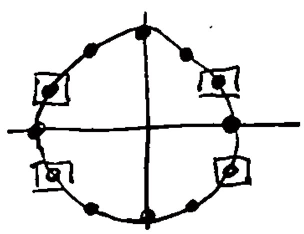
3/10 Cyclotomic Extensions §5.8

Our goal now is to study finite extensions of $\mathbb{Q}$ of specific forms, leading up to a treatment of the problem which motivated the development of Galois theory: the solvability of polynomials by radicals.

<u>Def'n</u> Recall that a number $u \in \mathbb{C}$ is called an <u>n^{th} root of unity</u>, for some $n \geq 1$, if $u^n = 1$, i.e., if u is a root of $x^n - 1 \in \mathbb{Q}[x]$. If u is an n^{th} root of unity, it is also a $(mn)^{th}$ root of unity for any $m \geq 1$. We say u is a <u>primitive n^{th} root of unity</u> if it is an n^{th} root of unity but not a k^{th} root of unity for any $k < n$.

<u>Prop</u>. The n^{th} roots of unity are $e^{\frac{2\pi i}{n} \cdot j}$ for $j = 0, 1, \ldots, n-1$. The primitive n^{th} roots of unity are those $e^{\frac{2\pi i}{n} \cdot j}$ with $\gcd(j, n) = 1$.

<u>E.g.</u> We've seen before how the n^{th} roots of unity are equally spaced on the unit circle, for instance for $n = 12$ we get



$\Leftarrow$ the primitive 12^{th} roots of unity are circled: they are $e^{\frac{2\pi i}{12} \cdot j}$ for $j = 1, 5, 7, 11$, the integers coprime to 12.

<u>Pf sketch of prop</u>: That the $e^{\frac{2\pi i}{n} j}$ for $j = 0, 1, 2, \ldots, n-1$ are the n^{th} roots of unity follows from the fact that

$e^{\frac{2\pi i}{n} \cdot j} \cdot e^{\frac{2\pi i}{n} \cdot k} = e^{\frac{2\pi i}{n} (j + k \bmod n)}$ (phases of complex #'s add when multiplied).

That the primitive ones are the coprime j's then follow from $e^{\frac{2\pi i}{n} \cdot j}$ is a primitive n^{th} root of unity $\Leftrightarrow$
j is a generator of $(\mathbb{Z}/n\mathbb{Z}, +)$ $\Leftrightarrow$
j is a unit in the ring $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$
j is coprime to n. You will flesh out this argument on your next HW assignment. $\blacksquare$

Notice: $\zeta_n = e^{\frac{2\pi i}{n}}$ is always a primitive n^{th} root of unity, and all n^{th} roots of unity are powers of this ζ_n.

Def'n Let $n \geq 1$. The n^{th} cyclotomic polynomial $\Phi_n(x) \in \mathbb{C}[x]$ is $\Phi_n(x) = \prod_{\omega \text{ a primitive } n^{\text{th}} \text{ root of unity}} (x - \omega)$. (The book uses $g_n(x)$.)

E.g. The primitive 3^{rd} roots of unity are $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$; so $\Phi_3(x) = (x-\omega)(x-\omega^2) = x^2 + x + 1$.

In fact, the first 6 cyclotomic polynomials are:

$\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$, $\Phi_3(x) = x^2+x+1$, $\Phi_4(x) = x^2+1$

$\Phi_5(x) = x^4+x^3+x^2+x+1$, $\Phi_6(x) = x^2 - x + 1$.

Thm $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.

Pf: Every root of $x^n - 1$ is an n^{th} root of unity, which is a primitive d^{th} root of unity for some $d \mid n$. $\boxtimes$

Note: Even though $\Phi_d(n)$ is a priori defined as an element of $\mathbb{C}[x]$, looks like it belongs to $\mathbb{Q}[x]$. This is true and we'll prove it! In fact the coefficients are integers, which can get arbitrarily big, but take a while ($\Phi_{105}(x)$ is first with a coeff. not in $\{1,-1\}$).

The way we will show cyclotomic polynomials are rational is by studying the extensions of $\mathbb{Q}$ we get by adjoining their roots.

Def'n The n^{th} cyclotomic extension of $\mathbb{Q}$ is the splitting field of $x^n - 1$. Equivalently, ...

Thm The n^{th} cyclotomic extension is $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity.

Pf: Since ζ_n is an n^{th} root of unity, it belongs to splitting field of $x^n - 1$. But on other hand, every root of unity is a power of ζ_n, hence in $\mathbb{Q}(\zeta_n)$. ☒

Thm Let $\varphi_k : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ be defined by $\varphi_k(\zeta_n) = \zeta_n^k$.
Then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \subseteq \{\varphi_k : 1 \le k \le n,\ \gcd(n,k) = 1\}$.

Pf: Any $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ is determined by where it sends ζ_n, which must be to some ζ_n^k since these are roots of $x^n - 1$. But it cannot be sent to a non-primitive n^{th} root of unity, since it's not a root of any $x^m - 1$ with $m < n$ ☒

Cor The cyclotomic polynomial $\Phi_n(x) \in \mathbb{Q}[x]$.

Pf: $\mathbb{Q}(\zeta_n)$ is a Galois extension, since it's a splitting field, and every $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ fixes $\Phi_n(x)$ since just permutes roots, so in fact coefficients of $\Phi_n(x)$ are rational. ☒

Thm (Gauss) $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

Pf: This is non-trivial but I skip it - see the book. ☒

Cor $\Phi_n(x)$ is the minimal polynomial of ζ_n, and every φ_k for $\gcd(n,k)$ is indeed an element of $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$.
Hence $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group mod n, via the isomorphism $\varphi_k \mapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Remark: This shows $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group of order $\varphi(n)$ where $\varphi(n) = \#\{1 \le k \le n : \gcd(n,k) = 1\}$ is Euler's totient function. When $n = p$ is prime we have seen that $(\mathbb{Z}/p\mathbb{Z})^\times$ is in fact cyclic (of order $p-1$), but in general it need not be: e.g. $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

//

3/12

Cyclic Extensions §5.7

We are almost ready to study the solvability of polynomials by radicals. We just need one more preparatory result...

Def'n An algebraic, Galois extension L/K is called abelian if $Aut_K(L)$ is abelian, it is called cyclic if $Aut_K(L)$ is cyclic, and it is called cyclic of degree n if $Aut_K(L)$ is $\mathbb{Z}/n\mathbb{Z}$.

Remark: We have seen that the cyclotomic extension $\mathbb{Q}(\xi_n)$ of $\mathbb{Q}$ is always abelian, and sometimes cyclic (e.g. if n is prime) although not always.

In general it is hard to classify cyclic extensions, but there is a nice situation where we can do this.

Def'n For an arbitrary field K, $u \in K$ is called an n^{th} root of unity if $u^n = 1 \in K$, and is called a primitive nth root of unity if $u^0, u^1, \ldots, u^{n-1}$ are all distinct (hence are all the n^{th} roots of unity). For subfields of $\mathbb{C}$, this agrees with our previous definition...

Thm Let K be a field containing a primitive n^{th} root of unity ξ_n for some $n \geq 1$. Then the following are equivalent for L/K:

1) L/K is cyclic of degree d, for some $d \mid n$.
2) L/K is the splitting field of a polynomial of form $f(x) = x^n - a \in K[x]$, in which case $L = K(u)$ for u a root of $f(x)$.
3) L/K is splitting field of irreducible polynomial of form $f(x) = x^d - a$ for some $d \mid n$, in which case $L = K(u)$ for u root of $f(x)$.

E.g. Any degree 2 extension of $\mathbb{Q}$ is the splitting field of a polynomial of the form $x^2 - d$ where d is not a square in $\mathbb{Q}$, and this extension has Galois group $\mathbb{Z}/2\mathbb{Z}$.

prim. 3rd root of unity

E.g.: On a previous homework you showed that if $L = \mathbb{Q}(\omega, \sqrt[3]{2})$ is the splitting field of $x^3 - 2$ over $K = \mathbb{Q}$, then $\mathrm{Aut}_K(L) \simeq S_3$, which is not cyclic (not even abelian!). But $\mathbb{Q}$ does not have a prim. 3rd root of unity! If we instead take $K = \mathbb{Q}(\omega)$, then $\mathrm{Aut}_K(L) = \mathbb{Z}/3\mathbb{Z}$.

In the theorem, 2) and 3) are easily seen to be equivalent, just having to do with whether $x^n - a$ is irreducible, equivalently whether a has a d^{th} root in K for some $d \mid n$. The main point is showing 3) $\Leftrightarrow$ 1). In fact we will mostly care about 3) $\Rightarrow$ 1), which we will prove now: we just need:

Lemma If K is a field with a primitive n^{th} root of unity ξ, then for any $d \mid n$, $\eta = \xi^{n/d}$ is a primitive d^{th} root of 1. And if L is an extension of K such that $u \in L$ is a root of $x^d - a \in K[x]$, then all the roots of $x^d - a$ are $u, \eta u, \eta^2 u, \dots, \eta^{d-1} u$ (all distinct).

Pf: Straightforward exercise. $\square$

Pf of 3) $\Rightarrow$ 1) in thm: By the lemma, the roots of $x^d - a$ in L are $u, \eta u, \dots, \eta^{d-1} u$ where u is any root and $\eta = \xi^{n/d}$ as above. So any $\sigma \in \mathrm{Aut}_K(L)$ is determined by where it sends u (since $\eta \in K$ is fixed by σ). Since $x^d - a$ is irreducible, there must be some σ with $\sigma(u) = \eta u$, and this σ generates all of $\mathrm{Aut}_K(L)$ since $\sigma^k(u) = \eta^k u$, which give all the possible automorphisms in the Galois group by the previous sentence. $\square$

We will only sketch the ideas that go into the pf of 1) $\Rightarrow$ 3):

<u>Def'n</u> Let L/K be a finite Galois extension, and suppose that $\mathrm{Aut}_K(L) = \{\sigma_1, \dots, \sigma_n\}$. For any $u \in L$, the <u>norm</u> of u is $N(u) = \sigma_1(u)\cdot\sigma_2(u)\cdot \cdots \cdot \sigma_n(u)$.

<u>Eg.</u> Let $K = \mathbb{R}$ and $L = \mathbb{C}$. Recall that $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1, \sigma\}$ where $\sigma: z \mapsto \bar{z}$ is <u>complex</u> <u>conjugation</u>. So the <u>norm</u> of $z = a+bi \in \mathbb{C}$ is $N(z) = z\cdot\bar{z} = a^2+b^2$, usual complex norm.

<u>E.g.</u> For $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, the same is true: the norm of $a+bi$ is $(a+bi)(a-bi) = a^2+b^2 \in \mathbb{Q}$.

<u>Prop.</u> If L/K is a finite Galois extension, then the norm $N(u)$ of any $u \in L$ is an element of the base field K.

<u>Pf:</u> For any $\sigma \in \mathrm{Aut}_K(L)$, $\sigma(N(u)) = \sigma\sigma_1(u)\cdot\sigma\sigma_2(u)\cdots\sigma\sigma_n(u)$
$= \sigma_{i_1}(u)\cdot \cdots \sigma_{i_n}(u) = N(u)$
(where $i_1, \dots, i_n$ is some permutation of $1, \dots, n$), so because L/K is Galois, $N(u) \in K$ as claimed. ☒

<u>Remark:</u> We can define the norm for non-Galois extensions too, and it remains true that it belongs to the ground field, but it's a little more technical.

Another important property of the norm is multiplicativity:

<u>Prop.</u> We have $N(u)\cdot N(v) = N(uv)$ for $u, v \in L$.

<u>Pf:</u> Straightforward exercise. ☒

The norm is particularly useful for cyclic extensions...

Thm (Hilbert Theorem 90) Let L/K be a finite cyclic (Galois) extension and let $\sigma \in \mathrm{Aut}_K(L)$ be a generator of the Galois group. Then for $u \in L$, $N(u)=1 \iff u = v/\sigma(v)$ for some $v \in L$.

Pf: One direction is easy: if $u = \frac{v}{\sigma(v)}$ then $N(u) = \frac{\sigma_1(v)\cdots\sigma_n(v)}{\sigma_{i_1}(v)\cdots\sigma_{i_n}(v)} = 1$

The other direction is nontrivial - see the book for a proof! ☒

E.g. Consider $L = \mathbb{Q}(i)$ over $K=\mathbb{Q}$. The elements in $\mathbb{Q}(i)$ of norm 1 are $\frac{p}{r} + \frac{q}{r} i$ with $\frac{p^2}{r^2} + \frac{q^2}{r^2} = 1$, i.e., $p^2+q^2=r^2$, $p,q,r \in \mathbb{Z}$. These are Pythagorean triples. Hilbert's Thm 90 says they can all be written in form $\frac{a+bi}{a-bi} = \frac{a^2-b^2}{a^2+b^2} + \frac{2ab}{a^2+b^2} i$, $a,b \in \mathbb{Z}$

It is a classic fact going back to Euclid that (primitive) Pythagorean triples can be parameterized in this way.

With Hilbert's thm 90 we can complete the pf of main thm:

Pf of 1) $\Rightarrow$ 3): Let $\sigma \in \mathrm{Aut}_K(L)$ be a generator, and let $\eta = \zeta^{n/d}$ be a primitive dth root of unity. Then $N(\eta) = \eta \cdot \sigma(\eta) \cdots \sigma^{d-1}(\eta) = \underbrace{\eta^d}_{=1}$ (since $\eta \in K$) so by Hilbert 90 we can write $\eta = v/\sigma(v)$ for some $v \in L$. Notice $\sigma(v^d) = (\sigma(v))^d = \left(\frac{v}{\eta}\right)^d = \frac{v^d}{\eta^d} = v^d$ (since $\eta^d = 1$), so because the extension L/K is Galois, this means that $v^d \in K$. Then v is a root of the polynomial $x^d - v^d \in K[x]$, and it can be shown that this polynomial is in fact irreducible over K and that $L = K(v)$ is the splitting field.

☒

3/17 **Radical Extensions & Solving Polynomials** §5.9

We come now to one of the major achievements of Galois theory: a precise understanding of when polynomial equations can be solved by expressions using radicals. The famous quadratic formula $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ says that the roots of any quadratic ax^2+bx+c can be expressed in terms of the coefficients using the basic field operations $(+,-,*,\%)$ together with the square root $\sqrt{\ }$. Similarly, you saw on HW #4 how for any cubic equation $ax^3+bx^2+cx+d=0$, we can express the solutions in terms of the coefficients using field operations together with square roots and cube roots. In fact, there is also a "quartic formula" expressing the solutions to a degree 4 equation in terms of radicals (i.e., n^{th} roots $\sqrt[n]{\ }$), but the pattern stops there: as we will see, there is no general "quintic formula."

Def'n Let K be a field. We say a finite (hence, algebraic) extension $L = K(u_1, u_2, \ldots, u_n)$ of K is a radical extension if for each $i = 1, \ldots, n$, there is an $m \geq 1$ such that $u_i^m \in K(u_1, \ldots, u_{i-1})$, i.e. u_i is an "m^{th} root" of an element in $K(u_1, \ldots, u_{i-1})$

Def'n Let $f(x) \in K[x]$ be a polynomial. We say that $f(x)$ is solvable by radicals if the splitting field of $f(x)$ is a subfield of some radical extension of K.

This captures the notion of the roots of $f(x)$ being expressible from K using the field operations & radicals.

Not only will we show that there is no general formula for equations of degree $n \geq 5$ (using radicals), we will show that, for all degrees $n \geq 5$, there are specific polynomials $f(x) \in \mathbb{Q}[x]$ for which $f(x)$ is not solvable by radicals.

Remark: Notice that we take $K = \mathbb{Q}$ here. If we took, e.g., $K = \mathbb{C}$, then every $f(x) \in \mathbb{C}[x]$ is "solvable by radicals" for the trivial reason that the roots of $f(x)$ belong to the base field $\mathbb{C}$.

The key to showing that some polynomials are not solvable by radicals is to show that the Galois groups of polynomials that are solvable by radicals have a restricted form. So we need to recall some notions from group theory.

Def'n Let G be a group. For $x, y \in G$, $[x,y] = xyx^{-1}y^{-1}$ is the commutator of x and y (measures extent to which x and y fail to commute) and for $H_1, H_2 \leq G$ we use $[H_1, H_2] = \langle [x,y] : x \in H_1, y \in H_2 \rangle$. The derived subgroup of G is $G' = [G,G]$, it is $= \{e\}$ exactly when G is abelian. We say that G is solvable if the derived series $G^{(0)} = G$, $G^{(i)} = (G^{(i-1)})'$ eventually reaches the trivial subgroup:

$$\{e\} = G^{(k)} \trianglelefteq G^{(k-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

(That G' is normal in G is an easy exercise.)

Recall by comparison that G is nilpotent if its lower central series $G^0 = G$, $G^i = [G, G^{i-1}]$ eventually reaches the trivial subgroup:

$$\{e\} = G^k \trianglelefteq G^{k-1} \trianglelefteq \cdots \trianglelefteq G^1 \trianglelefteq G^0 = G.$$

Every abelian group is nilpotent, and every nilpotent group is solvable (but not conversely).

E.g. The dihedral group D_4 of order 8 is nilpotent but not abelian. The symmetric group S_3 on 3 letters is soluble but not nilpotent. The alternating group A_5 of order 60 is not solvable, since it is simple and non-abelian.

Prop. If G is solvable and $H \subseteq G$ then H is solvable.
Pf: Derived series of H is "smaller" than that of G. ∎

E.g. For any $n \geq 5$, the symmetric group S_n is not solvable, since A_n, a simple nonabelian group, is not solvable.

Thm A group G is solvable if and only if it has a subnormal series $\{e\} = G_k \triangleleft G_{k-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ such that the factor groups G_i / G_{i+1} are all abelian.

Pf: The derived series of a solvable group is such a series, since G/G' is always abelian. We proved the other direction last semester when discussing composition series and the Jordan-Hölder Theorem. ∎

Explaining the name "Solvable", we have the following main result:

Thm A polynomial $f(x) \in K[x]$ is solvable by radicals only if its Galois group, i.e. the group $\mathrm{Aut}_K(L)$ where L is its splitting field, is a solvable group.

A "generic" polynomial $f(x) \in \mathbb{Q}[x]$ of degree n has S_n as its Galois group, hence by the previous theorem it does not have a solution in radicals for $n \geq 5$ (this is the "Abel-Ruffini Theorem").

3/19

We have already seen the main ideas that go into the proof of this theorem, which are:

- cyclotomic extensions are abelian,
- If F contains a primitive n^{th} root of unity and $E = F(u)$ where $u^d \in F$ for some $d|n$, then E is an abelian (cyclic!) extension.

In fact, we will focus on the case $K = \mathbb{Q}$ for this theorem, which is the one of most interest. And as we'll explain, when $K = \mathbb{Q}$, the "only if" becomes an "if and only if".

<u>Lemma</u> If $L = K(u_1, \ldots, u_n)$ is a radical extension of K, then there is a finite, <u>normal</u> extension M of K with $K \subseteq L \subseteq M$ such that M is also a radical extension of K.

<u>Pf sketch</u>: Recall that normal means that when the extension has one root of an irreducible polynomial, it has all of them. So to build a normal, radical extension containing L, whenever we adjoin u_i satisfying $u_i^{m_i} \in L(u_1, \ldots, u_{i-1})$, we also adjoin all other roots of its minimal polynomial. Any other such root v will also have $v^{m_i} \in L(u_1, \ldots, u_{i-1})$ (since it must satisfy same poly's as u_i), and hence the extension will stay radical. $\boxtimes$

We now prove the main theorem about solvable $f(x)$ and solvable Galois groups, in the case $K = \mathbb{Q}$.

<u>Pf of main thm</u>: Let $f(x) \in \mathbb{Q}[x]$ be solvable by radicals. Hence there is a radical extension $L = \mathbb{Q}(u_1, \ldots, u_n)$ such that the splitting field of $f(x)$ is contained in L. Our goal is to show that the Galois group of the splitting field is solvable. By the preceding lemma, we may assume that L itself is a normal, hence Galois, ext. of $\mathbb{Q}$. Then by the Fund. Thm., the Galois gp. of the splitting field is a quotient of $Aut_{\mathbb{Q}}(L)$. Since solvability of groups is preserved by quotients, it is enough to show that $Aut_{\mathbb{Q}}(L)$ is solvable.

Let $m_1, \dots, m_n$ be such that $u_i^{m_i} \in \mathbb{Q}(u_1, \dots, u_{i-1})$ for all i. Let $m = m_1 \cdot m_2 \cdots m_n$. The trick is to first adjoin a primitive m^{th} root of unity, so that then all the extensions we do by adjoining m_i^{th} roots will be cyclic. Thus, letting $\xi = \xi_m = e^{2\pi i/m}$ be a prim. m^{th} root of 1, consider:

$$\begin{array}{ccccc} & & M = L(\xi) = \mathbb{Q}(\xi, u_1, \dots, u_n) & & \\ & \mathbb{Q}(\xi) & & L = \mathbb{Q}(u_1, \dots, u_n) & \\ & & \mathbb{Q} & & \end{array}$$

Cyclotomic extensions are Galois, so all these extensions are Galois. Thus $Aut_{\mathbb{Q}}(L) \cong Aut_{\mathbb{Q}}(M)/Aut_L(M)$ and $Aut_{\mathbb{Q}}(\mathbb{Q}(\xi)) \cong Aut_{\mathbb{Q}}(M)/Aut_{\mathbb{Q}(\xi)}(M)$. Since solvability is preserved by subgroups, quotients, and extensions by abelian groups (recall: $Aut_{\mathbb{Q}}(\mathbb{Q}(\xi))$ is abelian), it suffices to show $Aut_{\mathbb{Q}(\xi)}(M)$ is solvable.

So now we prove $G = Aut_{\mathbb{Q}(\xi)}(M)$ is solvable. Thus consider:

$$\begin{array}{ccc} M = M_n = \mathbb{Q}(\xi, u_1, \dots, u_n) & - & G_n = Aut_{M_n}(M) = \{e\} \\ \vdots \cup\!| & & \vdots \trianglelefteq \\ M_1 = \mathbb{Q}(\xi, u_1) & - & G_1 = Aut_{M_1}(M) \\ \cup\!| & & \trianglelefteq \\ M_0 = \mathbb{Q}(\xi) & - & G_0 = Aut_{M_0}(M) = G \end{array}$$

i.e., $M_i = \mathbb{Q}(\xi, u_1, \dots, u_i)$ and $G_i = Aut_{M_i}(M)$ for $i = 0, 1, \dots, n$. From our analysis of cyclic extensions, it follows that M_i, which is obtained from M_{i-1} by adjoining an m_i^{th} root, is a Galois extension and has $Aut_{M_{i-1}}(M_i)$ cyclic. Hence by the Fund. Thm., $G_{i-1} \trianglelefteq G_i$ is normal and we have $G_i / G_{i-1} \cong Aut_{M_{i-1}}(M_i)$ is cyclic. So then

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G \quad \text{is}$$

a subnormal series with abelian factor groups, proving G is solvable! ☒

Remark: As mentioned, over $K=\mathbb{Q}$ the main thm has a converse: if the splitting field of $f(x) \in \mathbb{Q}[x]$ has solvable Galois group, then $f(x)$ is solvable by radicals. The proof of the converse follows a similar strategy. We need to use the fact that if G is solvable, then it has a subnormal series (composition series) $G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ where the factor groups are all cyclic. And we also need to use the fact that, in the presence of sufficient roots of unity, cyclic extensions correspond to adjoining roots of $x^m - a$, i.e., m^{th} roots (recall: Hilbert's Thm 90).

There are algorithms for computing the Galois group of a polynomial $f(x) \in \mathbb{Q}[x]$, hence by the above theorem (and its converse) for deciding if a polynomial has roots that are expressible in terms of radicals.

The theorem shows not only that there is no general formula for solving polynomial equations of degree $n \geq 5$ (in radicals), i.e., the "Abel-Ruffini Theorem," it also leads to specific polynomials whose roots cannot be so expressed.

E.g. The polynomial $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ has Galois group the full symmetric group S_5 (exercise), which is not solvable, and so its roots are not expressible in radicals.

Galois theory gives us a very satisfying account of this classical problem of finding formulas for solving polynomial equations! //

3/26

Transcendental extensions & transcendence bases §6.1

We have so far focused almost entirely on algebraic extensions of fields (in fact, usually finite extensions). In this last lecture we will discuss transcendental extensions. We will see that every extension can be realized as a combination of an algebraic extension and a "purely transcendental" extension. Let's recall some terminology:

Def'n Let L/K be an extension. We say $u \in L$ is algebraic over K if $\exists f(x) \in K[x]$, $f \neq 0$ such that $f(u) = 0$, and say u is transcendental otherwise. We say L/K is algebraic if every $u \in L$ is algebraic over K, and say L/K is transcendental otherwise.

Remark: Recall that every simple, transcendental extension of K is isomorphic to $K(x)$, field of rational functions, which in particular has infinite degree.

Remark: It follows from the previous remark that every finite extension is algebraic, but there are also infinite algebraic extensions. E.g., with $K = \mathbb{Q}$ and $L = \overline{K} = \mathbb{Q}^{alg}$ (field of algebraic numbers) L/K has infinite degree since $\{\sqrt{p} : p \text{ prime}\} = \{\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots\} \subseteq L$ is an infinite, K-linearly independent subset.

In order to understand "how transcendental" an extension L/K is, we need the notion of algebraic independence:

Def'n Let L/K be an extension and $S \subseteq L$ a subset of elements. We say S is algebraically dependent over K if there is $n \geq 1$ and $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, $f \neq 0$, such that $f(s_1, \ldots, s_n) = 0$ for some distinct elements $s_1, \ldots, s_n \in S$. Otherwise we say S is algebraically independent over K.

E.g. $\{u\} \subseteq L$ is algebraically independent $\Leftrightarrow$ u is transcendental.
So $\{\pi\}$ is algebraically independent over $\mathbb{Q}$, but $\{\pi, \pi^2\}$ is algebraically dependent, since with $f(x,y) = x^2 - y$ we have $f(\pi, \pi^2) = \pi^2 - \pi^2 = 0$.

E.g. It is a big open problem in number theory to show that $\{\pi, e\}$ is algebraically independent over $\mathbb{Q}$ (though of course both π and e are known to be transcendental).

Def'n Let L/K be an extension. We say $S \subseteq L$ is a transcendence basis for L over K if it is algebraically independent over K and is maximal (w.r.t. inclusion) among alg. ind. subsets.

E.g. $\{x\}$ is a transcendence basis for $k(x)$ over k. (exercise)
But notice that $\{x\}$ is not a k-linear basis of $k(x)$; recall that $[k(x):k] = \infty$ (e.g. $\{1, x, x^2, \dots\}$ is lin. ind.).

Prop. If S is a transcendence basis of L over K, and $u \in L$, then u is algebraic over $K(S)$.
Pf: Since the claim is trivial if $u \in S$, suppose $u \notin S$. Then since $S \cup \{u\}$ is algebraically dependent over K, there is $f(x_1, \dots, x_n, y) \in K[x_1, \dots, x_n, y]$ with $f(s_1, \dots, s_n, u) = 0$ but $f \neq 0$ for some $s_1, \dots, s_n \in S$.
Thus u is a root of $f(s_1, \dots, s_n, y) \in K(S)[y]$. $\square$

Cor An algebraically independent subset $S \subseteq L$ is a transcendence basis if and only if L is algebraic over $K(S)$. $\square$
Pf: straightforward from above, exercise.

Remark: An application of "Zorn's lemma" (which relies on the axiom of choice) shows that any algebraically independent subset S can be extended to a transcendence basis. In particular, transcendence bases always exist!

Def'n An extension L/K is called <u>purely</u> <u>transcendental</u> if $L = K(S)$ for $S \subseteq L$ an algebraically independent subset (which then must be a transcendence basis of L).

<u>E.g.</u> $K(x)$ is a purely transcendental extension of K. More generally, for any $n \geq 1$, $K(x_1, \ldots, x_n)$, the field of multivariable rational functions in variables $x_1, \ldots, x_n$ with coefficients in K, is a purely transcendental extension, since $\{x_1, \ldots, x_n\}$ is a trans. basis (<u>exercise</u>).

<u>E.g.</u> $\mathbb{R}$ is a transcendental extension of $\mathbb{Q}$, since it contains e.g. π which is transcendental over $\mathbb{Q}$, but it is <u>not</u> a purely transcendental extension because it also contains e.g. $\sqrt{2}$ which is algebraic over $\mathbb{Q}$ but not an element of $\mathbb{Q}$.

<u>Remark</u>: If L/K is any extension and $S \subseteq L$ is a trans. basis, then $K(S)/K$ is a purely transcendental extension and $L/K(S)$ is an algebraic extension, so every extension is a "combination" of a purely trans. ext. and ~~and~~ algebraic ext.

Basic linear algebra tells us that any basis of a vector space V over a field K has the same size as any other. The same is true for transcendence bases (leading to a notion of dimension):

<u>Thm</u> Let S and T be two transcendence bases of L/K. Then S and T have the same cardinality.

We will only prove this theorem in the case when the cardinality is finite ("finite transcendence degree"), because the infinite cardinality case requires a little more advanced set theory.

Pf: Suppose that $S = \{s_1, s_2, \dots, s_n\}$. We claim some $t_1 \in T$ is transcendental over $K(s_2,\dots,s_n)$. Otherwise $K(s_2,\dots,s_n)(T)$ would be algebraic over $K(s_2,\dots,s_n)$, and since L is algebraic over $K(T)$, this would mean that L would be algebraic over $K(s_2,\dots,s_n)$ (composition of algebraic ext.'s is algebraic). But of course s_1 cannot be algebraic over $K(s_2,\dots,s_n)$ because S is a trans. basis, in particular algebraically independent.

So indeed $\{t_1, s_2, \dots, s_n\}$ is algebraically independent. If s_1 were transcendental over $K(t_1, s_2, \dots, s_n)$, then $\{t_1, s_1, s_2, \dots, s_n\} = S \cup \{t_1\}$ would be algebraically independent, contradicting that S is a trans. basis, i.e. maximal alg. independent set (assuming $t_1 \neq s_1$). So we conclude that $\{t_1, s_2, \dots, s_n\}$ is a trans. basis of L/K.

Repeating this argument, we can find $t_2 \in T \setminus \{t_1\}$ such that $\{t_1, t_2, s_3, \dots, s_n\}$ is a trans. basis, and so on until we conclude that $\{t_1, t_2, \dots, t_n\} \subseteq T$ is a trans. basis. But then we must have $T = \{t_1, t_2, \dots, t_n\}$ because T is a trans. basis. So indeed $\# S = \# T$ as claimed. $\boxtimes$

Def'n For L/K, we define the transcendence degree of L/K, denoted tr. deg.(L/K), to be the cardinality of any transcendence basis of L over K.

E.g. L/K is algebraic $\Leftrightarrow$ tr. deg.$(L/K) = 0$.

E.g. tr. deg.$(K(x_1,\dots,x_n)/K) = n$. More generally, any purely transcendental ext. of K of trans. deg. $= n$ is isomorphic to $K(x_1,\dots,x_n)$.

E.g. On the last HW you will show that tr. deg.$(\mathbb{C}/\mathbb{Q}) = \infty$, and tr. deg.$(\mathbb{R}/\mathbb{Q}) = \infty$ as well.

//