$F \to E$, to get n homomorphism $\hat{\varphi} : E \to E$ that fix the elements of F. Each of these is injective, and F-linear. Since E is finite dimensional over F, each $\hat{\varphi}$ is a bijection, hence an element of $\mathrm{Aut}_F(E)$. In other words, we have $\mathrm{Aut}_F(E) \geq [E : F]$. From Proposition 7.4.1.2 we have $\mathrm{Aut}_F(E) \leq [E : F]$, so we get the desired equality. ■

Given a field tower $E/L/F$, some properties of the big extension E/F imply the same properties for the two step extensions, E/L and L/F. That is the case for the properties: 04/15/19

Finite See Corollary 6.4.4, the Multiplicative Property of Extension Degrees.

Algebraic See Corollary 6.4.10.

Separable See Proposition 7.2.5.

However, this is not the case for normal extensions. For example, in the tower $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, the big extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal, the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. However, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal (see Example 7.4.2.1).

We do get, however, the following lemma, whose proof is immediate.

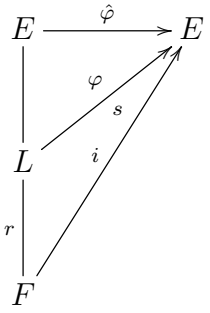
Lemma 7.4.7 *Let $E/L/F$ be a field tower. If E/F is normal, then E/L is normal.*

Combining this lemma with Proposition 7.2.5 and Proposition 7.4.3.4, we get:

Proposition 7.4.8 *Let $E/L/F$ be a field tower. If E/F is a Galois extension, then E/L is also Galois.*

For a finite extension E/F, the property of being Galois has some important consequences that make them nice and convenient to work with. The main of those properties is the Fundamental Theorem of Galois Theory, coming up in the next section. Here is another nice property of Galois extensions.

Proposition 7.4.9 *Let E/F be a finite Galois extension. If $p(x) \in F[x]$ is irreducible and has a root in E, then it splits in E, and is separable.*



Proof. By Proposition 7.4.3, E is the splitting field of a separable polynomial $f(x) \in F[x]$. Let $u \in E$ be a root of $p(x)$, and let $L = F(u)$. Let $r = \deg(p(x))$. By Scholium 7.1.8, the number of ways of extensing the inclusion map $i : F \to E$ to a homomorphism $\varphi : F(u) \to E$ is the number s of distinct roots of $p(x)$ in E, and each of these φ fixes the coefficients of $f(x)$. Applying Lemma 7.4.6, to the extension E/F and map i, and to the extension E/L and each of the maps φ, we get:

- there are $[E : L]$ ways to extend each $\varphi : L \to E$ to a homomorphism $\hat{\varphi} : E \to E$.
- there are $[E : F]$ ways of extending the inclusion map to a homomorphism $\hat{\varphi} : E \to E$.

Thus, we have

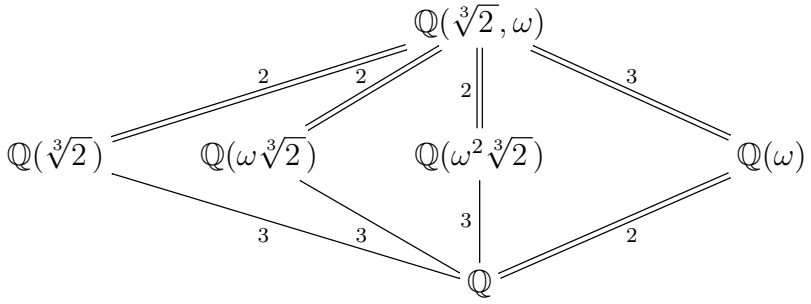
$$[E : F] = s \cdot [E : L] \leq r \cdot [E : L] = [L : F] \cdot [E : L] = [E : F]$$

and therefore $s = r$, i.e. $p(x)$ has r distinct roots in E. It splits in E, and is separable. ■

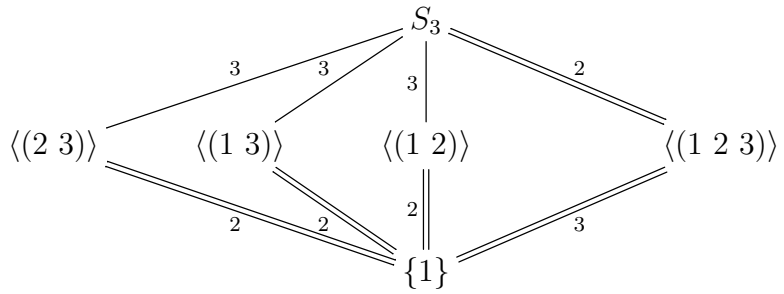
7.4.3 The Fundamental Theorem

We now have all the elements needed to state and prove the Fundamental Theorem of Galois Theory. As indicated earlier, we have limited our attention to the finite extension case. We should point out, however, that there is a slightly weaker, and more complicated version that holds for arbitrary extensions, finite or infinite, but we will not cover it here.

Before stating and proving the Fundamental Theorem, let's take a look at the following example. Recall from Examples 6.4.2 and 7.1.2.4 that $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$, and $\mathrm{Gal}_{\mathbb{Q}}(E) \approx D_3 \approx S_3$. Some of the intermediate fields of this extension appear in the following diagram. The numbers indicate the degree of each extension. Double lines denote normal extensions.



On the other hand, we have that the lattice of subgroups of S_3 looks like:



where double lines denote normal subgroups, and the numbers next to the edges denote the index.

Notice the remarkable similarity between these two lattices. The Fundamental Theorem of Galois Theory tells us, among other things, that this is not a coincidence. That such similarity holds for any Galois Extension, and we will make precise the sense in which these lattices are *similar*. Something else that we will get from the FTGT is that in the first lattice there are no other intermediate fields, something we have not established yet, and not at all obvious.

Theorem 7.4.10 [The Fundamental Theorem of Galois Theory] *Let* 04/16/19
E/F *be a (finite) Galois extension, with Galois group* $G = \mathrm{Gal}_F(E)$.

1. *The maps*

$$\begin{array}{rccc} {}^*: & \mathrm{Sub}_F(E) & \to & \mathrm{Sub}(G) \\ & L & \mapsto & L^* = \mathrm{Aut}_L(E) \end{array} \qquad \begin{array}{rccc} {}^*: & \mathrm{Sub}(G) & \to & \mathrm{Sub}_F(E) \\ & H & \mapsto & H^* = E_H \end{array}$$

are inverse of each other, and hence bijective.

2. *The maps * are order reversing, i.e. for intermediate subfields L_1 and L_2,*

$$L_1 \leq L_2 \Rightarrow L_2^* \leq L_1^*$$

and for subgroups $H_1, H_2 \leq G$,

$$H_1 \leq H_2 \Rightarrow H_2^* \leq H_1^*$$

3. *The maps * preserve index, i.e. for intermediate subfields $L_1 \leq L_2$,*

$$[L_2 : L_1] = [L_1^* : L_2^*]$$

and for subgroups $H_1 \leq H_2 \leq G$,

$$[H_2 : H_1] = [H_1^* : H_2^*]$$

4. *The maps * preserve normality, i.e. for intermediate subfields $L_1 \leq L_2$, L_2/L_1 is a normal extension iff L_2^* is a normal subgroup of L_1^*. Moreover, when L_2/L_1 is a normal extension, we have*

$$\mathrm{Gal}_{L_1}(L_2) \approx \frac{L_1^*}{L_2^*}$$

Proof. 1. We need to show that $L^{**} = L$ and $H^{**} = H$, for any $L \in \mathrm{Sub}_F(E)$ and any $H \in \mathrm{Sub}(G)$. From Lemma 7.4.4 we already know that $L \leq L^{**}$ and $H \leq H^{**}$.
Let $L \in \mathrm{Sub}_F(E)$. By Propositions 7.4.8, E/L is Galois, and Proposition 7.4.3 yields $L^{**} = L$.
Let $H \in \mathrm{Sub}(G)$. From Corollary 7.4.5, the "3 = 1" property, we have $H^* = H^{***}$. By the Dedeking-Artin Theorem,

$$|H| = [E : E_H] = [E : H^*] = [E : H^{***}] = [E : E_{H^{**}}] = |H^{**}|.$$

Therefore, $H = H^{**}$.

2. This was proved in Lemma 7.4.4.

3. Let $L \in \mathrm{Sub}_F(E)$. Since E/L is Galois, by Proposition 7.4.3 we have: $[E : L] = |\mathrm{Aut}_L(E)| = |L^*|$. Now, if $L_1, L_2 \in \mathrm{Sub}_F(E)$ are such that $L_1 \leq L_2$, then, using the multiplicative property of extension degrees,

$$[L_2 : L_1] = \frac{[E : L_1]}{[E : L_2]} = \frac{|L_1^*|}{|L_2^*|} = [L_1^* : L_2^*].$$

Let $H \in \mathrm{Sub}(G)$. By the Dedekind-Artin Theorem, $|H| = [E : E_H]$. Now, if $H_1, H_2 \in \mathrm{Sub}(G)$ are such that $H_1 \leq H_2$, then

$$[H_2 : H_1] = \frac{|H_2|}{|H_1|} = \frac{[E : E_{H_2}]}{[E : E_{H_1}]} = [E_{H_1} : E_{H_2}] = [H_1^* : H_2^*].$$

4. Note first that it suffice to consider the case when $L_1 = F$.
Let $L \in \mathrm{Sub}_F(E)$. We want to show that L is a normal extension of F iff L^* is a normal subgroup of $F^* = G$. Since L/F is a finite, separable extension, by the Primitive Element Theorem, there is $u \in L$ such that $L = F(u)$. Since any $\sigma \in G$ fixes F, we have $\sigma \in L*$ iff σ fixes L, iff $\sigma(u) = u$.
Assume L/F is a normal extension. By Proposition 7.4.9, $\min_F(u)$ splits in L. Let $\sigma \in L*$ and $\tau \in G$. We want to show $\tau^{-1}\sigma\tau \in L^*$. By Proposition 7.1.5 $\tau(u)$ is a root of $\min_F(u)$, and therefore $\tau(u) \in L$. Therefore $\sigma(\tau(u)) = \tau(u)$, and $\tau^{-1}\sigma\tau(u) = u$. So, $\tau^{-1}\sigma\tau \in L^*$.
Conversely, assume L^* is a normal subgroup of G.
Claim: $\min_F(u)$ splits in L. Suppose otherwise, i.e. there is a root $v \in E$ of $\min_F(u)$ such that $v \notin L$. By Proposition 7.1.5 there is a homomorphism $\varphi : F(u) \to E$ such that $\varphi(u) = v$. By Corollary 6.4.14, φ can be extended to an automorphism $\tau : E \to E$, that is, $\tau \in \mathrm{Aut}_F(E)$, such that $\tau(u) = v$. Since $v \notin L = L^{**}$, there is $\sigma \in L^*$ such that $\sigma(v) \neq v$. Since $L^* \trianglelefteq G$, we have $\tau^{-1}\sigma\tau \in L^*$. If follows that

$$u = \tau^{-1}\sigma\tau(u) = \tau^{-1}\sigma(v), \text{ and } \tau(u) = \sigma(v) \neq v,$$

a contradiction.
Since $\min_F(u)$ splits in L and $L = F(u)$, L is the splitting field of $\min_F(u)$, and L/F is a normal extension.
To prove the second part of the statement, namely, that 04/17/19

$$\mathrm{Gal}_F(L) \approx \frac{F^*}{L^*} = \frac{G}{L^*}, \tag{7.11}$$

note that for any $\tau \in G$, $\tau(u)$ is a root of $\min_F(u)$, hence an element of L. The restriction $\tau|_L$ maps L to L, fixing F. This tells us that $\tau|_L$ is an injective F-linear transformation from the finite dimensional vector space L to itself. It follows that $\tau|_L$ is bijective, and $\tau|_L \in \mathrm{Aut}_F(L)$. The restriction map

$$\begin{array}{rccc} \rho: & \mathrm{Aut}_F(E) & \to & \mathrm{Aut}_F(L) \\ & \tau & \mapsto & \tau|_L \end{array}$$

is a group homomorphism, and $\ker(\rho) = \mathrm{Aut}_L(E)$. It is easy to show that ρ is surjective (see Exercise 7.4.3 below). By the First Isomorphism Theorem, we get (7.11). ■

Exercise 7.4.3. Show that the restriction map ρ in the proof of Theorem 7.4.10 is a group epimorphism.

Corollary 7.4.11 *Let E/F be a (finite) Galois extension, with Galois group $G = \mathrm{Gal}_F(E)$. Let $L_1, L_2 \in \mathrm{Sub}_F(E)$ and $H_1, H_2 \in \mathrm{Sub}(G)$.*

1. $(L_1 \wedge L_2)^* = L_1^* \vee L_2^*$
2. $(L_1 \vee L_2)^* = L_1^* \wedge L_2^*$
3. $(H_1 \wedge H_2)^* = H_1^* \vee H_2^*$
4. $(H_1 \vee H_2)^* = H_1^* \wedge H_2^*$

Exercise 7.4.4. Prove Corollary 7.4.11 using only the statement of the Fundamental Theorem.

Exercise 7.4.5. Prove the general case in Part 7.4.10.4 of Theorem 7.4.10 using the special cased already proved.

PS 06

7.4.4 More Examples

04/22/19

We now present a few more examples to illustrate the Fundamental Theorem.

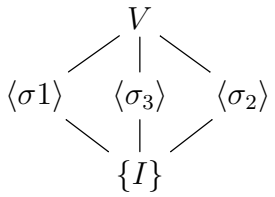
Examples 7.4.3. 1. Let E be the finite field $E = \mathbb{F}_{p^n}$. By Proposition 7.2.4, E is separable over $F = \mathbb{F}_p$. In the proof of Theorem 6.6.6 we showed that E is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$, so E/F is a normal extension. It is a Galois extension. The subfields of E are all the finite fields of the form $\mathbb{F}_{p^d}$ as d ranges over the divisors of n. It follows that the lattice of subfields of E is isomorphic to the lattice of divisors of n. On the other hand, the Galois group $G = \mathrm{Gal}_F(E)$ is cyclic of order n. The subgroups of G are cyclic groups of order d where d ranges over the divisors of n. As G is abelian, all subgrops of G are normal. On the other hand, all subfields of E are normal over $\mathbb{F}_p$.

2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbb{Q}$. In Example 7.3.2 we have seen that E is the splitting field of $(x^2-2)(x^2-3)$, so E/F is a Galois extension. We also showed that $\mathrm{Gal}_F(E)$ is the Klein 4-group $V = \{I, \sigma_1, \sigma_2, \sigma_3\}$, where

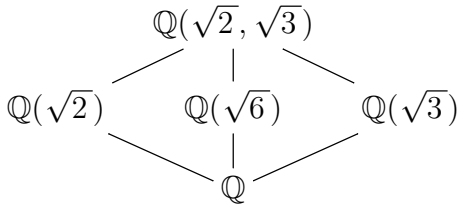
$$I: \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \sigma_1: \begin{array}{ccc} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

$$\sigma_2: \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \sigma_3: \begin{array}{ccc} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

The lattice of subgroups of V is



so the diagram of subfields of E on page 92 is missing one subfield. $\mathbb{Q}(\sqrt{2})$ is the subfield fixed by $\langle\sigma_1\rangle$, and $\mathbb{Q}(\sqrt{3})$ is the subfield fixed by $\langle\sigma_2\rangle$. We are missing the subfield fixed by $\langle\sigma_3\rangle$. It is easy to see that $\sigma_3(\sqrt{6}) = \sqrt{6}$, and it follows that the subfield fixed by $\langle\sigma_3\rangle$ is precisely $\mathbb{Q}(\sqrt{6})$. Moreover, the Fundamental Theorem of Galois Theory tells us that there are no other subfields of E. Here is the lattice of subfields.



3. From Example 7.4.2.4, on page 98, we have that $E = \mathbb{Q}(\sqrt[4]{2}, i)$, the splitting field of $x^4 - 2$ over $\mathbb{Q}$ has Galois group

$$G = D_4 = \{I, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}.$$

If we denote the roots of $x^4 - 2$ as follows:

$$\alpha_1 = \sqrt[4]{2}, \quad \alpha_2 = i\sqrt[4]{2}, \quad \alpha_3 = -\sqrt[4]{2}, \quad \alpha_4 = -i\sqrt[4]{2},$$

then the elements of G are permutations of $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

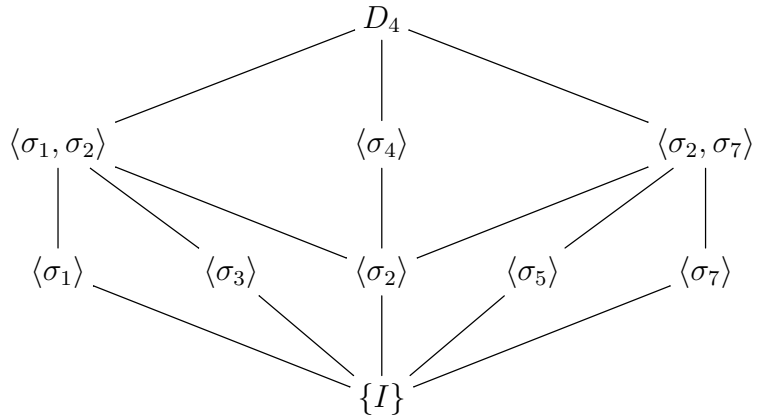
$$\begin{array}{rcl} I: \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \\ i & \mapsto & i \\ \multicolumn{3}{c}{\epsilon} \end{array} \qquad \begin{array}{rcl} \sigma_1: \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \\ i & \mapsto & -i \\ \multicolumn{3}{c}{(\alpha_2\ \alpha_4)} \end{array}$$

$$\begin{array}{rcl} \sigma_2: \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} \\ i & \mapsto & i \\ \multicolumn{3}{c}{(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_4)} \end{array} \qquad \begin{array}{rcl} \sigma_3: \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} \\ i & \mapsto & -i \\ \multicolumn{3}{c}{(\alpha_1\ \alpha_3)} \end{array}$$

$$\begin{array}{rcl} \sigma_4: \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} \\ i & \mapsto & i \\ \multicolumn{3}{c}{(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4)} \end{array} \qquad \begin{array}{rcl} \sigma_5: \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} \\ i & \mapsto & -i \\ \multicolumn{3}{c}{(\alpha_1\ \alpha_2)(\alpha_3\ \alpha_4)} \end{array}$$

$$\begin{array}{rcl} \sigma_6: \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2} \\ i & \mapsto & i \\ \multicolumn{3}{c}{(\alpha_1\ \alpha_4\ \alpha_3\ \alpha_2)} \end{array} \qquad \begin{array}{rcl} \sigma_7: \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2} \\ i & \mapsto & -i \\ \multicolumn{3}{c}{(\alpha_1\ \alpha_4)(\alpha_2\ \alpha_3)} \end{array}$$

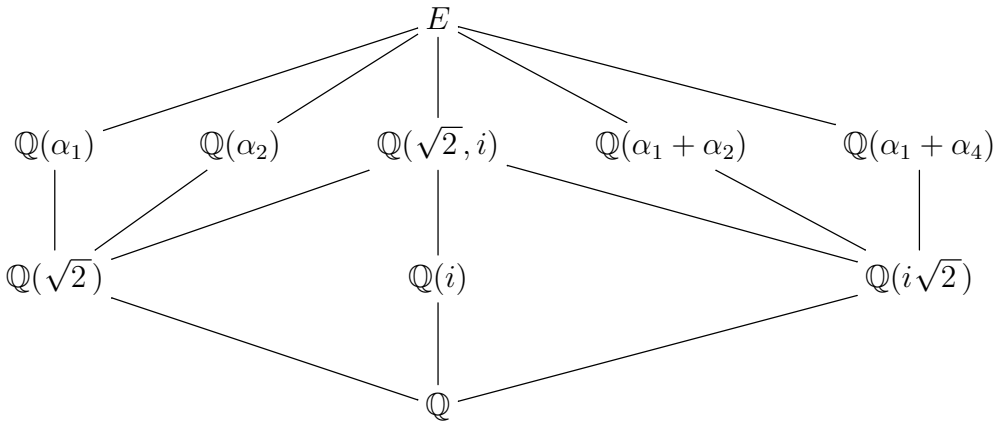
The lattice of subgroups of G is



The fixed subfields are: 04/23/19

$$\begin{array}{rclrcl} E_{\sigma_1} &=& \mathbb{Q}(\alpha_1) & E_{\sigma_3} &=& \mathbb{Q}(\alpha_2) \\ E_{\sigma_5} &=& \mathbb{Q}(\alpha_1+\alpha_2) & E_{\sigma_2} &=& \mathbb{Q}(\sqrt{2}\,,i) \\ E_{\sigma_7} &=& \mathbb{Q}(\alpha_1+\alpha_4) & E_{\sigma_4} &=& \mathbb{Q}(i) \\ E_{\langle\sigma_1,\sigma_2\rangle} &=& \mathbb{Q}(\alpha_1^2)=\mathbb{Q}(\sqrt{2}\,) & E_{\langle\sigma_2,\sigma_7\rangle} &=& \mathbb{Q}(\alpha_1\alpha_2)=\mathbb{Q}(i\sqrt{2}\,) \end{array}$$

and the lattice of subfields is:



4. Let E be the splitting field of $f(x)=x^5-20x+6\in\mathbb{Q}[x]$. It is a Galois extension of $\mathbb{Q}$. Let $G=\mathrm{Gal}_{\mathbb{Q}}(E)=\mathrm{Aut}_{\mathbb{Q}}(E)$. Using the Eisenstein

Criterion, with $p = 2$, we see that $f(x)$ is irreducible over $\mathbb{Q}$. From the first and second derivatives of $f(x)$

$$\begin{aligned} f'(x) &= 5x^4 - 20 \\ f''(x) &= 20x^3 \end{aligned}$$

we see that $f''(x)$ has a single real root, so by the Mean Value Theorem $f'(x)$ has at most two real roots, and $f(x)$ has at most three real roots. The table of values

x	-3	0	1	3
$f(x)$	-177	6	-13	189

and the Intermediate Value Theorem, tell us that $f(x)$ has three real roots. Therefore of the five roots of $f(x)$, three of them $\alpha_1, \alpha_2, \alpha_3$ are real, and the other two are non-real conjugate of each other $\overline{\alpha_4} = \alpha_5$.

Complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$, given by $a + bi \mapsto a - bi$, fixes the coefficients of f, and therefore it permutes its roots. Restricting τ to E yields an automorphism of E that fixes $\mathbb{Q}$, i.e. $\tau \in G$. Since τ fixes all real numbers, as a permutation of the roots, we can write it $\tau = (\alpha_4\ \alpha_5)$.
Since $f(x)$ is irreducible over $\mathbb{Q}$, the extension $\mathbb{Q}(\alpha_1)$ has degree 5 over $\mathbb{Q}$. By the multiplicative property of extension degrees, we get that 5 divides $[E : \mathbb{Q}] = |G| \leq S_5$. The only elements in S_5 of order 5 are 5-cycles, so by Caucy's Theorem G contains a 5-cycle, call it ρ. It is easy to see that ρ and τ generate all of S_5, see Exercise 7.4.8 below. Therefore $G \approx S_5$. We immediately get that $[E : \mathbb{Q}] = 120$. The lattice of subgroups of S_5 is large, and so is the lattice of intermediate fields of $E/\mathbb{Q}$. It can be shown that the only proper non-trivial normal subgroup of S_5 is A_5. Therefore, of all intermediate subfields of $E/\mathbb{Q}$ there is only one that is normal over $\mathbb{Q}$, and it must have degree 2.

Exercise 7.4.6. Show that the transpositions $(1\ \ 2), (2\ \ 3), \ldots, (n-1\ \ n)$ generate the group S_n.

Exercise 7.4.7. Show that S_n is generated by the following two permutations:

$$\rho = (1\ \ 2\ \ \ldots\ \ n) \quad \text{and} \quad \sigma = (1\ \ 2)$$

root of unity|slantit
complex n-th roots of unity
cis|slantit
μ_n
primitive roots of unity|slantit

Exercise 7.4.8. Let p be prime, ρ a p-cycle, and σ a transposition. Show that ρ and σ generate S_p. Show, by counterexample, that the hypothesis of p being prime cannot be removed.

Exercise 7.4.9. Refer to Example 7.4.3.4. Show that

$$E \cap \mathbb{R} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3).$$

7.5 Cyclotomic Extensions of $\mathbb{Q}$

We now extend the results in Proposition 7.3.1 from the case of a prime p to arbitrary positive integer n.

The roots of the complex polynomial $x^n - 1$ are called *complex n-th roots of unity* . By Theorem 4.1.5 there are at most n of them, counting multiplicity. A simple check shows that if we let $\xi_n = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ ($\mathrm{cis}(\frac{2\pi}{n})$ for short), then the following:

$$1, \xi_n, \xi_n^2, \ldots, \xi_n^{n-1}$$

are all roots of the polynomial, and hence they are all the n-th roots of unity and each has multiplicity 1.

Note that the n-th roots of unity form a multiplicative subgroup of $\mathbb{C}^*$ of order n. Let's denote it by μ_n . By Proposition 6.6.8 it must be cyclic and it is obvious that $\xi_n = \mathrm{cis}(\frac{2\pi}{n})$ is a generator of μ_n. By Proposition 2.0.1 the multiplicative order of ξ_n^k is equal to $\dfrac{n}{\text{g.c.d.}(n,k)}$. In particular ξ_n^k is a generator of μ_n, i.e. has order n, iff g.c.d.$(n,k) = 1$. Such ξ_n^k's are called primitive n-th roots of unity .

Proposition 7.3.1 tells us that when p is a prime number the polynomial

$$\phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

is irreducible over $\mathbb{Q}$. We called it the p-th cyclotomic polynomial. Its roots are precisely the primitive p-th roots of unity, so $\phi_p(x)$ is the minimal polynomial over $\mathbb{Q}$ of any primitive p-th root of unity. We want to extend the previous ideas and results to non-primes. Observe that $\mathbb{Q}(\xi_n)$ is the splitting

field of $x^n - 1$ over $\mathbb{Q}$. The polynomial

cyclotomic polynomial

$$\phi_n(x) = \prod_{\text{g.c.d.}(n,k)=1} (x - \xi^k)$$

whose roots are precisely the primitive n-th roots of unity, is called the n-th *cyclotomic polynomial*.

Since any root of $x^n - 1$ is an element of μ_n, its order has to be a divisor d of n. It is a primitive d-th root of unity, i.e. a root of $\phi_d(x)$. Since $x^n - 1$ has no multiple roots, it follows that

$$x^n - 1 = \prod_{d|n} \phi_d(x) \tag{7.12}$$

which gives us a recursive method to compute the cyclotomic polynomials. First of all, when we take $n = 1$ we get

$$(x - 1) = \phi_1(x).$$

When $n = p$ is a prime then we get

$$x^p - 1 = \phi_1(x) \cdot \phi_p(x)$$

which yields what we already knew

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

04/24/19

PS 07

Now, for a non-prime like $n = 6$, to compute $\phi_6(x)$ we only need to know $\phi_1(x) = (x - 1)$, $\phi_2(x) = x + 1$ and $\phi_3(x) = x^2 + x + 1$. Thus we have

$$x^6 - 1 = \phi_1(x) \cdot \phi_2(x) \cdot \phi_3(x) \cdot \phi_6(x)$$

so

$$\phi_6(x) = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)} = x^2 - x + 1.$$

Similar computations yield the following:

$$\begin{aligned}
\phi_1(x) &= x-1\\
\phi_2(x) &= x+1\\
\phi_3(x) &= x^2+x+1\\
\phi_4(x) &= x^2+1\\
\phi_5(x) &= x^4+x^3+x^2+x+1\\
\phi_6(x) &= x^2-x+1\\
\phi_7(x) &= x^6+x^5+x^4+x^3+x^2+x+1\\
\phi_8(x) &= x^4+1\\
\phi_9(x) &= x^6+x^3+1\\
\phi_{10}(x) &= x^4-x^3+x^2-x+1\\
\phi_{11}(x) &= x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+-1\\
\phi_{12}(x) &= x^4-x^2+1
\end{aligned}$$

Exercise 7.5.1. Use the recursive formula (7.12) to obtain the cyclotomic polynomials in the table above.

We can easily see patterns connecting different cyclotomic polynomials. It is a fun exercise to write them down and try to prove them.

Exercise 7.5.2.

1. How are $\phi_n(x)$ and $\phi_{2n}(x)$ related when n is odd? Prove it.
2. How are $\phi_n(x)$ and $\phi_{2n}(x)$ related when n is even? Prove it.
3. Prove that for $n>2$ the degree of $\phi_n(x)$ is even.

Proposition 7.5.1 [Gauss] *The cyclotomic polynomial $\phi_n(x)$ is monic, irreducible with integral coefficients.* 04/26/19

Proof. The fact that it is monic is immediate from the definition. That it has rational coefficients follows by induction on n and the division algorithm for the Euclidean Domain $\mathbb{Q}[x]$. From the recursive formula (7.12) we have in $\mathbb{Q}(\xi)$

$$x^n-1=\phi_n(x)\cdot\prod_{d|n,d<n}\phi_d(x) \tag{7.13}$$

Since, by inductive hypothesis, $\displaystyle\prod_{d|n,d<n}\phi_d(x)\in\mathbb{Q}[x]$, the existence in $\mathbb{Q}[x]$ and the uniqueness in $\mathbb{C}[x]$ from the division algorithm forces $\phi_n(x)$ to be in $\mathbb{Q}[x]$.

Now, using again induction on n and Corollary 4.5.8 to Gauss' Lemma, we get that $\phi_n(x) \in \mathbb{Z}[x]$.
To see that $\phi_n(x)$ is irreducible, write $\phi_n(x) = f(x) \cdot g(x)$ with $f(x), g(x) \in \mathbb{Z}[x]$, and $f(x)$ irreducible. Since $\phi_n(x)$ is monic, WLOG we can take both $f(x)$ and $g(x)$ to be monic, hence primitive. We claim that if β is a root of $f(x)$ and p is a prime not divisor of n then β^p is also a root of $f(x)$. Assume otherwise. Note, first of all, that $f(x)$ is the minimal polynomial for β over $\mathbb{Q}$. Since $p \nmid n$, β^p is also a primitive n-th root of unity, hence a root of $\phi_n(x)$. From the assumption that β^p is not a root of $f(x)$ we get that it has to be a root of $g(x)$, so $g(\beta^p) = 0$, and β is a root of $g(x^p)$. This means that $f(x)$ divides $g(x^p)$, i.e. $g(x^p) = f(x) \cdot h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let's now reduce coefficients modulo p to get

$$\overline{g}(x)^p = \overline{g}(x^p) = \overline{f}(x) \cdot \overline{h}(x) \in \mathbb{Z}_p[x]$$

which tells us that any root of $\overline{f}(x)$ is also a root of $\overline{g}(x)$. Since $\overline{\phi_n}(x) = \overline{f}(x) \cdot \overline{g}(x)$, then $\overline{\phi_n}(x)$ has a multiple root, and so does $x^n - 1 \in \mathbb{Z}_p[x]$. But this contradicts Proposition 6.6.2 since $p \nmid n$, and $(x^n - 1)' = nx^{n-1}$, whose only root is 0. Repeated use of the claim we just proved, shows that for any k with g.c.d.$(k, n) = 1$, β^k is a root of $f(x)$, so all the roots of $\phi_n(x)$ are roots of $f(x)$. Since $\phi(x)$ has no multiple roots then we conclude that $g(x) = 1$ and $\phi(x) = f(x)$ is irreducible. ■

Theorem 7.5.2 *The extension $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is a Galois extension of degree $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$ and Galois group*

$$\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \approx U_n,$$

the multiplicative group of units of the ring $\mathbb{Z}_n$.

Proof. We have already seen that $\mathbb{Q}(\xi_n)$ is the splitting field of $x^n - 1 \in \mathbb{Q}[x]$, so $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is Galois. Since $\phi_n(x)$ is irreducible and monic it is the minimal polynomial of ξ_n over $\mathbb{Q}$, and therefore $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \deg(\phi_n(x)) = \varphi(n)$,
04/29/19 the number of primitive n-th roots of unity. For each k between 1 and n, relatively prime to n, ξ_n^k is a primitive n-th root of unity, so there is an automorphism

$$\begin{array}{rccc} \psi_k : & \mathbb{Q}(\xi_n) & \to & \mathbb{Q}(\xi_n) \\ & \xi_n & \mapsto & \xi_n^k \end{array}$$

Klein group|slantit

but these k's are precisely the elements of U_n. Moreover, if $k, l \in U_n$ then

$$\psi_k \circ \psi_l(\xi_n) = \psi_k(\xi_n^l) = \xi_n^{kl} = \psi_{kl}(\xi_n),$$

and $\psi_k \circ \psi_l = \psi_{kl}$. So, the map

$$\begin{array}{rccc} \psi: & U_n & \to & \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \\ & k & \mapsto & \psi_k \end{array}$$

is the desired isomorphism. ■

Exercise 7.5.3. Show that the map ψ in the proof of Theorem 7.5.2 is indeed injective and surjective.

Exercise 7.5.4. Show that if d is a divisor of n then $\mathbb{Q}(\xi_d)$ is a subfield of $\mathbb{Q}(\xi_n)$. Conclude that $\varphi(d)$ divides $\varphi(n)$, and U_d is a quotient of U_n.

Example 7.5.1. Let's analize the cyclotomic extension for $n = 12$ in detail. Let's write ξ for ξ_{12}. We have $\varphi(12) = 4$, so $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$ and $\min_{\mathbb{Q}}(\xi) = x^4 - x^2 + 1$. The group $U_{12} = \{1, 5, 7, 11\}$ is isomorphic to the Klein group , and its non-trivial proper subgroups are $\{1, 5\}$, $\{1, 7\}$, and $\{1, 11\}$, for a total of five subgroups. For each divisor d of 12, $\xi^{12/d}$ is a primitive d-th root of unity, and by Exercise 7.5.4 we have that $\mathbb{Q}(\xi^{12/d})$ is a subfield of $\mathbb{Q}(\xi)$. This seems to give us more subfields than we would expect based on the FTGT. The subfields are: $\mathbb{Q}(\xi^{12})$, $\mathbb{Q}(\xi^6)$, $\mathbb{Q}(\xi^4)$, $\mathbb{Q}(\xi^3)$, $\mathbb{Q}(\xi^2)$, and $\mathbb{Q}(\xi)$. Note, however, that in addition to $\xi^{12} = 1$, ξ also satisfies the equations

$$\xi^2 = \xi^4 + 1 \quad \text{and} \quad \xi^6 = -1. \tag{7.14}$$

This tells us that

$$\mathbb{Q}(\xi^{12}) = \mathbb{Q}(\xi^6) = \mathbb{Q} \quad \text{and} \quad \mathbb{Q}(\xi^4) = \mathbb{Q}(\xi^2),$$

so we really only have $\mathbb{Q}$, $\mathbb{Q}(\xi^3)$, $\mathbb{Q}(\xi^2)$, and $\mathbb{Q}(\xi)$, one fewer that the five fields we expect. Clearly $\mathbb{Q}^* = U_{12} = \{1, 5, 7, 11\}$, and $\mathbb{Q}(\xi)^* = \{1\}$. Now, note that $(\xi^2)^7 = \xi^{14} = \xi^2$, so $\mathbb{Q}(\xi^2)$ is fixed by $\psi_7 : \xi \mapsto \xi^7$. In fact, since $\xi^2 = \xi_6$ is a root of the irreducible polynomial $\phi_6(x) = x^2 - x + 1$, we have $[\mathbb{Q}(\xi^2) : \mathbb{Q}] = 2$, and this forces $\mathbb{Q}(\xi^2)^* = \{1, 7\}$. A similar argument, noting that $(\xi^3)^5 = \xi^{15} = \xi^3$, shows that $\mathbb{Q}(\xi^3)^* = \{1, 5\}$. That leaves us with the question of what is the field $\{1, 11\}^*$? A generic element of $\mathbb{Q}(\xi)$ can be uniquely written as

$$\gamma = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 \quad \text{with} \quad a_0, a_1, a_2, a_3 \in \mathbb{Q}$$

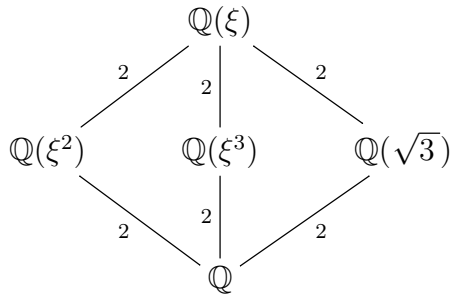
When we apply the automorphism ψ_{11} to γ, and using Equations 7.14, we get

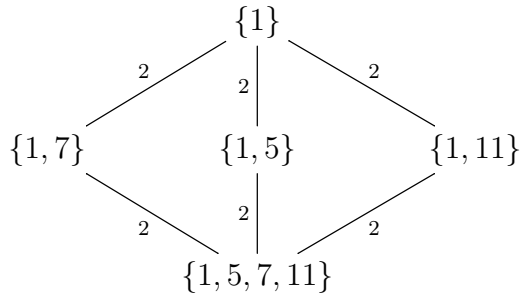
$$\begin{aligned}\psi_{11}(\gamma) &= a_0 + a_1\xi^{11} + a_2\xi^{22} + a_3\xi^{33} \\ &= a_0 - a_1\xi^5 - a_2\xi^4 - a_3\xi^3 \\ &= a_0 - a_1(\xi^3 - \xi) - a_2(\xi^2 - 1) - a_3\xi^3 \\ &= (a_0 + a_2) + a_1\xi - a_2\xi^2 - (a_1 + a_3)\xi^3\end{aligned}$$

So, we get that $\psi_{11}(\gamma) = \gamma$ iff $a_2 = 0$ and $a_1 = -2a_3$. Therefore $\{1, 11\}^* = \mathbb{Q}(\xi^3 - 2\xi)$. We have

$$\begin{aligned}\xi &= \text{cis}(2\pi/12) = \tfrac{\sqrt{3}}{2} + \tfrac{1}{2}i, \\ \xi^3 - 2\xi &= \text{cis}(2\pi/4) - 2\text{cis}(2\pi/12) = i - (\sqrt{3} + i) = -\sqrt{3},\end{aligned}$$

and therefore $\{1, 11\}^* = \mathbb{Q}(\sqrt{3})$.
We summarize these calculations in the following lattice diagrams:





Since the group U_{12} is abelian, all subgroups are normal, and all extensions are Galois.

An important consequence of Theorem 7.5.2 is the following corollary.

Corollary 7.5.3 *Let F be a field of characteristic zero, and $\xi = \xi_n$ a primitive n-th root of unity. The extension $F(\xi)/F$ is Galois, and its Galois group is isomorphic to a subgroup of U_n, hence it is abelian.*

Proof. Note that $\phi_n(x) \in F[x]$ since $\mathbb{Q}$ is a subfield of F, and ξ is a root of $\phi_n(x)$. Therefore $\min_F(\xi)$ divides $\phi_n(x)$, and the roots of $\min_F(\xi)$ are some of the primitive n-th roots of unity. It follows that all automorphisms of the extension $F(\xi)/F$ are of the form $\psi_k : \xi \mapsto \xi^k$, and the map

$$\begin{array}{rccc}\Upsilon: & \text{Gal}(F(\xi)/F) & \to & U_n \\ & \psi_k & \mapsto & k\end{array}$$

$\sqrt[n]{a}$

is a monomorphism. ■

Exercise 7.5.5. Show with an example that $\mathrm{Gal}(F(\xi)/F)$ does not need to be all of U_n, i.e. the map Υ used in the proof of Corollary 7.5.3 need not be surjective.

Exercise 7.5.6. Let ξ_{15} be a primitive complex 15-th root of unity.

1. Find the group $\mathrm{Gal}(\mathbb{Q}(\xi_{15})/\mathbb{Q})$ and draw its lattice of subgroups.
2. Find and draw the lattice of intermediate fields of the extension $\mathbb{Q}(\xi_{15})/\mathbb{Q}$.
3. Write down the correspondence between the subgroups in part 1 and the subfields in part 2, using the Fundamental Theorem of Galois Theory.

7.6 The Splitting Field of $x^n - a$

04/30/19

Closely related to cyclotomic extensions are the splitting fields of polynomials of the form $x^n - a$ in characteristic zero. The example we have extensively considered x^3-2 is just a particular case of what we are going to consider here. Let F be a field of characteristic zero, and $a \in F$. Select and fix a root of $x^n - a$, and denote it by $\sqrt[n]{a}$. All the roots of $x^n - a$ are of the form $\xi^i \sqrt[n]{a}$ with ξ a primitive n-th root of unity (?) and $0 \le i \le n-1$[2]. The splitting field of this polynomial is $F(\xi, \sqrt[n]{a})$. Note that we can break this extension into a two step tower with $F(\xi)$ in the middle. By Corollary 7.5.3 the bottom extension is Galois with Abelian Galois group. Now consider the top extension $F(\xi, \sqrt[n]{a})/F(\xi)$. The minimal polynomial $\min_{F(\xi)}(\sqrt[n]{a})$ divides $x^n - a$, so all its roots are of the form $\xi^k \sqrt[n]{a}$. It follows then thal all automorphisms of $F(\xi, \sqrt[n]{a})/F(\xi)$ are of the form $\nu_k : \sqrt[n]{a} \mapsto \xi^k \sqrt[n]{a}$ with $0 \le k < n$. Note that $\nu_k \circ \nu_l = \nu_{k+l}$, and $\nu_k = \mathrm{id}$ iff $k = 0$. So the map

$$F(\xi, \sqrt[n]{a})$$
$$|$$
$$F(\xi)$$
$$|$$
$$F$$

$$\begin{array}{rccc} \Xi: & \mathrm{Gal}(F(\xi, \sqrt[n]{a})/F(\xi)) & \to & C_n \\ & \nu_k & \mapsto & k \end{array} \tag{7.15}$$

[2]The notation $\sqrt[n]{a}$ is ambiguous since the choice is arbitrary. However, for any choice we make, the expression $\xi^i \sqrt[n]{a}$, with $i = 0, \ldots, n-1$, yields all the roots of $x^n - a$.

is a monomorphism and $\mathrm{Gal}(F(\xi, \sqrt[n]{a})/F(\xi))$ is cyclic.

cyclic-by-abelian
Galois
group|slantit
transitive
action|slantit
solvable
group!solvable

We have just proved that $\mathrm{Gal}(F(\xi, \sqrt[n]{a})/F)$ has a cyclic normal subgroup $\mathrm{Gal}(F(\xi, \sqrt[n]{a})/F(\xi))$ with abelian quotient $\mathrm{Gal}(F(\xi)/F)$. We call such group a *cyclic-by-abelian* group.

Remark 7.6.1. When the splitting field of a polynomial is separable, for example, in characteristic zero, we refer to the Galois group of the splitting field as the Galois group of the polynomial. Proposition 7.1.5 tells us that any element of the Galois group of a polynomial permutes its roots, and Lemma 6.4.13 tells us that if the polynomial is irreducible then the action of the Galois group on its roots is transitive .

So we have just proved the following theorem.

Theorem 7.6.1 *Let F be a field of characteristic zero, and $a \in F$. The Galois group of the polynomial $x^n - a$ is cyclic-by-Abelian. Moreover, the cyclic normal subgroup is a subgroup of C_n and the abelian quotient is a subgroup of U_n.*

Exercise 7.6.1. Show with an example that $\mathrm{Gal}(F(\xi)/F)$ does not need to be all of C_n, i.e. the map Ξ of Formula (7.15) used in the proof of Theorem 7.6.1 need not be surjective.

Corollary 7.6.2 *Let F be a field of characteristic zero, and $a \in F$. If $\xi_n \in F$, then $F(\sqrt[n]{a})$ is the splitting field of $x^n - a$, and the Galois group of the polynomial $x^n - a$ is cyclic.*

7.7 Solvable Groups

Cyclic-by-abelian groups are a special case of a larger class of groups, the so-called *solvable* groups. A group G is said to be *solvable* if there is a finite sequence of subgroups

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{7.16}$$

such that each H_{i+1}/H_i is Abelian.

Abelian series
solvable length
length!solvable
derived length
length!␣derived
metabelian

The sequence (7.16) is called an *Abelian series* for G and n is called the length of the series. The smallest n for which the group G has an Abelian series of length n is called the *solvable length* or *derived length* of G. Solvable groups of length ≤ 2 are also called *metabelian*.

Examples 7.7.1.
1. Every Abelian group is solvable, of length ≤ 1, and conversely.
2. Every cyclic-by-Abelian group is solvable of length ≤ 2. In particular the Galois group of the splitting field of $x^n - a$ over a field of characteristic zero is solvable.
3. The group A_5 is not solvable. We will prove this below in Theorem 7.7.1.

Exercise 7.7.1.
1. Let G be a finite group. Show that G is solvable iff there is a finite sequence of subgroups
$$1 = H_0 \leq H_1 \leq \cdots \leq H_{n-1} \leq H_n = G$$
such that each $H_i \trianglelefteq H_{i+1}$ and H_{i+1}/H_i is cyclic. In other words, for finite groups, we can replace Abelian with cyclic in the definition of solvable.
2. Show, with a counterexample, that for infinite groups the two conditions are not be equivalent.

Theorem 7.7.1 *The group A_5 is not solvable.*

Proof. It is clear that A_5 is not Abelian, since the two three-cycles (1 2 3) and (3 4 5) do not commute. We will show that A_5 has no proper non-trivial normal subgroup. From these two facts the result follows. By Theorem **??.??** the non-trivial elements of A_5 have one of the following shapes when written in disjoint cycle form:

a 3-cycle	$(a\ b\ c)$,
a 5-cycle	$(a\ b\ c\ d\ e)$.
a product of two 2-cycles	$(a\ b)(c\ d)$,

Let $1 \neq H \trianglelefteq A_5$. Consider 3 cases:
Case 1: H contains a 3-cycle $(a\ b\ c)$. Any other 3-cycle has one or two

symbols in common with this one. Note that

simple group

$$(a\ b\ c)^{(a\ b\ c\ d\ e)} = (b\ c\ d), \quad (a\ b\ c)^{(a\ c\ e\ b\ d)} = (c\ d\ e),$$

and since H is normal it contains all 3-cycles. By Exercise 7.7.3, we get $H = A_5$.

Case 2: H contains a 5-cycle $(a\ b\ c\ d\ e)$. Note that

$$(a\ b\ c\ d\ e)^{(b\ c)(d\ e)} = (a\ c\ b\ e\ d), \quad \text{and} \quad (a\ b\ c\ d\ e)(a\ c\ b\ e\ d) = (a\ d\ b).$$

So H contains a 3-cycle and by case 1, $H = A_5$.

Case 3: H contains a product of two 2-cycles $(a\ b)(c\ d)$. Note that

$$(a\ b)(c\ d)^{(c\ d\ e)} = (a\ b)(d\ e) \quad \text{and} \quad (a\ b)(c\ d)(a\ b)(d\ e) = (c\ d\ e).$$

So H contains a 3-cycle and by case 1, $H = A_5$. ■

It can be shown that A_5 is in fact the smallest non-solvable group, i.e. any group of order less than or equal to 59 is solvable. A group that has no normal subgroup other than itself and the trivial subgroups is called a *simple group*.

Scholium 7.7.2 *The group A_5 is simple.*

Exercise 7.7.2. Show that any non-Abelian simple group is non-solvable.

Exercise 7.7.3. Prove that any element of the alternating group A_n can be written as a product of 3-cycles.

Exercise 7.7.4. Determine all the simple Abelian finite groups. (Hint: use Cauchy's Theorem for Abelian groups, **??**.)

05/01/19 Solvable groups have many nice properties. The following theorem is one of them.

Theorem 7.7.3 *Let G be a group.*

1. *If G is solvable then so is every subgroup of G.*
2. *For $N \trianglelefteq G$, G is solvable iff N and G/N are solvable.*

One refers to this result by saying that the class of solvable groups is closed under subgroups, quotients and extensions.

Proof. (1) Suppose G is solvable. Let

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G \tag{7.17}$$

be an Abelian series for G, and $K \leq G$ a subgroup of G. It follows from the Second Isomorphism Theorem that for $i = 1, \ldots, n$

$$K \cap H_{i-1} = K \cap H_i \cap H_{i-1} \trianglelefteq K \cap H_i,$$

and

$$\frac{K \cap H_i}{K \cap H_{i-1}} = \frac{K \cap H_i}{K \cap H_i \cap H_{i-1}} \approx \frac{(K \cap H_i)H_{i-1}}{H_{i-1}} \leq \frac{H_i}{H_{i-1}}$$

which is Abelian. Therefore,

$$1 = K \cap H_0 \trianglelefteq K \cap H_1 \trianglelefteq \cdots \trianglelefteq K \cap H_{n-1} \trianglelefteq K \cap H_n = K$$

is an Abelian series for K
(2) Assume G is solvable, with Abelian series as (7.17). Then by part (1) N is solvable.

■

Exercise 7.7.5. Let G be a group. If $K \leq G$ and $N \trianglelefteq G$ then $(K \cap N) \trianglelefteq K$.

Corollary 7.7.4 *If G and H are solvable groups then so is their direct product $G \times H$.*

Exercise 7.7.6. Prove Corollary 7.7.4.

7.8 Solvability by Radicals

Throughout this section all fields we consider will have characteristic zero. The quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{7.18}$$

expresses the solutions of the polynomial equation

$$ax^2 + bx + c = 0 \tag{7.19}$$

using the coefficients, field constants and operations, and radicals. So, we say that Equation 7.19) can be solved by radicals. In general, we say that the polynomial equation $f(x) = 0$ is *solvable by radicals* if the roots of $f(x)$ can be expressed using the coefficients of $f(x)$, field constants and operations, and taking radicals.

solvable by radicals
Cardano's formula

05/03/19

Board presentations PS 08

05/06/19

In the early 1500's a number of Italian mathematicians, including dal Ferro, Tartaglia, Fior, Ferrari and Cardano found the solution to the *depressed* cubic equation

$$x^3 + ax + b = 0 \tag{7.20}$$

Cardano published it 1545 in his Ars Magna. The roots to the depressed cubic equation (7.20) are given by:

$$\alpha_1 = \frac{A+B}{3}, \quad \alpha_2 = \frac{\omega A + \omega^2 B}{3}, \quad \text{and} \quad \alpha_3 = \frac{\omega^2 A + \omega B}{3}$$

where ω is a primitive cubic root of unity and A and B are given by

$$\begin{aligned} A &= \sqrt[3]{\tfrac{-27}{2}b + \tfrac{3}{2}\sqrt{-3D}} \\ B &= \sqrt[3]{\tfrac{-27}{2}b - \tfrac{3}{2}\sqrt{-3D}} \\ D &= -4a^3 - 27b^2 \end{aligned}$$

This solution became known as *Cardano's formula*.

A simple change of variable can transform any cubic equation into a depressed one, hence Cardano's formula can be used to solve any cubic equation.

Exercise 7.8.1. Show that the change of variable $y = x + (a/3)$ transforms the general cubic equation

$$x^3 + ax^2 + bx + c = 0$$

into a depressed cubic. Therefore, Cardano's formula is useful to solve any cubic equation.

radical extension
radical tower
root extension
solvable by radicals
Galois cyclic

Note that Cardano's formula involves only the equation's coefficients, field constants and operations, and (repeated) taking of radicals. So it shows that any cubic equation can be solved by radicals.

With these two examples in mind, we can now proceed to the appropriate definition.

Definition 7.8.1. 1. A field extension of the form $F(\alpha)/F$ where α is a root of a polynomial $x^n - a \in F[x]$ for some $a \in F$, is called a *radical extension*.

2. A tower of fields $E = F_l/F_{l-1}/\ldots/F_1/F_0 = F$ is called a *radical tower* if each F_i is a radical extension of F_{i-1}, i.e. $F_i = F_{i-1}(\alpha_i)$ where α_i is a root of a polynomial of the form $x^{n_i} - a_i$ where $a_i \in F_{i-1}$. In other words, any element of F_i can be obtained from elements of F_{i-1}, using field operations, and an n-th root of a_i. The extension E/F is called a *root extension*.

3. A polynomial $f(x) \in F[x]$ is said to be *solvable by radicals* if all its roots, and hence its splitting field, can be included in a root extension.

Remark 7.8.1. 1. Note that any quadratic extension is a radical extension.

2. Corollary 7.6.2 tells us that the radical extension $F(\alpha)/F$ with $\alpha = \sqrt[n]{a}$ i.e. a root of $x^n - a \in F[x]$, is a Galois extension with cyclic Galois group provided $\xi_n \in F$. We call such extension a *Galois cyclic* extension.

3. To say that E/F is a root extension means that there are $\alpha_1, \ldots, \alpha_l \in E$ and $n_1, \ldots, n_l \in \mathbb{N}$, such that $E = F(\alpha_1, \ldots, \alpha_l)$, with $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$.

4. Every root extension is a finite extension.

Theorem 7.8.1 *Let F be a field of characteristic zero, and $f(x) \in F[x]$. If $f(x)$ is solvable by radicals, then its Galois group is solvable.*

In order to prove this theorem we will need the following lemmas. 05/07/19

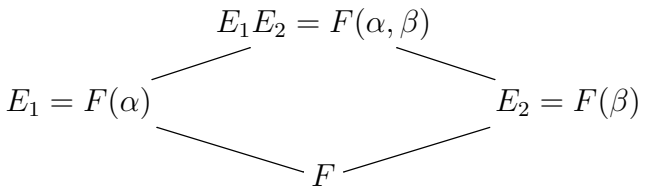
Lemma 7.8.2 *1. Let E_1/F and E_2/F be isomorphic as F-extensions. E_1/F is a root extension iff E_2/F is also a root extension.*

2. *Let E_1/F and E_2/F be finite F-extensions, and E_1E_2 their join, say inside an algebraic closure of F.*

$$[E_1E_2 : E_2] \leq [E_1 : F] \text{ and } [E_1E_2 : E_1] \leq [E_2 : F]$$

3. *Let E/F be a field extension, and $\alpha, \beta \in E$ be such that $F(\alpha)/F$ and $F(\beta)/F$ are roots extensions. Then $F(\alpha, \beta)/F$ is also a root extension.*

Proof. (1) This is obvious.
(2) Since we are working in characteristic zero, by the PET, there are α, β such that $E_1 = F(\alpha)$ and $E_2 = F(\beta)$. Note that $E_1E_2 = F(\alpha, \beta)$.



Let $p(x) = \min_F(\alpha)$. Then $\min_{F(\beta)}(\alpha)$ is a factor of $p(x)$, and therefore

$$\begin{array}{rcl} [E_1E_2 : E_2] = [F(\alpha, \beta) : F(\beta)] & = & \deg(\min_{F(\beta)}(\alpha)) \\ & \leq & \deg(p(x)) \\ & = & [F(\alpha) : F] = [E_1 : F]. \end{array}$$

The other inequality is similar.
(3) By assumption there are $\alpha_1, \ldots, \alpha_k$ and $n_1, \ldots, n_k \in \mathbb{N}$ such that $F(\alpha) = F(\alpha_1, \ldots, \alpha_k)$ and $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$. Similarly there are $\beta_1, \ldots, \beta_l$ and $m_1, \ldots, m_l \in \mathbb{N}$ such that $F(\beta) = F(\beta_1, \ldots, \beta_l)$ and $\beta_i^{m_i} \in F(\beta_1, \ldots, \beta_{i-1})$. Note then that $F(\alpha, \beta) = F(\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l)$ showing that $F(\alpha, \beta)/F$ is also a root extension. ■

The next lemma tells us that any root extension can be embedded in a Galois root extension with some extra features.

Lemma 7.8.3 1. *Let E/F be a root extension. There is a Galois root extension L/F such that $E \leq L$.*

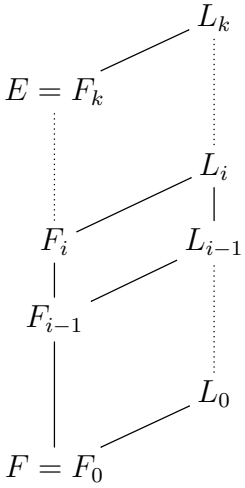
2. *Let E/F be a Galois root extension. There is a Galois root extension L/F, with radical tower $L = L_k/L_{k-1}/\cdots/L_1/L_0/F$ such that*

- $E \leq L$,
- *for each* $i > 0$, *and* $n_i = [L_i : L_{i-1}]$, *we have* $\xi_{n_i} \in L_1$.

Proof. (1) Note first that E/F is a separable finite extension, so by the Primitive Element Theorem there is $\alpha \in E$ such that $E = F(\alpha)$. Let $p(x) = \min_F(\alpha)$ be the minimal polynomial of α over F, and L the splitting field of $p(x)$. We clearly have that L/F is a Galois extension and $E \leq L$. Let $G = \mathrm{Gal}(L/F) = \{\gamma_1, \ldots, \gamma_n\}$, with $\gamma_1 = 1$. Let $\alpha_i = \gamma_i(\alpha)$, so $\alpha_1 = \alpha$, and $E_i = \gamma_i(E) = F(\alpha_i)$, so $E_1 = E$. For each root of $p(x)$ there is $\gamma_i \in G$ such that $\gamma_i(\alpha)$ equals that root, so the list $\alpha_1, \ldots, \alpha_n$ contains all the roots of $p(x)$, maybe with repetitions. Therefore $L = F(\alpha_1, \ldots, \alpha_n)$. Each E_i/F is isomorphic to E/F, via γ_i, so by Lemma 7.8.2.1, it is a root extension, and repeated application of Lemma 7.8.2.3 gives that L/F is a root extension.

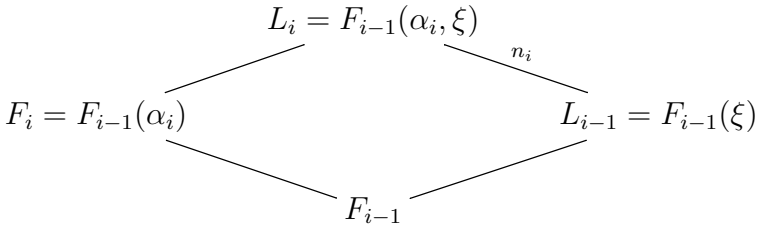
(2) Since E/F is a root extension, there is an extension tower

$$E = F_k/F_{k-1}/\ldots/F_1/F_0 = F \text{ with } F_i = F_{i-1}(\alpha_i),$$



where each α_i is a root of $x^{m_i} - a_i \in F_{i-1}[x]$, $a_i \in F_{i-1}$. Let $n = ([E : F])!$, and $\xi = \xi_n$ a primitive n-th root of unity. Let $L_i = F_i(\xi)$, so that $L_0 = F(\xi)$. Note that

$$L_i = F_i(\xi) = F_{i-1}(\alpha_i, \xi) = L_{i-1}(\alpha_i)$$



and $a_i \in F_{i-1} \leq L_{i-1}$, so L_i/L_{i-1} is a radical extension. By Lemma 7.8.2.2,

$$n_i = [L_i : L_{i-1}] \leq [F_i : F_{i-1}] \leq [E : F]$$

so $n_i | n$. Therefore $\xi^{n/n_i} \in L_0$ is a primitive n_i-th root of unity. Since E/F is a Galois extension, E is the splitting field of a polynomial $f(x) \in F[x]$. Then L is the splitting field of the polynomial $f(x)(x^n - 1) \in F[x]$, so L/F is also Galois. ∎

enough roots of unity

Remark 7.8.2. 1. The $n = ([E : F])!$ used in the proof of part 2 is an overkill, as all we need is n to be a multiple of each n_i. A more delicate analysis could be used to show that in fact taking $L = E$ works.

2. Note that the second property in part 2, together with Corollary 7.6.2, yield that L_i/L_{i-1} is a cyclic Galois extension. We'll refer to this1 by saying that L_0 contains *enough roots of unity*.

05/08/19

Board presentations PS 09

05/10/19

Proof. [Proof of Theorem 7.8.1] Assume $f(x) \in F[x]$ is solvable by radicals. Let K be the splitting field of $f(x)$ over F. Hence, K/F is normal. It is separable since we are working in characteristic zero. We want to show that $\mathrm{Gal}_F(K)$ is a solvable group. Let E be a root extension of F such that $f(x)$ splits in E, i.e. $K \leq E$. Combining both parts of Lemma 7.8.3, there is a Galois root extension L of F, with radical tower $L = L_k/L_{k-1}/\cdots/L_1/L_0/F$ such that L_0 contains enough roots of unity. Let $G = \mathrm{Gal}_F(L)$. By Proposition 7.4.8, L/L_i is a Galois extension. Let $H_i = \mathrm{Gal}_{L_i}(L)$. By Corollary 7.6.2 L_i/L_{i-1} is Galois cyclic, and since L/F is Galois, by the FTGT, Theorem 7.4.10.4, we get $H_i \trianglelefteq H_{i-1}$ and $H_{i-1}/H_i \approx \mathrm{Gal}_{L_{i-1}}(L_i)$ is cyclic, hence

$$1 = H_k \trianglelefteq H_{k-1} \cdots H_i \trianglelefteq H_{i-1} \cdots H_0 \trianglelefteq G$$

is an abelian series for G, and G is solvable. Now consider the tower $L/K/F$. Once again, using the FTGT, Theorem 7.4.10.4, we get that $\mathrm{Gal}_F(K)$ is a quotient of $G = \mathrm{Gal}_F(L)$. By Theorem 7.7.3, $\mathrm{Gal}_F(K)$ is solvable. ■

The converse of Theorem 7.8.1 is also true, but we will not prove it here.

Corollary 7.8.4 *There is no general solution by radicals for the quintic equation.*

Proof. It suffice to show one quintic polynomial that is not solvable by radicals. The polynomial $x^5 - 20x + 6 \in \mathbb{Q}[x]$ from Example 7.4.3.4, has Galois group isomorphic to S_5. S_5 is not solvable since it has a non-solvable subgroup, namely A_5. Therefore $x^5 - 20x + 6 = 0$ is not solvable by radicals. ■

Exercise 7.8.2. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5, which has only one real root. show that the Galois group of $f(x)$ contains a subgroup isomorphic to D_5.