For the material on Galois theory we will be assuming that the fields all have characteristic zero. When we get to solvability by radicals we will assume that all fields are subfields of the complex numbers $\mathbb{C}$.

1 Review

The following results are from the review sheet for the midterm.

Theorem 1.1 *Minimal polynomials are irreducible: If α is in some extension field of F and define:*

$$I = \{f(x) \in F[x] : f(\alpha) = 0\}$$

Then:

(a) I is an ideal in $F[x]$

(b) (assuming I is nontrivial) $I = \langle p(x) \rangle$ where $p(x)$ is any polynomial of minimal positive degree in I and

(c) $p(x)$ is irreducible and so I is a maximal ideal.

Theorem 1.2 *If $p(x)$ is an irreducible polynomial of degree n in $F[x]$ and α a root of p in some extension field, then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis for $F(\alpha)$ as a vector space over F and hence $[F(\alpha) : F] = n$.*

Theorem 1.3 *Suppose char(F)=0 and $p(x) \in F[x]$ is irreducible, then p does not have any multiple roots in any extension of F.*

Theorem 1.4 *Suppose char(F)=0 and $[E : F] < \infty$, then there exists $\alpha \in E$ such that $E = F(\alpha)$.*

Theorem 1.5 *If $p(x) \in F[x]$ is an irreducible polynomial and α and β are two roots of p, then $F(\alpha) \simeq F(\beta)$ with an isomorphism which fixes F and takes α to β.*

Theorem 1.6 *If $\sigma : F \to F'$ is an isomorphism, $f \in F[x]$ any polynomial, $E \supseteq F$ a splitting field of f over F, and $E' \supseteq F'$ a splitting field of $\sigma(f)$ over F', then there exists an isomorphism $\rho \supseteq \sigma$ such that $\rho : E \to E'$.*

2 Galois Theory

In this section we assume that all fields have characteristic 0.

Definition 2.1 *The field $K \supseteq F$ is a Galois extension of the field F iff K is the splitting field over F of some polynomial with coefficients in F.*

Proposition 2.2 *Suppose $F \subseteq E \subseteq K$ are fields and K is a Galois extension of F. Then K is a Galois extension of E.*

Proof:
Suppose F_3 is the splitting field of $f \in F_1[x]$. This means that F_3 is the smallest field containing F_1 and all the roots of f. Then $f \in F_2[x]$ since $F_1 \subseteq F_2$ and therefore F_3 is the smallest field containing F_2 and all the roots of f.
:foorP

Definition 2.3 *For fields $F \subseteq E$ define* $\mathrm{aut}(E|F)$ *to be the set of all automorphisms σ of E which fix F, i.e., $\sigma(a) = a$ for all $a \in F$.*

Proposition 2.4 $\mathrm{aut}(E|F)$ *is a group. Furthermore, if $F \subseteq E \subseteq K$ are fields, then* $\mathrm{aut}(K|E)$ *is a subgroup of* $\mathrm{aut}(K|F)$.

Proof:
If $\sigma, \tau \in \mathrm{aut}(E|F)$, then clearly $\sigma \circ \tau$ is an automorphism of E. Given $a \in F$ we have that $\sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a$ and so $\sigma \circ \tau$ fixes F and therefore $\sigma \circ \tau \in \mathrm{aut}(E|F)$. Similarly, $\sigma(a) = a$ implies $\sigma^{-1}(a) = a$ and so $\mathrm{aut}(E|F)$ is a group under composition.

$\mathrm{aut}(K|E)$ is a subgroup of $\mathrm{aut}(K|F)$ since the operation (composition) is the same and any automorphism which fixes E must also fix the smaller field F.
:foorP

Lemma 2.5 *Suppose $\sigma, \rho \in \mathrm{aut}(F(\alpha)|F)$. Then $\sigma = \rho$ iff $\sigma(\alpha) = \rho(\alpha)$.*

Similarly, if $\sigma, \rho \in \mathrm{aut}(F(\alpha_1, \alpha_2, \ldots, \alpha_n)|F)$ then $\sigma = \rho$ iff $\sigma(\alpha_k) = \rho(\alpha_k)$ for all $k = 1, 2, \ldots, n$.

Proof:
The elements of $F(\alpha)$ have the form $\frac{f(\alpha)}{g(\alpha)}$ where $f(x), g(x) \in F[x]$ are polynomials with $g(\alpha) \neq 0$. But then

$$\sigma(\frac{f(\alpha)}{g(\alpha)}) = \frac{\sigma(f(\alpha))}{\sigma(g(\alpha))} = \frac{f(\sigma(\alpha))}{g(\sigma(\alpha))}$$

this last is true because elements of F are fixed by σ. Since the same is true for τ, if $\sigma(\alpha) = \tau(\alpha)$, then

$$\sigma(\frac{f(\alpha)}{g(\alpha)}) = \frac{f(\sigma(\alpha))}{g(\sigma(\alpha))} = \frac{f(\tau(\alpha))}{g(\tau(\alpha))} = \tau(\frac{f(\alpha)}{g(\alpha)})$$

The similar result holds for $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ since its elements have the form

$$\frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)}$$

where f, g are polynomials in $F[x_1, x_2, \ldots, x_n]$.
:foorP

Theorem 2.6 *Suppose that K is the splitting field of a polynomial in $F[x]$ of degree n. Then* $\mathrm{aut}(K|F)$ *is isomorphic to a subgroup of S_n.*

Proof:
Let $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where the α_i are all the roots of $f \in F[x]$ and K is the splitting field of f. If $\sigma \in \text{aut}(K|F)$, then $\sigma(f) = f$ and so if α is a root of f then so is $\sigma(\alpha)$, i.e., $f(\alpha) = 0$ implies $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$. Hence σ must permute the roots α_i of f. By Lemma 2.5 we see that elements of $\text{aut}(K|F)$ are determined by this permutation. Hence the mapping:

$$h : \text{aut}(K|F) \to S_n$$

given by $h(\sigma) = \delta$ where $\sigma(\alpha_i) = \alpha_{\delta(i)}$ is a one-to-one homomorphism and therefore $\text{aut}(K|F)$ is isomorphic to its image which is a subgroup of S_n.
:foorP

Lemma 2.7 *Suppose K is a Galois extension of F, $K \subseteq L$, and $\sigma : K \to L$ an embedding which fixes F. Then and $\sigma(K) = K$.*

Proof:
Note that an embedding is a one-to-one homomorphism and $\sigma(K) = \{\sigma(a) : a \in K\}$. Since $K = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ where the α_i are the roots of some polynomial $f \in F[x]$ and since σ fixes the coefficients of f it must be that for every i there is j such that $\sigma(\alpha_i) = \alpha_j$. Hence $\sigma(K) = K$.
:foorP

Theorem 2.8 *Suppose K is a Galois extension of F, then $|\text{aut}(K|F)| = [K : F]$*

Proof:
By Theorem 1.4 there exists $\alpha \in K$ such that $K = F[\alpha]$. By Theorem 1.1 there exists an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

Claim. K is the splitting field of p.

Proof of Claim: Let L be any extension field in which p splits and suppose β is any root of p in L. Then there exists an isomorphism $\sigma : F(\alpha) \to F(\beta)$ which fixes F and sends α to β (Theorem 1.5). But then by Theorem 1.6 the map σ extends to an automorphism $\rho : L \to L$. Since ρ fixes F and by Lemma 2.7 $\rho(K) = K$. Since $\rho(\alpha) = \beta$ this means β is in K. Since β was an arbitrary root of p this means that p splits in K.

End proof of Claim.

We have that by Theorem 1.2 that $[K : F] = n$ where n is the degree of p and since irreducible polynomial have distinct roots (Theorem 1.3), the roots of p are $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. By Theorem 1.5 for every i there exists $\sigma_i : F(\alpha) \to F(\alpha_i)$. But automorphisms of $F(\alpha)$ which fix F are determined by the values on α (Lemma 2.5) we have that

$$\text{aut}(K|F) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$$

Hence the theorem is proved.
:foorP

Lemma 2.9 *Suppose $F \subseteq E, E' \subseteq K$, K is a Galois extension of F and $\sigma : E \to E'$ and isomorphism which fixes F. Then there exists $\rho \in \text{aut}(K|F)$ which extends σ.*

Proof:
This is just a special case of Theorem 1.6. If K is the splitting field of $f \in F[x]$ over F, then $\sigma(f) = f$ since σ fixes F and $K = K'$ is the splitting field of f over both E and E'.
:foorP

Theorem 2.10 *Suppose K and E are Galois extensions of F and $F \subseteq E \subseteq K$. Then* $\text{aut}(K|E)$ *is a normal subgroup of* $\text{aut}(K|F)$ *and*

$$\frac{\text{aut}(K|F)}{\text{aut}(K|E)} \simeq \text{aut}(E|F)$$

Proof:
Define the map

$$h : \text{aut}(K|F) \to \text{aut}(E|F) \text{ by } h(\rho) = \rho\restriction E$$

i.e., we restrict ρ to E. By Lemma 2.7 we have that $\rho(E) = E$ and so this restriction is in $\text{aut}(E|F)$. It is easy to check that h is a group homomorphism.

Claim. The kernel of h is $\text{aut}(K|E)$. This is clear because
$h(\rho) =$identity iff $\rho\restriction E$ fixes E iff $\rho \in \text{aut}(K|E)$.

Claim. h is onto. This follows from Lemma 2.9, since if we take $E = E'$ in that Lemma then for every $\sigma \in \text{aut}(E|F)$ there exists $\rho \in \text{aut}(K)$ such that $\rho \supseteq \sigma$. But this means $h(\rho) = \rho\restriction E = \sigma$. Hence h is onto.

The homomorphism theorem of group theory says the range of h is isomorphic to the quotient group of its domain by its kernel (which is a normal subgroup) and so the Theorem is proved.
:foorP

3 More Galois Theory

In this section we develop some more of the basics of Galois Theory. It will not be needed for the section on solvability by radicals.

Theorem 3.1 *Suppose K is a Galois extension of F and $p(x) \in F[x]$ is an irreducible polynomial. Then either all the roots of p are in K or none of them are.*

Proof:

Suppose K is the splitting field of $f(x)$ over F. Let L be the splitting field of $p(x)$ over K. It follows that L is the splitting field of $f(x)p(x)$ over F and so it is a Galois extension of F.

Suppose $\alpha \in K$ and $p(\alpha) = 0$. We need to show all the roots of p are in K. Let $\beta \in L$ be any root of p. We have that there exists $\sigma : F(\alpha) \to F(\beta)$ which fixes F and maps α to β. By Lemma 2.9 that there exists $\rho : L \to L$ which extends σ. But by Lemma 2.7 we have that $\rho(K) = K$. But this implies that $\rho(\alpha) = \beta \in K$. Hence K contains all the roots of p.
:foorP

Example 3.2 *(a) There exists fields $F_1 \subseteq F_2 \subseteq F_3$ such that F_3 is a Galois extension of F_1 but F_2 is* **not** *a Galois extension of F_1.*

(b) There exists fields $F_1 \subseteq F_2 \subseteq F_3$ such that F_3 is a Galois extension of F_2 and F_2 is a Galois extension of F_1, but F_3 is **not** *a Galois extension of F_1.*

Proof:
Hint:
(a) $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha\beta, \alpha^2\beta)$ where $\alpha = e^{\frac{2\pi}{3}i}$ and $\beta =^3 \sqrt{2}$
(b) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$
:foorP

Definition 3.3 *For $H \subseteq \text{aut}(K|F)$ define* $\text{fix}(H) = \{a \in K : \ \forall \sigma \in H \ \ \sigma(a) = a\}$

Proposition 3.4 *Suppose $F \subseteq K$ are fields and $H \subseteq \text{aut}(K|F)$, then $E = \text{fix}(H)$ is a field such that $F \subseteq E \subseteq K$.*

Proof:
Since $\sigma \in \text{aut}(K|F)$ implies it fixes each element of F, this implies that $F \subseteq E$. $E \subseteq K$ by definition. To see that E is a subfield of K. Suppose $x, y \in E$. Then for every $\sigma \in H$ we know that $\sigma(x) = x$ and $\sigma(y) = y$. Since σ is a field automorphism we have that

$$\sigma(x + y) = \sigma(x) + \sigma(y) = x + y \text{ and } \sigma(xy) = \sigma(x)\sigma(y) = xy$$

and so $x + y \in E$ and $xy \in E$. Similarly $x - y$ and x/y are in E, so its a subfield.
:foorP

Lemma 3.5 *Suppose K is a Galois extension of F, then $F = \text{fix}(\text{aut}(K|F))$.*

Proof:
$F \subseteq \text{fix}(\text{aut}(K|F))$ is trivial, since by definition every $\sigma \in \text{aut}(K|F)$ fixes F.

To see the other way that $\text{fix}(\text{aut}(K|F) \subseteq F$, what we need to show is that for every $\alpha \in K$ with $\alpha \notin F$ there exists $\rho \in \text{aut}(K|F)$ such that $\rho(\alpha) \neq \alpha$.

So fix such an α and let $p(x) \in F[x]$ be the minimal (irreducible) polynomial such that $p(\alpha) = 0$. We know that since irreducible polynomials have distinct roots (Theorem 1.3) that p has a root $\beta \neq \alpha$. Since p splits in K (Lemma 3.1) there is such a $\beta \in K$. Let $\sigma : F(\alpha) \to F(\beta)$ be an isomorphism fixing F and taking α to β (Theorem 1.5). Using Lemma 2.9 with $E = F(\alpha)$ and $E' = F(\beta)$ we get that there exists $\rho \in \text{aut}(K|F)$ extending σ. Since $\rho(\alpha) = \beta \neq \alpha$ we are done.
:foorP

Lemma 3.6 *Suppose K is a Galois extension of F and G a subgroup of* $\text{aut}(K|F)$ *and* $\text{fix}(G) = F$*, then* $G = \text{aut}(K|F)$.

Proof:
As in the proof of Theorem 2.8 let $K = F[\alpha]$, $p(x) \in F[x]$ the minimal polynomial of α, and $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where $\alpha_i \in K$ are the roots of p. In that proof we showed that $|\text{aut}(K|F)| = n$.

Suppose for contradiction that $|G| = m < n$. By reordering the α_i let

$$\{\alpha_1, \alpha_2, \ldots, \alpha_m\} = \{\sigma(\alpha) : \sigma \in G\}$$

Consider the polynomial

$$q(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)$$

Note that each $\sigma \in G$ permutes the set $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and hence

$$\sigma(q(x)) = (x - \sigma(\alpha_1))(x - \sigma(\alpha_2)) \cdots (x - \sigma(\alpha_m)) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) = q(x)$$

It follows if we write

$$q(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

that for each $\sigma \in G$ that $\sigma(b_k) = b_k$ for each k. But this implies (since $\text{fix}(G) = F$) that $q(x) \in F[x]$. This is a contradiction since q divides p but p is supposed to be irreducible in $F[x]$.
:foorP

Theorem 3.7 *Suppose K is a Galois extension of F, then there is a one-to-one correspondence between the subgroups of* $\text{aut}(K|F)$*,*

$$\mathcal{G} = \{H : H \subseteq \text{aut}(K|F) \textit{ is a subgroup}\}$$

and the set of intermediate fields between F and K,

$$\mathcal{F} = \{E : F \subseteq E \subseteq K \textit{ and } E \textit{ is a field}\}$$

This correspondence is given by the two maps

$$\phi : \mathcal{G} \to \mathcal{F} \textit{ defined by } \phi(H) = \text{fix}(H)$$

and

$$\psi : \mathcal{F} \to \mathcal{G} \textit{ defined by } \phi(E) = \text{aut}(K|E)$$

which are inverses of each other.

Proof:

Suppose $E \in \mathcal{F}$. Then K is a Galois extension of E and so by Lemma 3.5 we have that $E = \text{fix}(\text{aut}(K|E))$. But this means $E = \phi(\psi(E)$.

Suppose $G \in \mathcal{G}$. Let $E = \text{fix}(G)$. By Lemma 3.6 we have that $G = \text{aut}(K|E)$. But this just means that $G = \psi(\phi(G)$.

Hence the two maps are inverses of each other and the Theorem is proved.
:foorP

4 Tartaglia's method for solving cubics

Step 1. Given $x^3+ax^2+bx+c=0$ substitute $x+\alpha$ for x and pick α so as to eliminate the coefficient of x^2.

Step 2. Given $x^3+px+q=0$ substitute $x+\frac{\beta}{x}$ for x and choose β so as to eliminate the two most complicated coefficients.

The resulting equation will be:

$$x^3+\frac{\beta^3}{x^3}+q=0$$

which is quadractic in x^3. If u is a solution of it, then $u+\frac{\beta}{u}+\alpha$ is a solution of the original equation.

Definition 4.1 *A polynomial $f(x)\in\mathbb{Q}[x]$ is solvable by radicals iff its roots are in the smallest subfield $S\subseteq\mathbb{C}$ which is closed under taking all complex roots, i.e., if $a\in S$ and $n\in\mathbb{N}$ then all n complex roots of a are in S, i.e., x^n-a splits in S.*

It is also true that every $f(x)\in\mathbb{Q}[x]$ of degree 4 is solvable by radicals.
Hint: To solve the quartic below factor it into quadratics:

$$x^4+px^2+qx+r=(x^2+ax+b)(x^2-ax+c)$$

and then show that a^2 is the solution of a cubic:

$$\begin{aligned} c+b-a^2 &= p \\ (c-b)a &= q \\ bc &= r \\ (c+b)^2-(c-b)^2 &= 4bc=4r \\ (p+a^2)^2-q^2/a^2 &= 4r \end{aligned}$$

5 Solvability by radicals

In this section we assume all our fields are subfields of the complex numbers $\mathbb{C}$.

Definition 5.1 *For G a finite group define G is a solvable group by induction on $|G|$. G is solvable iff either G is abelian or there exists a normal subgroup $H\triangleleft G$ such that both H and G/H are solvable.*

Definition 5.2 *Given fields $F\subseteq E\subseteq\mathbb{C}$ we say that E is a radical Galois extension of F iff there exists $n\in\mathbb{N}$ and $a\in F$ such that E is the splitting field of the polynomial x^n-a over F.*

Theorem 5.3 *Suppose that E is a radical Galois extension of F, then* $\mathrm{aut}(E|F)$ *is a solvable group.*

Proof:
Suppose E is the splitting field of $x^n - a$ over F. Let $\beta \in \mathbb{C}$ be any complex number such that $\beta^n = a$. Let $\alpha = e^{\frac{2\pi i}{n}}$. Then we have that

$$E = F(\beta, \beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^{n-1}) = F(\alpha, \beta)$$

(Note that $\frac{\alpha\beta}{\beta} = \alpha$ so $\alpha \in E$.)

$F \subseteq F(\alpha) \subseteq F(\alpha, \beta) = E$ the field $F(\alpha)$ is a Galois extension of F since it is the splitting field of $x^n - 1$, so we have (by Theorem 2.8) that $H = \mathrm{aut}(F(\alpha, \beta)|F(\alpha))$ is a normal subgroup of $G = \mathrm{aut}(F(\alpha, \beta)|F)$ and $\mathrm{aut}(F(\alpha)|F)$ is isomorphic to their quotient G/H.

Claim. $G/H \simeq \mathrm{aut}(F(\alpha)|F)$ is abelian.

Suppose $\sigma, \tau \in \mathrm{aut}(F(\alpha)|F)$, then for some i we have $\sigma(\alpha) = \alpha^i$ and for some j $\tau(\alpha) = \alpha^j$. But then

$$\sigma(\tau(\alpha)) = \sigma(\alpha^j) = (\alpha^j)^i = \alpha^{ji} = \alpha^{ij} = \tau(\sigma(\alpha))$$

Hence (by Lemma 2.5) we have that $\sigma\tau = \tau\sigma$.

Claim. $H = \mathrm{aut}(F(\alpha, \beta)|F(\alpha))$ is abelian.

Suppose $\sigma, \tau \in \mathrm{aut}(F(\alpha, \beta)|F(\alpha))$, then for some then for some i we have $\sigma(\beta) = \alpha^i\beta$ and for some j we have $\tau(\beta) = \beta\alpha^j$. By definition both fix α. But then

$$\sigma(\tau(\beta)) = \sigma(\alpha^j\beta) = (\alpha^j)\sigma(\beta) = \alpha^{j+i}\beta = \alpha^{i+j}\beta = \tau(\sigma(\beta))$$

Hence we have that $\sigma\tau = \tau\sigma$.

Since H and G/H are abelian they are solvable and so by definition G is solvable.
:foorP

Lemma 5.4 *Suppose that G is solvable group and G' is a homomorphic image of G, then G' is solvable. Hence quotient groups of solvable groups are solvable.*

Proof:
Let $h : G \to G'$ be an onto homomorphism. We prove the lemma by induction on $|G|$.

Suppose G is abelian. Then G' is abelian since

$$h(x)h(y) = h(xy) = h(yx) = h(y)h(x)$$

Suppose there exists $H \triangleleft G$ such that H and G/H are solvable. Let $H' = h(H)$. Then H' is a normal subgroup of G' because given $y \in H$ and $x \in G$ we have

$$h(x)h(y)h(x)^{-1} = h(xyx^{-1}) \in H'$$

By induction H' is solvable. It is also true that G'/H' is the homomorphic image of G/H since we can define

$$k : G/H \to G'/H' \text{ by } k(aH) = h(a)H'$$

This is well-defined because $aH = bH$ implies $b^{-1}a \in H$ implies $h(b^{-1}a) \in h(H) = H'$ which implies $h(a)H' = h(b)H'$. It is easy to check that k is an onto homomorphism. Hence by induction G'/H' is solvable. By definition G' is solvable.
:foorP

Theorem 5.5 *Suppose that $F_1 \subseteq F_2 \subseteq F_3 \cdots \subseteq F_m$ is a sequence of radical Galois extensions, i.e., F_{k+1} is a radical Galois extension of F_k for each $k = 1, 2, \ldots, m-1$. Suppose that K is a Galois extension of F_1 such that $K \subseteq F_m$. Then* $\text{aut}(K|F_1)$ *is a solvable group.*

Proof:
This is proved by induction on m

$m = 2$: In this case we have that $F_1 \subseteq K \subseteq F_2$. We have that $\text{aut}(K|F_1)$ is isomorphic to a quotient of $\text{aut}(F_2|F_1)$ (by Theorem 2.8) and we have that $\text{aut}(F_2|F_1)$ is a solvable group by Theorem 5.3. Hence by Lemma 5.4 we have that $\text{aut}(K|F_1)$ is solvable.

$m > 2$: In this case suppose that F_2 is splitting field of $x^n - a \in F_1[x]$ over F_1 and K is the splitting field of $f(x) \in F_1[x]$. Let L be the splitting field of $(x^n - a)f(x)$ over F_1. Then we have

$$F_1 \subseteq F_2 \subseteq L \subseteq F_m \text{ and } F_1 \subseteq K \subseteq L$$

By induction on m we have that $\text{aut}(L|F_2)$ is a solvable group. We also know that L is a Galois extension of F_1 and by Theorem 2.8 we that $H = \text{aut}(L|F_2)$ is a normal subgroup of $G = \text{aut}(L|F_1)$ with quotient group isomorphic to $G/H \simeq \text{aut}(F_2|F_1)$. Since both H and G/H are solvable, we have that G is solvable.

Finally since $F_1 \subseteq K \subseteq L$ we know (by Theorem 2.8) that $\text{aut}(K|F_1)$ is isomorphic to a quotient of $\text{aut}(L|F_1)$ and hence by Lemma 5.4 is solvable.
:foorP

Corollary 5.6 *Suppose $f \in \mathbb{Q}[x]$ is a polynomial which is solvable by radicals. Then if K is the splitting field of f over $\mathbb{Q}$, then* $\text{aut}(K|\mathbb{Q})$ *is a solvable group.*

Theorem 5.7 *The group A_5 is simple.*

Proof:
Recall: A_5 is the subgroup of S_5 consisting of those permutations which can be written as the product of an even number of transpositions. A group is simple if has no nontrivial normal subgroups. Let $H \triangleleft A_5$.

Case 1. H contains a 3-cycle. First note that the 3-cycles generate A_n. This is because: $(12)(23) = (123)$ and $(123)(234) = (12)(34)$. These equations show that for

any pair of transpositions if they overlap their product is a 3-cycle and if they don't overlap, then they can written as a product of 3-cycles. Hence the 3-cycles generate A_n. Next note that since H is a normal subgroup, if it contains one 3-cycle then it contains them all:

Suppose not. If $a \in H$ and $b \notin H$ are 3-cycles (and n-cycles have order n), then we see that 3 divides $|H|$ and since bH has order 3 in $\frac{A_5}{H}$ we see that 3 divides $|\frac{A_5}{H}|$. But by Lagrange' Theorem $|A_5| = |\frac{A_5}{H}|\ |H|$ we would then have that 9 divides $|A_5| = 5 \cdot 4 \cdot 3 = 60$.

Hence H contains all 3-cycles and so $H = A_5$.

Case 2. H contains a 5-cycle. By a similar argument to Case 1, we have that H contains all 5-cycles. But $(12345)(54312) = (132)$ is a 3-cycle in H and so we are done by Case 1.

Case 3. H contains a product of two disjoint transposition. For example, suppose $(12)(34) = \alpha \in H$. Let $\beta = (345) \in A_5$. Then by normality of H, $\beta\alpha\beta^{-1} \in H$ and (using that disjoint cycles commute):

$$\beta\alpha\beta^{-1} = (345)(12)(34)(543) = (12)(345)(34)(543) = (12)(35)$$

But the product of α and $\beta\alpha\beta^{-1}$ is in H and

$$\alpha(\beta\alpha\beta^{-1}) = (12)(34)(12)(35) = (34)(35) = (543)$$

and so we are done by Case 1.

Every permutation in S_5 can be written as a product of disjoint cycles, e.g.,

$$(12) \qquad (123) \qquad (1234) \qquad (12345) \qquad (12)(34) \qquad (123)(45)$$

The cycle structures of the elements of A_5 are exactly covered by the 3 cases.
:foorP

Corollary 5.8 *The group S_5 is not solvable.*

Proof:
A_5 is not solvable since it is not abelian and has no nontrivial normal subgroups. A subgroup of solvable group is solvable (exercise) and hence S_5 is not solvable.
:foorP

Lemma 5.9 *Suppose G is a subgroup of S_5 which contains a transposition and a 5-cycle. Then $G = S_5$.*

Proof:
By automorphing G around we can assume without loss of generality that (12345) and $(1i)$ are elements of G. Again by symmetry it really reduces to cases $(1i) = (12)$ or $(1i) = (13)$. In the first case by using the 5-cycle it is clear that any adjacent

transposition $(i\ i+1)$ can be obtained, i.e., rotate around until i on top, switch the top two, then rotate back. But it is easy to see that adjacent transposition generate S_n: visual a stack of plates numbered 1 thru n. Any plate can be brought to the top by adjacent switches of plates. Then any plate below the top can then be brought to the second position, etc. Hence any permutation of the plates can be obtained by repeatedly switching adjacent plates.

In the other case, $(1i) = (13)$, by using the 5-cycle we can obtain (35). But $(13)(35)(13) = (15)$ and (15) is an adjacent transposition.
:foorP

Example 5.10 *There is a polynomial $f \in \mathbb{Q}[x]$ of degree 5 whose splitting field K has $\mathrm{aut}(K|\mathbb{Q})$ isomorphic to S_5, i.e., the Galois group of f is S_5.*

Proof:
Suppose $f(x)$ is irreducible and has exactly three real roots. Then we claim that its Galois group G is S_5. Since the nonreal roots of a real polynomial must occur in complex conjugate pairs, the roots of f must be $\alpha_1, \alpha_2, \alpha_3, \beta, \overline{\beta}$. Conjugation is an automorphism of $\mathbb{C}$ which fixes the α_i and swaps β and $\overline{\beta}$. Hence G contains a transposition. Also since $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$ we know that 5 divides $[K : \mathbb{Q}]$ where K is the splitting field of f. But since $|G| = [K : \mathbb{Q}]$ (Theorem 2.8) we have that 5 divides the order of G. By Cauchy's Theorem G has an element of order 5. The only elements of S_5 of order 5 are 5-cycles, hence by Lemma 5.9 it must be that $G \simeq S_5$.

There are many examples of such polynomials. Let

$$f(x) = x^5 - 80x + 5$$

Then f is irreducible by Eisenstein's criterion with prime 5.

$$f'(x) = 5x^4 - 80$$

has zeros at 2 and -2, $f(-2) > 0$ and $f(2) < 0$. But since f' is positive in the interval $(-\infty, -2)$, its increasing there and so has exactly one real root in this interval. Similarly f' is negative in $(-2, 2)$ so f is decreasing and so has exactly one real root in this interval. Finally f has exactly one real root in the interval $(2, \infty)$.
:foorP

Corollary 5.11 *(Abel) Fifth degree polynomials are not solvable by radicals.*

6 Solvable by real radicals, constructible polygons

Definition 6.1 *A polynomial $f(x) \in \mathbb{Q}[x]$ is solvable by real radicals iff its roots are in the smallest subfield $S \subseteq \mathbb{R}$ which is closed under taking real roots, i.e., if $a \in S$, $a > 0$ and $n \in \mathbb{N}$ then $\sqrt[n]{a} \in S$.*

Lemma 6.2 *Suppose $F \subseteq \mathbb{C}$ is a subfield, p a prime, and $a \in F$. Then $f(x) = x^p - a$ is reducible in F iff it has a root in F.*

Proof:
Suppose $f(x) = x^p - a = g(x)h(x)$ is reducible in F. We must find a root of it in F. So let $\beta \in \mathbb{C}$ be any root of $f(x)$ and let $\alpha = e^{\frac{2\pi i}{p}}$ be the usual primitive pth root of unity. Then we know that the zeros of f are: $\beta, \alpha\beta, \alpha^2\beta, \ldots, \alpha^{p-1}\beta$ and f factors in $\mathbb{C}$ by

$$f(x) = x^p - a = \prod_{i=0}^{p-1}(x - \alpha^i\beta)$$

Now suppose that the degree of $g(x)$ is k with $1 \leq k < p$. If we factored g in $\mathbb{C}$ we would see that it contains k of the factors of f, i.e., there exists a set $A \subseteq \{0, 1, \ldots, p-1\}$ of size k such that

$$g(x) = \prod_{i \in A}(x - \alpha^i\beta)$$

Suppose $b \in F$ is the constant term of g. We will show how to use b and a to construct a root of f. First note that $b = (-1)^k\alpha^l\beta^k$ for some l. Let $c = \alpha^l\beta^k$ and notice that $c^p = (\beta^p)^k = a^k$ since $\alpha^p = 1$. Now since p is prime and $1 \leq k < p$ we have that there exists $s, t \in \mathbb{Z}$ with $sk + tp = 1$. It follows that

$$a^1 = a^{sk+tp} = ((a^k)^s)((a^t)^p) = ((c^p)^s)((a^t)^p) = (c^s a^t)^p$$

Hence $(c^s a^t) \in F$ is a root of f.
:foorP

Theorem 6.3 *Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible cubic with three real roots. Then $f(x)$ is not solvable by real radicals.*

Proof:
For contradiction suppose $K \subseteq S$ is the splitting field of $f(x)$.

Claim. There exists a subfield F_0 such that $\mathbb{Q} \subseteq F_0 \subseteq K$ and $[K : F_0] = 3$.

Note that the Galois group of f is a subgroup of the group S_3 of permutations of its three roots. Since f is irreducible we have that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ where α is any of the three roots of f. So if $K = \mathbb{Q}(\alpha)$ we can take $F_0 = \mathbb{Q}$. Otherwise the Galois group of f is S_3. Let $H \subseteq S_3$ be any (the) subgroup of S_3 with $|H| = 3$. Then the fixed field:

$$F_0 = \text{fix}(H) = \{x \in K : \forall \sigma \in H \;\; \sigma(x) = x\}$$

has the property desired, i.e., $[K : F_0] = |\text{aut}(K|F_0)| = |H| = 3$ by Theorems 2.8 and 3.7. This proves the Claim.

Note: f is irreducible over F_0. This is because $[F_0 : \mathbb{Q}]$ is either 1 or 2 but f is an irreducible cubic, so if α any root of f we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Note: If $F_0 \subseteq F$ then either f is irreducible over F or f splits in F. This is because $[K : F_0] = 3$ and hence for any root α of f we have that $F_0[\alpha] = K$. Hence if one root exists in F then all roots are in F.

Note: S is the smallest subfield of $\mathbb{R}$ closed under taking real roots of prime degree. This is because, for example, the sixth root is the square root of the cube root, etc.

Therefore, it follows that if $K \subseteq S$ there must be some subfield $F \subseteq S$ with $F_0 \subseteq F \subseteq S$, $a \in F$ and p prime such that f is irreducible over F but f is reducible over $F(\sqrt[p]{a})$. By the Lemma we have that $x^p - a$ is irreducible over F and so $[F(\sqrt[p]{a}) : F] = p$. We also know that for any root α of f that $[F(\alpha) : F] = 3$ and since $F \subseteq F(\alpha) \subseteq [F[\sqrt[p]{a}]$ we have that 3 divides p. Since p was prime we must have that $p = 3$ and therefore $F(\alpha) = F(\sqrt[3]{a})$. Since adding one root of f adds all roots of f we know that $F(\sqrt[3]{a})$ is the splitting field of f over F. But this contradicts Theorem 3.1 which says that for a Galois extension an irreducible which has a root splits. But the irreducible polynomial $x^3 - a$ has only one root in $F(\sqrt[3]{a})$, the other two roots are not real.
:foorP

Theorem 6.4 *(Gauss) Let p be a prime. Then the regular p-gon is constructible with straight edge and compass iff p is a Fermat prime, i.e., $p = 2^{2^n} + 1$ for some n.*

Proof:
See Chapter 33.
:foorP