NAP 2018 Module III Lecture 8 Thursday, June 14, 2018, 18:00 – 19:30.

- Fermat numbers. Mersenne primes.

- Constructions with straight edge and compass revisited (Milne p. 43–44)

Theorem 3.23. If a positive real number is contained in a subfield of $\mathbb{R}$ which is a *Galois* extension of $\mathbb{Q}$ of degree a power of 2, then it is constructible.

Uses the fact that a group of order a power of 2 is solvable.

Corollary: for p a Fermat prime $p = F_n = 2^{2^n} + 1$, a regular polygon with p sides can be constructed with ruler and compass.

The Galois group of $\mathbb{Q}(e^{2i\pi/p}$ over $\mathbb{Q}$. The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Example: $p = 7$.

- Example of a constructible number: $\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}$ (Milne exercise 3.4 p. 46 and solution p.129).

In the solution, Milne implicitly defines $\alpha = \sqrt{(\sqrt{2}+2)\sqrt{3}+3)}$. When he considers $\sigma(\alpha^2)$ in the solution of (b), he uses the fact that $\alpha^2 \in M$. Next he writes: *Extend σ to an automorphism of E.* The following result should be added after Theorem 3.16.

> *Under the hypotheses of Theorem 3.16 (d), when H is a normal subgroup of G and $M = E^H$, the map $G = \mathrm{Gal}(E/F) \to G/H = \mathrm{Gal}(M/F)$ is a surjective homomorphism, hence for any $\tau \in \mathrm{Gal}(M/F)$ there exists $\sigma \in \mathrm{Gal}(E/F)$ such that the restriction of σ to M is τ.*

Remark. Proposition 3.18, 3;19 and 3.20 have hardly been discussed in the class for lack of time.

Reference: J.S. Milne, Fields and Galois Theory Version 4.52 March 17, 2017.