19. Abelian Galois groups.

In this section, we will study the Galois group of some very well behaved polynomials f(X), and conclude that their Galois groups are Abelian. The first interesting case, we leave to the reader in the next set of exercises.

(19.1) Exercises: Let K be the splitting field for $X^k - 1$ over F. Let ω be a primitive k-th root of unity.

a) Show that $K = F[\omega]$.

b) Let $\Theta \in G(K/F)$. Show that Θ is determined by what it does to ω. That is, if Θ and ϕ are both in G(K/F), and if $\Theta(\omega) = \phi(\omega)$, then $\Theta = \phi$.

c) Show that G(K/F) is Abelian. (Hint: If $\Theta \in G(K/F)$, then $\Theta(\omega)$ is a root of $X^k - 1$, and so is just some power of ω.)

d) If $\Theta \in G(K/F)$, show that $\Theta(\omega)$ is a primitive k-th root of unity.

e) Argue that G(K/F) can be indentified with a subgroup of the group of permutations of the primitive k-th roots of unity.

(19.2) Theorem: Let k be a positive integer, and suppose that F contains all of the k-th roots of unity. Let $a_1, a_2, \ldots, a_m$ be elements of F, and let K be the splitting field of $f(X) = (X^k - a_1)(X^k - a_2) \ldots (X^k - a_m)$ over F. Then G(K/F) is Abelian.

Proof: For $1 \leq i \leq m$, let α_i be any root of $X^k - a_i$. Also, let ω be a primitive k-th root of unity. Thus α_i, $\alpha_i\omega$, $\alpha_i\omega^2$, ..., $\alpha_i\omega^{k-1}$ are all of the roots of $X^k - a_i$, and so we see that $K = F[\alpha_1, ..., \alpha_m]$ (since $\omega \in F$). If $\Theta \in G(K/F)$, then Θ is determined by the values of $\Theta(\alpha_1)$, ..., $\Theta(\alpha_m)$. (Note that $\Theta(\omega) = \omega$, since $\omega \in F$.) Of course $\Theta(\alpha_i)$ must be a root of $X^k - a_i$, and so $\Theta(\alpha_i) = \alpha_i\omega^{n(i)}$ for some positive integer n(i) depending on i. If also $\phi \in G(K/F)$, then similarly $\phi(\alpha_i) = \alpha\omega_i^{m(i)}$ for some m(i). In order to show that $\Theta\phi = \phi\Theta$, it will suffice to show that $\Theta\phi(\alpha_i) = \phi\Theta(\alpha_i)$ for all $1 \leq i \leq m$ We have $\Theta\phi(\alpha_i) = \Theta(\alpha_i\omega^{m(i)}) = \Theta(\alpha_i)\Theta(\omega^{m(i)}) = \Theta(\alpha_i)\omega^{m(i)} = \alpha_i\omega^{n(i)}\omega^{m(i)} = \alpha_i\omega^{m(i)}\omega^{n(i)} = \phi(\alpha_i)\omega^{n(i)} = \phi(\alpha_i)\phi(\omega^{n(i)}) = \phi(\alpha_i\omega^{n(i)}) = \phi\Theta(\alpha_i)$. Thus $\Theta\phi = \phi\Theta$, and so G(K/F) is Abelian.

20. Solvable Galois groups

(20.1) Lemma: Let $F \subseteq E \subseteq L$ be fields, with E/F Galois, and G(E/F) Abelian. Then for all Θ and ϕ in G(L/F), $\Theta\phi\Theta^{-1}\phi^{-1}$ is in G(L/E). (Recall that Exercise (18.2) shows that $G(L/E) \lhd G(L/F)$.)

Proof: Since Θ and ϕ are automorphisms of L, so is $\Theta\phi\Theta^{-1}\phi^{-1}$. Therefore, to show that $\Theta\phi\Theta^{-1}\phi^{-1} \in G(L/E)$, we must only show that $\Theta\phi\Theta^{-1}\phi^{-1}$ restricted to E is the identity on E. By Theorem (12.4), $\Theta|E$ and $\phi|E$ are both in G(E/F). We now easily see that $(\Theta\phi\Theta^{-1}\phi^{-1})|E = (\Theta|E)(\phi|E)(\Theta|E)^{-1}(\phi|E)^{-1}$. However, since G(E/F) is

Abelian, $(\Theta|E)(\phi|E)(\Theta|E)^{-1}(\phi|E)^{-1}$ equals I, the identity on E. Thus $(\Theta\phi\Theta^{-1}\phi^{-1})|E$ is the identity on E, as desired.

(20.2) Theorem: Let $F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ be fields. Suppose for each $1 \leq i \leq n$, that K_i/K_{i-1} is Galois, and $G(K_i/K_{i-1})$ is Abelian. Then $G(K_n/F)$ is solvable.

Proof: We have a sequence of subgroups
$(I) = G(K_n/K_n) < G(K_n/K_{n-1}) < \ldots < G(K_n/K_1) < G(K_n/K_0) = G(K_n/F)$.
We claim that this sequence satisfies the condition needed to show that $G(K_n/F)$ is solvable. Thus, we must show for any $1 \leq i \leq n$, and any Θ and ϕ in $G(K_n/K_{i-1})$, that $\Theta\phi\Theta^{-1}\phi^{-1} \in G(K_n/K_i)$. Consider $K_{i-1} \subseteq K_i \subseteq K_n$. We are told that K_i/K_{i-1} is Galois and $G(K_i/K_{i-1})$ is Abelian. Therefore, Lemma (20.1) (with $F = K_{i-1}$, $E = K_i$, and $L = K_n$) shows that $\Theta\phi\Theta^{-1}\phi^{-1} \in G(K_n/K_i)$, as desired.

Remark: Actually, the hypothesis of Theorem (20.2) can be weakened slightly. We do not really need K_n/K_{n-1} to be Galois, as a careful examination of the proof reveals.

Example: Let ω be a primitive 6-th root of unity. We will show that $G(\mathbb{Q}[\omega, \sqrt[3]{2}, \sqrt{1+\sqrt[3]{2}}]/\mathbb{Q})$ is solvable. Consider $\mathbb{Q} = K_0 < \mathbb{Q}[\omega] = K_1 < \mathbb{Q}[\omega, \sqrt[3]{2}] = K_2 < \mathbb{Q}[\omega, \sqrt[3]{2}, \sqrt{1+\sqrt[3]{2}}] = K_3$. We will show that the hypotheses of Theorem (20.2) are satisfied. First note that $K_1 = \mathbb{Q}[\omega]$ is the splitting field of

$X^6 - 1$ over $\mathbf{Q}$, so that $K_1/K_0 = \mathbf{Q}[\omega]/\mathbf{Q}$ is Galois. Also, Exercise (19.1)(c) shows that $G(K_1/K_0) = G(\mathbf{Q}[\omega]/\mathbf{Q})$ is Abelian. Next note that K_2 contains $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega^2$, and $\sqrt[3]{2}\,\omega^4$, which are all of the roots of $X^3 - 2$. We easily see that K_2 is the splitting field of this polynomial over K_1, so that K_2/K_1 is Galois. Since $\omega \in K_1$, we have that K_1 contains 1, ω^2, and ω^4, which are all of the cube roots of unity. By Theorem (19.2), $G(K_2/K_1)$ is Abelian. Next, note that K_3 contains $\sqrt{1+\sqrt[3]{2}}$ and $\sqrt{1+\sqrt[3]{2}}\,\omega^3$, which are all of the roots of the polynomial $X^2 - (1+\sqrt[3]{2}) \in K_2[X]$. We see that K_3 is the splitting field of this polynomial over K_2, so that K_3/K_2 is Galois. Also, K_2 contains 1 and ω^3 which are all of the square roots of unity. By Theorem (19.2), $G(K_3/K_2)$ is Abelian. By Theorem (20.2), $G(\mathbf{Q}[\omega, \sqrt[3]{2}, \sqrt{1+\sqrt[3]{2}}]/\mathbf{Q}) = G(K_3/\mathbf{Q})$ is solvable.

(20.3) Exercise: Let ω be a primitive 21-th root of unity. Show that $G(\mathbf{Q}[\omega, \sqrt[3]{5}, \sqrt[7]{2 + 4(\sqrt[3]{5}) + 3(\sqrt[3]{5})^2}]/\mathbf{Q})$ is solvable.

(20.4) Exercise: Let $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$ be a root tower. Show that there is a positive integer k such that $G(F_n[\omega]/F)$ is solvable, where ω is a k-th root of unity. (This result has a weakness. It may not be true that $F_n[\omega]/F$ is Galois. In Theorem (22.2), we will give a result which overcomes that weakness.)

(20.5) Theorem. Suppose $F \subseteq E \subseteq L$ with E/F and L/F both Galois, and with G(L/F) solvable. Then G(E/F) is solvable.

Proof: Since G(L/F) is solvable, there is a sequence of subgroups $\{I\} = H_0 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_m = G(L/F)$, such that for any $1 \leq i \leq m$, and any Θ and ϕ in H_i, $\Theta\phi\Theta^{-1}\phi^{-1} \in H_{i-1}$. We will use this sequence to build a sequence of subgroups of G(E/F). Pick $\Theta \in G(L/F)$. Since E/F is Galois, and Θ is an F-automorphism of L, by Theorem (12.4) we see that $\Theta|E$ is an F-automorphism of E. That is, for all $\Theta \in G(L/F)$, $\Theta|E \in G(E/F)$. For $0 \leq i \leq m$, we now define $G_i = \{\Theta|E \mid \Theta \in H_i\}$. We leave to the reader the very easy verification that since H_i is a subgroup of G(L/F), G_i is a subgroup of G(E/F). Notice that we have $\{I\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m \lhd G(E/F)$. In fact, we claim that $G_m = G(E/F)$. To see this, we must simply show that any automorphism in G(E/F) is the restriction to E of some automorphism in $H_m = G(L/F)$. However, Theorem (12.2) tells us that this is so. Therefore, we have $\{I\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_m = G(E/F)$. We claim that this sequence of subgroups satisfies the condition needed to show that G(E/F) is solvable. Thus, we must show for $1 \leq i \leq m$, and for σ and τ in G_i, that $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i-1}$. Since σ and τ are in G_i, by definition we have $\sigma = \Theta|E$ and $\tau = \phi|E$ for some Θ and ϕ in H_i. We already know that $\Theta\phi\Theta^{-1}\phi^{-1} \in H_{i-1}$. This shows that $(\Theta\phi\Theta^{-1}\phi^{-1})|E \in G_{i-1}$. However, $\sigma\tau\sigma^{-1}\tau^{-1} = (\Theta|E)(\phi|E)(\Theta|E)^{-1}(\phi|E)^{-1} = (\Theta\phi\Theta^{-1}\phi^{-1})|E \in G_{i-1}$, and we are done.

21. Fixed fields, I

We have seen throughout these notes that Galois extensions have many nice properties. In this section, we shall discuss one of their nicest properties.

Definition: Let $F \subseteq K$ be fields, and let H be a subgroup of $G(K/F)$. We define $F(H) = \{x \in K \mid \Theta(x) = x \text{ for all } \Theta \in H\}$. $F(H)$ is called the fixed field of H.

Remark: We will primarily be concerned with the case that $H = G(K/F)$.

(21.1) Exercises: a) Show that $F \subseteq F(G(K/F)) \subseteq K$.
b) Show that if $H_1 < H_2$ are subgroups of $G(K/F)$, then $F(H_2) \subseteq F(H_1)$.

Example: Consider $\mathbb{Q} \subseteq \mathbb{Q}[i]$, and let $H = G(\mathbb{Q}[i]/\mathbb{Q})$. We know by an example in section 18 that $G(\mathbb{Q}[i]/\mathbb{Q})$ contains just two automorphisms, the identity automorphism, and conjugation (restricted to $\mathbb{Q}[i]$). For $a + bi \in \mathbb{Q}[i]$ (with $a,b \in \mathbb{Q}$), we see that $a + bi$ will be in $F(G(\mathbb{Q}[i]/\mathbb{Q}))$ if and only if $a + bi$ is fixed by these two automorphisms. Now the identity automorphism fixes everything. Thus, $a + bi$ will be in $F(G(\mathbb{Q}[i]/\mathbb{Q}))$ exactly when it is fixed by conjugation, i.e., exactly when $a + bi = a - bi$. This occurs exactly when $b = 0$. Thus, $F(G(\mathbb{Q}[i]/\mathbb{Q})) = \mathbb{Q}$.

The next clever theorem shows a very important fact about Galois extensions.

(21.2) Theorem: Let $F \subseteq K$ be fields. If K/F is Galois, then $F(G(K/F)) = F$.

Proof: Say K is the splitting field of $f(X) \in F[X]$, and that the roots of $f(X)$ are $\alpha_1, \ldots, \alpha_m$, so that $K = F[\alpha_1, \ldots, \alpha_m]$. Since Exercise (21.1) gives $F \subseteq F(G/F))$, we need $F(G(K/F)) \subseteq F$. Let $\beta \in F(G(K/F))$. We must show that $\beta \in F$. To do this, we will let $\alpha_0 = 1$, and then show that for each $1 \leq i \leq m$, if $\beta \in F[\alpha_0, \alpha_1, \ldots, \alpha_i]$, then $\beta \in F[\alpha_0, \alpha_1, \ldots, \alpha_{i-1}]$. Since we have $\beta \in K = F[\alpha_0, \alpha_1, \ldots, \alpha_n]$, n iterations of this argument will show that $\beta \in F[\alpha_0] = F$, as desired.

Suppose that $\beta \in F[\alpha_0, \alpha_1, \ldots, \alpha_i]$. We want to show that $\beta \in F[\alpha_0, \alpha_1, \ldots, \alpha_{i-1}]$. Let $L = F[\alpha_0, \alpha_1, \ldots, \alpha_{i-1}]$. Thus, we have $\beta \in L[\alpha_i]$, and want $\beta \in L$.

Since $f(X) \in F[X] \subseteq L[X]$, and α_i is a root of $f(X)$, we see that α_i is algebraic over L, and so α_i has a minimal polynomial over L. Call that minimal polynomial $g(X)$. By Exercise (8.2)(c) $g(X)$ divides $f(X)$ in $L[X]$. Thus every root of $g(X)$ is also a root of $f(X)$, and so is in K. By Theorem (8.7), since $\beta \in L[\alpha_i]$, we may write $\beta = a_0 + a_1\alpha_i + a_2\alpha_i^2 + \ldots + a_{n-1}\alpha_i^{n-1}$, with $n = \deg g(X)$, and with the coefficients in L. Now let $h(X) = a_{n-1}X^{n-1} + \ldots + a_1X + (a_0 - \beta)$. We will show that this polynomial has n distinct roots. Since its degree is less than n, it must be the zero polynomial, and in particular its constant

term is zero. Thus, β must equal $a_0 \in L$, which is what we want. An earlier equation already shows that $h(\alpha_i) = 0$, so α_i is a root of $h(X)$. Since K is the splitting field of $f(X)$ over F, clearly K is the splitting field of $f(X)$ over L, so that K/L is Galois. Now let $\gamma_1, \ldots, \gamma_n$ be the roots of $g(X)$. (We know that these are distinct by Theorem (7.10), and of course α_i is one of them. We already noted that they are in K.) Pick any $1 \leq k \leq n$. By Corollary (12.3), there is a $\Theta \in G(K/L)$ with $\Theta(\alpha_i) = \gamma_k$. Since $\beta \in F(G(K/F))$, and since Θ is clearly in $G(K/F)$, we have $\Theta(\beta) = \beta$. Thus Θ fixes all the coefficients of $h(X)$, and so $\Theta(h(X)) = h(X)$. Since α_i is a root of $h(X)$, so is $\Theta(\alpha_i) = \gamma_k$, by Theorem (10.10). This shows that $\gamma_1, \ldots, \gamma_n$ are n distinct roots of $h(X)$. Thus, as explained above, $\beta \in L$, as desired. Iterating the argument gives $\beta \in F$.

Remark: If $K = F[\gamma_1, \ldots, \gamma_m]$ with each γ_i algebraic over F, then the converse of Theorem (21.2) is also true. That is, $F(G(K/F)) = F$ implies K/F is Galois. As we do not need that direction to reach our main goal, we will put off its proof until a later section. For now, we will be content with an exercise.

(21.3) Exercise: Show that $F(G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) \neq \mathbb{Q}$.

Suppose that K/F is Galois, so that K is the splitting field of some polynomial $f(X) \in F[X]$ over F. If f(X) has m roots, then Theorem (18.5) shows that G(K/F) can be thought of as a subgroup of S_m. In particular, this shows that G(K/F) is finite. Let us write $G(K/F) = \{\Theta_1, \Theta_2, \ldots \Theta_r\}$.

Suppose $\phi \in G(K/F)$. Then since that group is closed under multiplication, each of $\phi\Theta_1, \phi\Theta_2, \ldots, \phi\Theta_r$ is in G(K/F). However, this last list of r products contains r distinct things, since if $\phi\Theta_i = \phi\Theta_j$, then multiplying on the left by ϕ^{-1} shows $\Theta_i = \Theta_j$. Therefore, we see $G(K/F) = \{\phi\Theta_1, \phi\Theta_2, \ldots, \phi\Theta_r\}$. This fact will be useful in the next proof (and is similarly used in many proofs involving finite groups).

(21.4) Corollary: Let K/F be Galois, and let $\alpha \in K$. Let k be any positive integer, and let $f(X) = \Pi(X^k - \Theta(\alpha))$ over all $\Theta \in G(K/F)$. Then $f(X) \in F[X]$.

Proof: We will show that if $\phi \in G(K/F)$, then $\phi(f(X)) = f(X)$. This will show that each coefficient of f(X) is fixed by each $\phi \in G(K/F)$. Thus, each coefficient of f(X) will be in F(G(K/F)). However, by Theorem (21.2), F(G(K/F)) = F. Thus, each coefficient of f(X) will be in F, so that f(X) will be in F[X], as desired. Therefore, we must only show that $\phi(f(X)) = f(X)$. Now $\phi(f(X)) = \Pi(X^k - \phi\Theta(\alpha))$ over all $\Theta \in G(K/F)$. However, as Θ varies through G(K/F), so does $\phi\Theta$ (as the previous comments show), and so $\Pi(X^k - \phi\Theta(\alpha)) = \Pi(X^k - \Theta(\alpha)) = f(X)$, and we are done.

Example. We know that $\mathbf{Q}[i]/\mathbf{Q}$ is Galois, and that $G(\mathbf{Q}[i]/\mathbf{Q})$ contains just two automorphisms I and conjugation. Thus for any $a + bi \in \mathbf{Q}[i]$, (with $a,b \in \mathbf{Q}$), this lemma says that $(X^k - (a+bi))(X^k - (\overline{a+bi}))$ is in $\mathbf{Q}[X]$. Note that $\overline{a+bi} = a-bi$, and $(X^k - (a+bi))(X^k - (a-bi)) = X^{2k} - 2aX^k + (a^2+b^2)$. As $2a$ and a^2+b^2 are in $\mathbf{Q}$, the lemma is directly verified in this case.

(21.5) Exercises: a) Let K/F be Galois, and let $\alpha \in K$. Suppose that $\{\Theta(\alpha) \mid \Theta \in G(E/F)\} = \{\alpha_1, \ldots, \alpha_m\}$. Show that α is a root of $(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_m) \in F[X]$, (so that α is algebraic over F), and this polynomial is in fact the minimal polynomial of α over F. (Note: $(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_m)$ may differ from $\Pi(X - \Theta(\alpha))$ over all $\Theta \in G(E/F)$, since it may happen that Θ and ϕ may be two different elements in $G(E/F)$, and yet have $\Theta(\alpha) = \phi(\alpha)$. We of course understand $\alpha_1, \ldots, \alpha_m$ to all be distinct.

b) Let β be algebraic over the field F. Show that any $\alpha \in F[\beta]$ is algebraic over F. (Hint: Let $f(X) \in F[X]$ be the minimal polynomial of β over F, and let K be the splitting field of $f(X)$ over F.)

(21.6) Exercise: Let k be a positive integer, and let $\omega_1, \omega_2, \ldots, \omega_m$ be all the primitive k-th roots of unity. Show that $(X - \omega_1)(X - \omega_2) \ldots (X - \omega_m) \in \mathbf{Q}$. (Hint: Let K be the splitting field of $X^k - 1$ over Q. Using Exercise (19.1)(d), show that if $\Theta \in G(K/\mathbf{Q})$, then Θ fixes $(X - \omega_1)(X - \omega_2) \ldots (X - \omega_m)$.)

Remark: The polynomial $(X - \omega_1)(X - \omega_2) \ldots (X - \omega_m)$, where $\omega_1, \ldots, \omega_m$ are all the primitive k-th roots of unity, is called the k-th cyclotonic polynomial. The preceding exercise shows that it is in $\mathbf{Q}[X]$. In fact, it is irreducible in $\mathbf{Q}[X]$, but the proof of that is a bit difficult. Being irreducible in $\mathbf{Q}[X]$, we see that it is the minimal polynomial of ω_1 over $\mathbf{Q}$.

22. Root towers revisited

(22.1) Lemma: Let $F \subseteq K \subseteq K[\alpha]$, with K/F is Galois. Suppose that $\alpha^k \in K$ for some positive integer k. Suppose also that K contains all the k-th roots of unity. Then there is a field K′ with $K[\alpha] \subseteq K'$, K′/F Galois, and G(K′/K) Abelian.

Proof: Suppose that $\alpha^k = a \in K$. By Corollary (21.4), if $f(X) = \Pi(X^k - \Theta(a))$ over all $\Theta \in G(K/F)$, then $f(X) \in F[X] \subseteq K[X]$. We let K′ be the splitting field of f(X) over K. Since the identity automorphism, I, is in G(K/F), and since I(a) = a, we see that $X^k - a$ is a factor of f(X), and so α is one of the roots of f(X). Thus K′ contains α, and so contains $K[\alpha]$, as desired. Since K contains all the k-th roots of unity, Theorem (19.2) shows that G(K′/K) is Abelian, as desired. It only remains to show that K′/F is Galois. We are told that K/F is Galois, and so K is the splitting field over F of some polynomial $g(X) \in F[X]$. Since $f(X) \in F[X]$, and K′ is the splitting field of f(X) over K, it is

an easy exercise to see that K' is the splitting field of $g(X)f(X)$ over F, and so K'/K is Galois, as desired.

(22.2) Theorem: Let $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$ be a root tower. Then there is a field L with $F_n \subseteq L$, L/F Galois, and $G(L/F)$ solvable.

Proof: We will build a sequence of fields $F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_{n+1}$, such that for $1 \leq i \leq n + 1$, $F_{i-1} \subseteq K_i$, K_i/F is Galois, and $G(K_i/K_{i-1})$ is Abelian. We will inductively construct these K_i.

Since $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$ is a root tower, for $1 \leq i \leq n$ we may write $F_i = F_{i-1}[\alpha_i]$ where ${\alpha_i}^{k_i} \in F_{i-1}$ for some positive integer k_i. Let $k = k_1 k_2 \ldots k_n$, and let ω be a primitive k-th root of unity. We let $K_0 = F$, and now construct K_1. We simply let K_1 be the splitting field of $X^k - 1$ over F. Thus K_1/F is Galois (as desired) and by Exercise (19.1)(c), $G(K_1/K_0) = G(K_1/F)$ is Abelian (as desired). Obviously $F_0 = F \subseteq K_1$ (as desired). Thus K_1 has been constructed, and satisfies the above properties. (Note that since $\omega \in K_1$ and ω is a primitive k-th root of unity, K_1 contains all of the k_i-th roots of unity for each of $k_1, k_2, \ldots, k_n$.)

Let us now suppose that $1 \leq m \leq n$, and that we have already constructed $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$ in such a way that for $1 \leq i \leq m$, K_i satisfies the above properties. We will now inductively construct K_{m+1}. Consider $F \subseteq K_m \subseteq K_m[\alpha_m]$. We

claim that this satisfies the hypotheses of Lemma (22.1). We have K_m/F Galois, as Lemma (22.1) requires. Also, we know that $F_{m-1} \subseteq K_m$, and that $\alpha_m{}^{k_m} \in F_{m-1}$. Thus, $\alpha_m{}^{k_m} \in K_m$, as Lemma (22.1) requires. Finally, since we already noted that K_1 contains all the k_m-th roots of unity, and since $K_1 \subseteq K_m$, we see that K_m contains all the k_m-th roots of unity, as Lemma (22.1) requires. Thus, the hypotheses of Lemma (22.1) are satisfied. That lemma now tells us that there is a field K' with $K_m[\alpha_m] \subseteq K'$, K'/F Galois, and $G(K'/K_m)$ Abelian. Note that since we already have $F_{m-1} \subseteq K_m$, we get $F_m = F_{m-1}[\alpha_m] \subseteq K_m[\alpha_m] \subseteq K'$. Therefore, if we let K_{m+1} be this K', then K_{m+1} satisfies the properties we seek. This concludes our construction of $F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_{n+1}$, such that for $1 \leq i \leq n+1$, $F_{i-1} \subseteq K_i$, K_i/F is Galois, and $G(K_i/K_{i-1})$ is Abelian.

We now let $L = K_{n+1}$, and claim that L satisfies the theorem we are currently proving. We already have $F_n \subseteq K_{n+1} = L$, as desired, and $L/F = K_{n+1}/F$ Galois, as desired. It only remains to show that G(L/F) is solvable. Since for $1 \leq i \leq n+1$, we know that K_i/F is Galois, Exercise (12.1)(a) shows that K_i/K_{i-1} is Galois. Thus Theorem (20.2) shows that $G(L/F) = G(K_{n+1}/F)$ is Galois.