4/22/15

HW 6 due now.
Exam 3 on Friday.

Today: Review for Exam 3.

The exam will deal with the chain of field extensions.

$$\mathbb{Q} \subsetneq \mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad} \subsetneq \mathbb{Q}_{alg} \subsetneq \mathbb{C}.$$

Recall the definitions:

$\mathbb{Q}$ = "rational numbers"
= fractions of integers

$\mathbb{Q}_{const}$ = "constructible numbers"
= numbers formed from 1 using $+, -, \times, \div, \sqrt{\ }$.

$\mathbb{Q}_{rad}$ = "radical numbers"
= numbers formed from 1 using $+, -, \times, \div, \sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }, \sqrt[5]{\ }, \ldots$

$\mathbb{Q}_{alg}$ = "algebraic numbers"
= complex roots of polynomials with rational coefficients.

We proved that $\mathbb{Q}_{const} \subsetneq \mathbb{C}$ as follows.

Useful Little Theorem: Let $\mathbb{F} \subseteq \mathbb{F}[\alpha]$ be a Quadratic Field Extension and consider $f(x) \in \mathbb{F}[x]$ of degree 3. If f has a root in $\mathbb{F}[\alpha]$ then it has a root in $\mathbb{F}$.

Proof: Let $f(u) = 0$ with $u \in \mathbb{F}[\alpha]$. If $u \in \mathbb{F}$ then we're done. Otherwise we have $u^* \neq u$ and u^* is another root of f, hence

$$f(x) = a(x-u)(x-u^*)(x-v)$$

where $v \in \mathbb{F}[\alpha]$. If $v \in \mathbb{F}$ then we're done. Otherwise we have $v^* \neq v$ and v^* is another root of f. But this contradicts the fact that f has degree 3. ///

Corollary: Consider $f(x) \in \mathbb{Q}[x]$ of degree 3. If f has a constructible root then f has a rational root.

Proof: Suppose $f(u) = 0$ where u is constructible. Then there exists a chain of QFE

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_k$$

such that $u \in \mathbb{F}_k$. By repeatedly applying the theorem we find that f must have a root in $\mathbb{Q}$. ///

Corollary: It is impossible to double the cube, trisect the angle, or construct the regular 7-gon.

Proof: The numbers $\sqrt[3]{2}$, $2\cos(\pi/9)$, $2\cos(\frac{2\pi}{7})$ are roots of the polynomials

$$x^3 - 2, \quad x^3 - 3x - 1, \quad x^3 + x^2 - 2x + 1,$$

respectively. These are degree 3 polynomials over $\mathbb{Q}$ with no rational roots. Hence their roots are not constructible. $\blacksquare$

Gauss & Wantzel took this idea further by showing the following.

Theorem: The number $\cos\left(\frac{\pi}{n}\right)$ is constructible if and only if $\varphi(n)$ is a power of 2. //

Q: Is the 48-gon constructible?

A: Let's compute $\varphi(48)$. Its prime factorization is

$$48 = 2^4 \cdot 3$$

Hence
$$\varphi(48) = 48\left(\frac{1}{2}\right)\left(\frac{2}{3}\right).$$
$$= 24\left(\frac{2}{3}\right)$$
$$= 16$$

Since 16 is a power of 2, the 48-gon <u>is</u> constructible.

We can rephrase the Gauss-Wantzel Theorem by noting that $\varphi(n)$ is a power of 2 if and only if

$$n = 2^k \cdot p_1 \cdot p_2 \cdots p_m$$

where $p_1, p_2, \ldots, p_m$ are distinct "Fermat primes". The only known Fermat primes are

$$3, 5, 17, 257, 65537.$$

///

Since $\sqrt[3]{2}$, $\cos\left(\frac{\pi}{9}\right)$, $\cos\left(\frac{\pi}{7}\right)$ are radical numbers (by Cardano's formula) we have also proved that

$$\mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad}.$$

The fact that $\mathbb{Q}_{rad} \subsetneq \mathbb{Q}_{alg}$ was proved by Abel and Ruffini before 1820. In fact they showed that there exists a polynomial $f(x) \in \mathbb{Q}[x]$ of degree 5 whose roots are not radical.

This means that there can be no such thing as a "Quintic Formula".

Galois soon came along and explained everything based on ideas of Lagrange.

Lagrange's solution of the Quadratic:

Consider $(x-r_1)(x-r_2) = x^2 - e_1 x + e_2$ where $e_1 = r_1 + r_2$ and $e_2 = r_1 r_2$.
Our goal is to solve algebraically for r_1 & r_2 in terms of e_1 & e_2.

Lagrange's first trick is to define

$$\left.\begin{aligned} s_1 &= r_1 + r_2 \\ s_2 &= r_1 - r_2 \end{aligned}\right\} \iff \left\{\begin{aligned} r_1 &= (s_1 + s_2)/2 \\ r_2 &= (s_1 - s_2)/2 \end{aligned}\right.$$

Thus we are done if we can solve for s_1 & s_2 in terms of e_1 & e_2.

$$s_1 = r_1 + r_2 = e_1 \ \checkmark \quad \text{is easy.}$$

But note that $s_2 = r_1 - r_2$ is <u>not</u> a <u>symmetric</u> function of r_1 & r_2, hence it is <u>not</u> a function of e_1 & e_2.

What can we do?

Lagrange's second trick is to square S_2 to make it symmetric.

$$S_2^2 = (r_1 - r_2)^2$$
$$= \underline{r_1^2} + r_2^2 - 2r_1r_2$$

The leading term is r_1^2. Note that

$$e_1^2 = (r_1 + r_2)^2$$
$$= \underline{r_1^2} + r_2^2 + 2r_1r_2$$

has the <u>same</u> leading term. Subtract to get

$$S_2^2 - e_1^2 = -4r_1r_2 = -4e_2$$

hence $S_2^2 = e_1^2 - 4e_2$.

Let $S_2 = \sqrt{e_1^2 - 4e_2}$ be <u>either</u> of the two square roots. (It doesn't matter which.).

Finally, we can solve for the roots

$$r_1 = \frac{1}{2}(s_1 + s_2) = \frac{1}{2}\left(e_1 + \sqrt{e_1^2 - 4e_2}\right)$$

$$r_2 = \frac{1}{2}(s_1 - s_2) = \frac{1}{2}\left(e_1 - \sqrt{e_1^2 - 4e_2}\right).$$

This is just the Quadratic Formula, but now we understand it better.

Lagrange's method also works for the cubic and quartic equations, and it led Galois to understand why there is <u>no</u> quintic formula.