Lecture 14.2

Last time:

- A polynomial $f \in \mathbb{Q}[x]$ is solvable with $+, -, \cdot, \div$ and $\sqrt[m]{\ }$ if and only if f splits in a tower

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r$$

with $K_j = K_{j-1}(\sqrt[m_j]{\beta_j})$ for $\beta_j \in K_{j-1}$.

- A finite group G is solvable if it has a chain of subgroups

$$\{1\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_r = G$$

with $G_{j-1} \trianglelefteq G_j$ and G_j / G_{j-1} abelian.

- (Galois, 1832) $f \in \mathbb{Q}[x]$ is solvable if and only if $\mathrm{Gal}(f) = \mathrm{Gal}(K_f/\mathbb{Q})$ is solvable.

- For $n \geq 5$, there are polynomials of degree n with $\mathrm{Gal}(f)$ not solvable, e.g. $\mathrm{Gal}(x^5 + 20x + 16) \cong A_5$.

Let's finish the proof of $(\Rightarrow)$ in Galois' Theorem.

We started with $f \in \mathbb{Q}[x]$ solvable, with

$$\begin{array}{ccccccccc} \mathbb{Q} = K_0 & \subseteq & K_1 & \subseteq & \cdots & \subseteq & K_n & = & K \\ & & \| & & & & \| & & \\ & & \mathbb{Q}(\alpha_1) & & & & \mathbb{Q}(\alpha_1, \ldots, \alpha_n) & & \end{array}$$

as above and $K = K_f$.

Consider the tower

$$\begin{tikzcd} K = E(\alpha_2, \ldots, \alpha_n) \arrow[d, dash, "\text{solvable by induction}"] \\ E = \mathbb{Q}(\zeta_{m_1}, \alpha_1) \arrow[d, dash] \\ F = \mathbb{Q}(\zeta_{m_1}) \arrow[d, dash, "\text{abelian}"] \\ \mathbb{Q} \end{tikzcd}$$

Notice that $E = F(\alpha_1)$ and since $\alpha_1^{m_1} \in E$,

E/F is a splitting field for $x^{m_1} - \alpha_1^{m_1}$.

Exercise 1 below will show that $Gal(E/F)$

is abelian.

Now $Gal(K/\mathbb{Q})$ has a chain of subgroups

$$Gal(K/\mathbb{Q}) \supseteq Gal(K/F) \supseteq Gal(K/E) \supseteq \{id\}$$

with :

- $Gal(K/F) \trianglelefteq Gal(K/\mathbb{Q})$ since $F = \mathbb{Q}(\zeta_{m_1})$ is a splitting field.

- $Gal(K/\mathbb{Q}) / Gal(K/F) \cong Gal(F/\mathbb{Q})$ by the Fundamental Theorem, and $\mathrm{Gal}(F/\mathbb{Q})$

is abelian.

- $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$ since E/F is a splitting field.

- $\mathrm{Gal}(K/F) / \mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F)$ is abelian.

- $\mathrm{Gal}(K/E)$ is solvable by induction.

This proves $\mathrm{Gal}(K/\mathbb{Q})$ is solvable. $\square$

Exercise 1: (a) Prove $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is

isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, which is abelian.

(b) For any $a \in F \subseteq \mathbb{C}$, prove that $\mathrm{Gal}(x^m - a)$ is abelian.

We didn't prove the converse of Galois' Theorem, but see section 18.4 in the textbook.

$\boxed{\text{Constructible Polygons, Revisited}}$

Recall: we proved that if $\alpha \in \mathbb{C}$ is a constructible number, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$.

The converse is not quite true.

However:

$\boxed{\text{Theorem}}$ Let $K/\mathbb{Q}$ be a Galois extension of degree 2^k for some $k \geq 1$. Then every $\alpha \in K$ is constructible.

Pf: Since $K/\mathbb{Q}$ is Galois, $G = \mathrm{Gal}(K/\mathbb{Q})$ is a group of order 2^k.

It is a fact from group theory (see Cor. 20.3 in the textbook) that any such G is solvable, with

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = G$$

having $|G_j| = 2^j$.

Then for each $1 \le j \le k$, $[G_j : G_{j-1}] = 2$.

Set $K_j = K^{G_{k-j}}$.

By the fundamental theorem of Galois theory,

$$[K_j : K_{j-1}] = [K^{G_{k-j}} : K^{G_{k-j+1}}]$$

$$= [G_{k-j+1} : G_{k-j}] = 2$$

and quadratic extensions are constructible,

so every $\alpha \in K$ is constructible. $\square$

Recall: for p prime, a regular p-gon is constructible only if p is a Fermat prime, $p = 2^{2^k} + 1$, $k \geq 0$.

$\boxed{\text{Theorem (Gauss)}}$ For $n \geq 2$, a regular n-gon is constructible if and only if $n = 2^m p_1 \cdots p_r$ for $m \geq 0$ and distinct Fermat primes p_j.

Pf: The vertices of a regular n-gon may be viewed as the nth root of unity in $\mathbb{C}$.

Set $\alpha = \cos\left(\frac{2\pi}{n}\right)$, where $\frac{2\pi}{n}$ is the

interior angle of $e^{2\pi i/n} = \zeta$.

Then $\alpha = \frac{1}{2}(\zeta + \zeta^{-1})$, which can be

rewritten $\zeta^2 - 2\alpha\zeta + 1 = 0$, so

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2.$$

By the tower law, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a

power of 2 if and only $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is.

We've seen before that for any $\zeta = e^{2\pi i/n}$,

$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, the totient of n.

From number theory, if $n = p_1^{m_1} \cdots p_s^{m_s}$,

$$\phi(n) = \prod_{j=1}^{s} p_j^{m_j - 1}(p_j - 1).$$

For any prime p, the expression $p^{m-1}(p-1)$ is a power of 2 if and only if $p = 2$ or $m = 1$ and $p - 1 = 2^r$.

We know this implies $r = 2^k$, so

$$p = 2^{2^k} + 1.$$

This finishes the proof. $\square$

THANKS FOR A

GREAT SEMESTER!