Ruler and compass constructions:

There are two famous problems in this regard:

(A) Is it possible to trisect an arbitrary angle using ruler and compass? I.e if you have two lines with angle θ between, can you construct two lines with angle $\theta/3$ between?

(B) Given a cube  with volume V, is it possible to construct the side length of a cube whose volume is $2V$? I.e. if $V = \ell^3$ then can we construct $\sqrt[3]{2}\,\ell$ so that $2V = (\sqrt[3]{2}\,\ell)^3$?

Terminology: Suppose $F \subset \mathbb{R}$ is a subfield. Then

$$\{(c,d) \mid c, d \in F\}$$ is called the

plane of F.

If P, Q are points in the plane of F then the line through P, Q is called a line in F and consists of the set of solutions (x,y) in the plane of F to an equation $ax + by + c = 0$ for some $a, b, c \in F$.

Similary a circle with centre P and radius PQ is a circle in F, an is all solutions to

$$x^2 + y^2 + ax + by + c = 0 \quad (\text{some } a, b, c \in F).$$

<u>Lemma</u>: Let $F \subseteq \mathbb{R}$ be a subfield, Suppose that L_1, L_2 are nonparallel lines in F and C_1, C_2 are distinct circles in F. Then:

(i) $L_1 \cap L_2$ is a point in the plane of F.

(ii) $L_1 \cap C_1 = \emptyset$ or $L_1 \cap C_1$ consists of points (one or two of them) in the plane of $F(\sqrt{u})$ for some $u \in F$.

(iii) $C_1 \cap C_2 = \emptyset$ or consists of one or two points in the plane of $F(\sqrt{u})$ for some $u \in F$.

<u>Proof</u>: (i) is an easy exercise, and (iii) reduces to (ii) by showing that and intersection of circles is equal to the intersection of some circle and a line.

To prove (ii):

Suppose L_1 has equation $dx + ey + f = 0$ $(d, e, f \in F)$.
We will consider the case $d \neq 0$, in which case we can assume $d = 1$ since

$$dx + ey + f = 0$$

$$\text{and } d^{-1}dx + d^{-1}ey + d^{-1}f = 0$$

have the same set of solutions.

Then $x = -(ey + f)$, so if $(x, y) \in L_1 \cap C_1$ then the equation of C_1 is of the form:

$$(-(ey+f))^2 + y^2 + a(-ey-f) + by + c = 0$$

$$\Rightarrow Ay^2 + By + C = 0 \text{ upon rearranging.}$$

If $A = 0$ then $y = \frac{-C}{B} \in F$ and $x \in F$. If $A \neq 0$

Then again multiply through by A^{-1} to assume $A=1$.
Then completing the square gives

$$\left(y+B/2\right)^2 + \left(C - B^2/4\right) = 0$$

So, either $L_1 \cap C_1 = \emptyset$ or $y + B/2 = \sqrt{C - B^2/4}$ so $y \in F(\sqrt{u})$ with $u = \sqrt{C - B^2/4}$ and $x \in F(\sqrt{u})$, too.

Definition: A number $c \in \mathbb{R}$ will be called constructible if $(c,0)$ can be constructed by a finite sequence of ruler/compass constructions beginning with a lattice of integer points. A point (c,d) is constructible if both c and d are constructible.

A long series of exercises using the above lemma shows:

Lemma: Suppose that c and d are constructible numbers. Then:
(i) If $c \geq 0$ then $\sqrt{c}$ is constructible
(ii) $c \pm d$, cd and c/d $(d \neq 0)$ are constructible.
(iii) The constructible numbers form a subfield of $\mathbb{R}$ containing $\mathbb{Q}$.

Proposition: If $c \in \mathbb{R}$ is constructible, then $[\mathbb{Q}(c):\mathbb{Q}] = 2^k$ for some $k \geq 0$.

Proof: Start with such a number c. Since c is constructible, there's a finite sequence of ruler and compass steps that leads to the creation of the point $(c, 0)$. In the course of these steps (starting from integer points only) various points are determined as the intersection of two lines / two circles, where the lines/circles are determined by points P, Q or a point P and radius r that have previously been constructed.

Starting from the integer points, the first point constructed which is not in $\mathbb{Q}^2$ will be a point with coordinates in $\mathbb{Q}(\sqrt{u})$ for some $u \in \mathbb{Q}$, or equivalently it will be in $\mathbb{Q}(v)$ with $v^2 \in \mathbb{Q}$. This extension is of degree 1 or 2, depending on $v \in \mathbb{Q}$ or $v \notin \mathbb{Q}$.

The next new point lies in $\mathbb{Q}(v)(w) = \mathbb{Q}(v, w)$ where $w^2 \in \mathbb{Q}(v)$. Continuing in this manner, any finite sequence of ruler/compass constructions gives

$$\mathbb{Q} \subset \mathbb{Q}(v_1) \subset \cdots \subset \mathbb{Q}(v_1, \ldots, v_n)$$

where $[\mathbb{Q}(v_1, \ldots, v_i) : \mathbb{Q}(v_1, \ldots, v_{i-1})] = 1$ or 2. The point $(c, 0)$ constructed this way has coordinates in $\mathbb{Q}(v_1, \ldots, v_n)$.

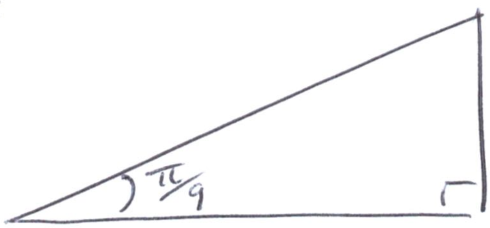
Then $[\mathbb{Q}(v_1, \ldots, v_n) : \mathbb{Q}] = 2^k$ for some k, and

$$[\mathbb{Q}(v_1, \ldots, v_n) : \mathbb{Q}] = [\mathbb{Q}(c) : \mathbb{Q}][\mathbb{Q}(v_1, \ldots, v_n) : \mathbb{Q}(c)]$$

Implies that $[\mathbb{Q}(c):\mathbb{Q}] = 2^l$ for some l, and that c is algebraic over $\mathbb{Q}$.

<u>Corollary</u>: One cannot trisect an angle of $\pi/3$ using a ruler and compass.

<u>Proof</u>: If it were possible, then one could construct a triangle:



and consequently construct the ratio $\cos(\pi/9)$.

However there is a trig identity:

$$\cos(3\alpha) = 4(\cos(\alpha))^3 - 3\cos\alpha,$$

and if $\alpha = \pi/9$ then $\cos(3\cdot(\pi/9)) = \cos(\pi/3) = \frac{1}{2}$

and so ~~$\alpha = \pi/9$ is a root of~~ $x = \cos(\pi/9)$ is a root of

$$4x^3 - 3x - \tfrac{1}{2},$$

hence a root of $8x^3 - 6x - 1$. This polynomial is irreducible in $\mathbb{Q}[x]$ and so $[\mathbb{Q}(\cos(\pi/9)) ; \mathbb{Q}] = 3$, thus $\cos(\pi/9)$ is not constructible and $\pi/3$ cannot be trisected.

Begin Galois theory and related topics:

Suppose that $K \subseteq E$, $L \subseteq F$ are fields and that $\sigma : K \longrightarrow L$ is an isomorphism. A central question is:

Q: Does there exist an isomorphism $\tau : E \longrightarrow F$ such that $\tau = \sigma$ when restricted to K?

There is an easy answer to this question for simple extensions. First recall (or notice) that if $\sigma : K \longrightarrow L$ is an isomorphism of fields, then there's a map (which we'll also call σ):

$$\sigma : K[x] \longrightarrow L[x]$$

given by applying σ to the coefficients:

$$\sigma\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \sigma(a_i) x^i.$$

To keep brackets from piling up, given $f \in R[x]$ we will write σf instead of $\sigma(f)$.

Theorem: Suppose $\sigma : K \longrightarrow L$ is an isomorphism of fields, and that u, v are elements of extension fields of K, L respectively. If either:

(i) u is transcendental over K and v is transcendental over L.

or

(ii) u is a root of an irreducible $f \in K[x]$ and v is a root of $\sigma f \in L[x]$,

then σ extends to an isomorphism of fields $K(u) \simeq K(v)$.

<u>Proof</u>: We already saw that (i) is true, since $\sigma: K \to L$ obviously extends to

$$\sigma: K(x) \longrightarrow L(x)$$
$$f/g \longmapsto \sigma f/\sigma g$$

and so $K(u) \simeq K(x) \xrightarrow{\sigma} L(x) \simeq L(v)$ when u, v are transcendental.

For (ii), we can assume that f is monic. Then as $\sigma: K \to L$ carries 1_K to 1_L, σf is also monic; and since $\sigma: K[x] \to L[x]$ is an isomorphism we know σf is also irreducible. From our earlier analysis of algebraic extensions we have isomorphisms:

$$K[x]/(f) \longrightarrow K[u] = K(u)$$
$$g(x) + (f) \longmapsto g(u)$$

and

$$L[x]/(\sigma f) \longrightarrow L[v] = L(v)$$
$$h(x) + (\sigma f) \longmapsto h(v).$$

The map σ satisfies $\sigma(I) = J$, where I is the ideal (f) and $J = (\sigma f)$, and therefore

σ gives an isomorphism

$$K[x]/(f) \longrightarrow L[x]/(\sigma f)$$

$$g(x) + (f) \longmapsto \sigma g(x) + (\sigma f).$$

Thus there's an isomorphism

$$K(u) = K[u] \simeq K[x]/(f) \simeq L[x]/(\sigma f) \simeq L[v] = L(v)$$

Given by $g(u) \longmapsto \sigma g(v)$, in particular if g is a constant polynomial (ie $g \in K$) then σg is the image of g under this isomorphism (ie the iso extends σ).

<u>Corollary</u>: Suppose $K \leq E$ and $K \leq F$ are fields, and suppose $u \in E$ and $v \in F$ are algebraic over K. Then u and v are roots of the same irreducible $f \in K[x]$ if and only if there's an isomorphism $\sigma : K(u) \longrightarrow K(v)$ with $\sigma|_K = id$.

<u>Proof</u>: ($\Longrightarrow$) Apply the previous theorem with $\sigma = id$.

($\Longleftarrow$). Suppose $K(u) \simeq K(v)$ via σ with $\sigma(k) = k \, \forall k \in K$ and $\sigma(u) = v$. Say f is the minimal poly of u, so $0 = f(u) = \sum_{i=0}^{n} a_i u^i$. Then

$0 = \sigma\left(\sum_{i=0}^{n} a_i u^i\right) = \sum_{i=0}^{n} \sigma(a_i u^i) = \sum_{i=0}^{n} a_i v^i = f(v)$, so v is also a root of f.

All this culminates in the following theorem:

Theorem: Suppose that K is a field and $f \in K[x]$ with $\deg f = n$. Then there exists a simple extension $F = K(u)$ such that

(i) u is a root of f,

(ii) $[F : K] \leq \deg f = n$ with equality iff f is irreducible

(iii) If $f(x)$ is irreducible then $K(u)$ is unique up to an isomorphism σ that is the identity on K.

Proof: Combine all previous facts in the obvious way.

This finishes the recap of field theory. There are other facts about algebraic extensions that I intend to skip, assuming they were covered in algebra II. They are theorems 1.11 – 1.14 of section IV. 1 in Hungerford, and are as follows:

Theorem: If $K \subseteq F$ are fields and $[F:K] < \infty$, then F is algebraic over K.

Proof (Sketch): If $[F:K] = n$ then $\forall u \in F$ $\{1, u, \ldots, u^n\}$ are linearly independent over K, giving

$$\sum_{i=0}^{n} a_i u^i = 0 \quad \text{for some } a_i \in K. \implies u \text{ algebraic.}$$

<u>Theorem</u>: Suppose that $K \subseteq F$ and X is a subset of F of elements algebraic over K. If $F = K(X)$ then F is algebraic over K. If $|X| < \infty$ then $[F : K] < \infty$.

<u>Proof</u> (Sketch):

If $v \in F$ then $\exists\, u_1, \ldots, u_n \in X$ s.t. $v \in K(u_1, \ldots, u_n)$. Using $K(u_1) \subset K(u_1)(u_2) = K(u_1, u_2)$, etc induct to show v is algebraic. If $|X| < \infty$ then do the same tower of fields

$$K(u_1) \subset K(u_1, u_2) \subset \ldots \subset K(u_1, \ldots, u_n); \ \{u_i\}_{i=1}^{n} = X$$

and then $[F : K]$ is the product of $[K(u_1, \ldots, u_{i+1}) : K(u_1, \ldots, u_i)]$

<u>Theorem</u>: If $K \subset E \subset F$ and F/E is algebraic and E/K is algebraic, then F/K is algebraic.

<u>Theorem</u>: If $K \subseteq F$ are fields, then

$$E = \{u \in F \mid u \text{ is algebraic over } F\}$$

is an algebraic field extension of K.

§4.2 The fundamental theorem

Let F be a field. Let

$$\mathrm{Aut}\, F = \{\sigma \mid \sigma : F \longrightarrow F \text{ is a field automorphism}\}$$

Then $\mathrm{Aut}\, F$ is a group with composition as the operation.

<u>Definition</u>: Suppose that K is a field and that E, F are extensions of K. A nonzero field homomorphism $\sigma : E \longrightarrow F$ which satisfies $\sigma(k) = k$ $\forall k \in K$ will be called a <u>K-homomorphism</u>. A field automorphism $\sigma : F \longrightarrow F$ with $\sigma(k) = k$ $\forall k \in K$ will be called a <u>K-automorphism</u>.

<u>Lemma</u>: If $K \subseteq F$ are fields, then the set of all K-automorphisms of F forms a group.

<u>Definition</u>: The group from the lemma above is called the <u>Galois group of F over</u> K and is denoted $\mathrm{Aut}_K F$.

<u>Example</u>: Let K be any field, and set $F = K(x)$. Then $\forall a \in K$ with $a \neq 0$ define

$$\sigma_a : F \longrightarrow F \text{ by}$$

$$f(x)/g(x) \longmapsto f(ax)/g(ax)$$

Then one can check that σ_a is a K-automorphism, so $\sigma_a \in \mathrm{Aut}_K F$.

If K is infinite, then each σ_a for $a \in K$ gives a new K-automorphism, so $\mathrm{Aut}_K F$ is infinite.

We can also define, for each $b \in K$, the map

$$\tau_b : F \longrightarrow F$$

$$f(x)/g(x) \longmapsto f(x+b)/g(x+b)$$

and it is also a K-automorphism. If $a \neq 1$ and $b \neq 0$ then $\tau_b \sigma_a \neq \sigma_a \tau_b$, so $\mathrm{Aut}_K F$ is nonabelian.

The most important property of $\mathrm{Aut}_K F$ is that it permutes the roots of polynomials, meaning:

<u>Theorem</u>: Suppose $K \subseteq F$ are fields, and $f \in K[x]$. If u is a root of f and $\sigma \in \mathrm{Aut}_K F$, then $\sigma(u)$ is also a root of F.

<u>Proof</u>: Say $f = \sum_{i=0}^{n} a_i x^i$, $a_i \in K$. Then $f(u) = 0$ so

$$\sum_{i=0}^{n} a_i u^i = 0$$ and we compute

$$0 = \sigma(f(u)) = \sigma\left(\sum_{i=0}^{n} a_i u^i\right) = \sum_{i=0}^{n} \sigma(a_i)\sigma(u^i)$$

$$= \sum_{i=0}^{n} a_i (\sigma(u))^i = f(\sigma(u)).$$

//