2.
  Squaring the circle, doubling the cube cannot be done with ruler and compass.