30 Suppose you know that for integers a and n with $\gcd(a, n) = 1$, there are infinitely many primes p that are congruent to a modulo n. Conclude that every finite abelian group occurs as a Galois group over the rational numbers.

Solution Let $n \geq 1$. We will first show that if ζ_n is a primitive n-th root of unity, then $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$.

ζ_n generates the other primitive n-th roots of unity, which are the roots of the n-th cyclotomic polynomial, and these are all ζ_n^r such that $\gcd(r, n) = 1$. But these r are precisely the elements of $(\mathbb{Z}/n\mathbb{Z})^{\times}$, by definition.

Given an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, its action is completely determined by its action on ζ_n, which is $\sigma(\zeta_n) = \zeta_n^r$, for some r. Thus $\sigma \mapsto r$ is an isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^{\times}$: it is certainly injective because if $\sigma(\zeta_n) = \tau(\zeta_n)$, then their actions are identical. On the other hand, it is surjective as there are

$$\varphi(n) = |\{r \mid 0 \leq d < n,\ \gcd(d, n) = 1\}| = \left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right|$$

roots of unity, which means that $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})|$, and this proves the claim.

Now let G be a finite abelian group. By the structure theorem,

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z},$$

with $n_1 \mid n_2 \mid \cdots \mid n_m$. By Dirichlet's theorem, there are distinct primes $p_1, \ldots, p_m$ so that $p_k = 1 \mod n_k$. If ζ_{p_k} is a primitive p_k-th root of unity, then consider the field extension $\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}$.

By the first claim,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p_k})/\mathbb{Q}) \simeq (\mathbb{Z}/p_k\mathbb{Z})^{\times} \simeq \mathbb{Z}/(p_k - 1)\mathbb{Z}.$$

Since $n_k \mid p_k - 1$ by construction, it follows that $\mathbb{Z}/n_k\mathbb{Z} \leq \mathbb{Z}/(p_k - 1)\mathbb{Z} \simeq (\mathbb{Z}/p_k\mathbb{Z})^{\times}$.

By the Chinese remainder theorem, if $\mathbb{Q}(\zeta_n)$ is a primitive n-th root of unity, then

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\simeq (\mathbb{Z}/n\mathbb{Z})^{\times} \\
&\simeq (\mathbb{Z}/p_1\mathbb{Z})^{\times} \times \cdots \times (\mathbb{Z}/p_m\mathbb{Z})^{\times} \\
&\simeq \mathbb{Z}/(p_1 - 1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_m - 1)\mathbb{Z} \\
&\geq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z} \\
&\simeq G.
\end{aligned}$$

Thus, G is a subgroup of a Galois group, and so it is the Galois group of a subfield of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, by the Galois correspondence theorem.

31 Let $K = \mathbb{Q}(r)$ with r a root of $t^3 + t^2 - 2t - 1 \in \mathbb{Q}[t]$. Let $r_1 = r^2 - 2$. Show that r_1 is also a root of this polynomial. Find $\mathrm{Gal}(K/\mathbb{Q})$ and show that $K/\mathbb{Q}$ is normal.

Solution Notice that by direct calculation,

$$\begin{aligned} r_1^3 + r_1^2 - 2r_1 - 1 &= r^6 - 5r^4 + 6r^2 - 1 \\ &= (r^3 - r^2 - 2r + 1)(r^3 + r^2 - 2r - 1) = 0, \end{aligned}$$

as required.

Notice also that

$$r_1^2 - 2 = r^4 - 4r^2 + 2 = -r^3 - 2r^2 + r + 2 = -r^2 - r + 1 := r_2$$

and

$$r_2^2 - 2 = r^4 + 2r^3 - r^2 - 2r - 1 = r^3 + r^2 - r - 1 = r.$$

Thus, the three distinct roots of the polynomial f are given by r, $r^2 - 2$, and $\left(r^2 - 2\right)^2 - 2 = -r^2 - r + 1$, so all the roots are of f are in K, so K is the splitting field of f, and hence $K/\mathbb{Q}$ is normal.

By the rational root theorem, the only possible rational roots of f are 1 and -1, but neither of them are roots, so f is irreducible over $\mathbb{Q}$, since f would have to factor into a quadratic and a linear term. Thus, f is the minimal polynomial of r, so $3 = [K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})|$. Thus, $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, by Cauchy's theorem.

---

32 Let K be a splitting field of $t^5 - 2 \in \mathbb{Q}[t]$.

a. Find $\mathrm{Gal}(K/\mathbb{Q})$.

b. Show that there exists a group monomorphism $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow S_5$.

c. Find all subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the corresponding fields.

Solution a. The splitting field of $t^5 - 2$ is $\mathbb{Q}(\alpha, \zeta)$, where $\alpha = \sqrt[5]{2}$ and $\zeta = e^{2\pi i/5}$, since the roots of $t^5 - 2$ are $\alpha, \zeta\alpha, \ldots, \zeta^4\alpha$. The minimal polynomial of α is $t^5 - 2$, which is irreducible by Eisenstein, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. On the other hand, the minimal polynomial of ζ over $\mathbb{Q}$ is $(t^5 - 1)/(t - 1)$. Replacing t with $t + 1$, we get

$$\frac{\left(t+1\right)^5 - 1}{t} = t^4 + 5t^3 + 10t^2 + 10t + 5,$$

which is irreducible by Eisenstein with $p = 5$. The polynomial has degree 4, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

Since $\gcd(4, 5) = 1$, by Problem 2, $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 4 \cdot 5 = 20$. Since $t^5 - 2$ has no multiple roots, $|\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta))/\mathbb{Q}| = 20$.

Let

$$\sigma \colon \begin{cases} \alpha & \mapsto & \zeta\alpha \\ \zeta & \mapsto & \zeta \end{cases} \quad \text{and} \quad \tau \colon \begin{cases} \alpha & \mapsto & \alpha \\ \zeta & \mapsto & \zeta^2. \end{cases}$$

Then $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$. Notice that the order of σ is 5, since $\sigma^5(\alpha) = \zeta^5\alpha = \alpha$, and the order of τ is 4, since $\tau^2(\zeta) = \zeta^4$, $\tau^3(\zeta) = \zeta^8 = \zeta^3$, and $\tau^4(\zeta) = \zeta^{16} = \zeta$.

We have that $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$, since τ always fixes α and σ always fixes ζ. Thus, $|\langle\sigma\rangle \cap \langle\tau\rangle| = 1$ and so

$$|\langle\sigma, \tau\rangle| = |\langle\sigma\rangle||\langle\tau\rangle|/|\langle\sigma\rangle \cap \langle\tau\rangle| = 20 = |\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q})|,$$

which means that $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}) = \langle\sigma, \tau\rangle$.

b. Define $\varphi \colon \mathrm{Gal}(K/\mathbb{Q}) \to S_5$ via $\sigma \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \end{pmatrix}$ and $\tau \mapsto \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$, which are simply the representations of their action on α.

Notice that $\tau\sigma = \sigma^2\tau$, so to calculate the kernel of φ, we just need to look at what happens to $\sigma^a\tau^b$ when $0 \le a < 5$ and $0 \le b < 4$.

Now, suppose $\varphi(\sigma^a\tau^b) = \mathrm{id}$. 0 is only affected by σ^a, an in order to fix 0, we need $a = 0$, so we are left with $\varphi(\tau^b) = \mathrm{id}$. Similarly, we need $b = 0$ in order to fix 1, so $\sigma^a\tau^b = e$, which means that φ is a group monomorphism.

c. There are 12 subgroups, and hence 12 subfields. These subgroups are: $\langle\tau^2\rangle$, $\langle\sigma\tau^2\rangle$, $\langle\sigma^2\tau^2\rangle$, $\langle\sigma^3\tau^2\rangle$, $\langle\sigma^4\tau^2\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, $\langle\sigma^2\tau\rangle$, $\langle\sigma^3\tau\rangle$, $\langle\sigma^4\tau\rangle$, $\langle\sigma\rangle$, $\langle\sigma,\tau^2\rangle$. We will try to prove this.

Subgroups of order 2:

We just need to look for an element of order 2, which will be of the form $\sigma^a\tau^b$. Only τ operates on ζ, so to fix ζ, we need $2b = 4 \implies b = 2$. Then we check the remaining through brute force:

$$(\tau^2)^2 = \tau^4 = \mathrm{id}$$
$$(\sigma\tau^2)^2 = \sigma\tau^2\sigma\tau^2 = \sigma\tau\sigma^2\tau^3 = \sigma^3\tau\sigma\tau^3 = \sigma^5\tau^4 = \mathrm{id}$$
$$\vdots$$

---

34 Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, u)$, where $u^2 = (9-5\sqrt{3})(2-\sqrt{2})$. Show that $K/\mathbb{Q}$ is normal and find $\mathrm{Gal}(K/\mathbb{Q})$.

Solution We first show that $u \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ be the automorphism which sends $\sqrt{2} \mapsto -\sqrt{2}$. Then

$$\frac{\sigma(u^2)}{u^2} = \frac{2+\sqrt{2}}{2-\sqrt{2}} = \frac{(2+\sqrt{2})^2}{2}$$

Thus, if $u \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $\sigma(u) = \pm u(2+\sqrt{2})/\sqrt{2}$. But then

$$\sigma^2(u) = \mp\sigma(u)\frac{2-\sqrt{2}}{\sqrt{2}} = -u\frac{(2+\sqrt{2})(2-\sqrt{2})}{2} = -u,$$

but σ had order 2 in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. Thus, $u \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This also shows that $\left[K : \mathbb{Q}(\sqrt{2}, \sqrt{3})\right] = 2$, since $t^2 - u^2$ is the minimal polynomial of u.

Consider the polynomial

$$f(t) = (t^2 - (9-5\sqrt{3})(2-\sqrt{2}))(t^2 - (9-5\sqrt{3})(2+\sqrt{2}))(t^2 - (9+5\sqrt{3})(2-\sqrt{2}))(t^2 - (9+5\sqrt{3})(2+\sqrt{2})).$$

By WolframAlpha,

$$f(t) = t^8 - 72^6 + 720t^4 - 864t^2 + 144,$$

and $f(u) = 0$, by definition of u.

Let L be its splitting field over F. We claim that $L = K$.

By some algebra,

$$(9-5\sqrt{3})(2-\sqrt{2}) = 18 - 9\sqrt{2} - 10\sqrt{3} + 5\sqrt{6} \qquad (1)$$
$$(9+5\sqrt{3})(2-\sqrt{2}) = 18 - 9\sqrt{2} + 10\sqrt{3} - 5\sqrt{6} \qquad (2)$$
$$(9+5\sqrt{3})(2+\sqrt{2}) = 18 + 9\sqrt{2} - 10\sqrt{3} - 5\sqrt{6} \qquad (3)$$

Then $(1) + (2) = 36 - 18\sqrt{2}$ and $(1) + (3) = 36 - 20\sqrt{3}$, and $u \in L$ by definition, so $L \geq K$.

Next, notice that by a previous problem $\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right] = 4$. Also, $m_{\mathbb{Q}(\sqrt{2},\sqrt{3})}(u) = t^2 - (9-5\sqrt{3})(2-\sqrt{2})$; it is irreducible since $u \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus, $\left[K : \mathbb{Q}(\sqrt{2}, \sqrt{3})\right] = 2$, and so

$$[K : \mathbb{Q}] = \left[K : \mathbb{Q}(\sqrt{2}, \sqrt{3})\right]\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\right] = 2 \cdot 4 = 8.$$

On the other hand, f is irreducible, $L/\mathbb{Q}$ has degree 8 and so $L = K$. Since L was a splitting field, it is normal.

Consider the automorphisms $\sigma\colon \sqrt{2} \mapsto -\sqrt{2}$ and $\tau\colon \sqrt{3} \mapsto -\sqrt{3}$. We claim that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{H}$, the quaternions.

From the first calculation, we see that

$$\sigma^4(u) = (-u)^2 = u,$$

so σ has order 4. Similarly,

$$\frac{\tau(u^2)}{u^2} = \frac{9+5\sqrt{3}}{9-5\sqrt{3}} = \frac{(9+5\sqrt{3})^2}{6} \implies \tau(u) = \pm u \frac{9+5\sqrt{3}}{\sqrt{2}\sqrt{3}} \implies \tau^2(u) = -u.$$

Thus, $\sigma^2 = \tau^2 = \upsilon$ and σ and τ have order 4, so $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{H}$.

---

35 Let $F \subseteq E \subseteq K$. If K/E and E/F are both normal, is K/F normal? Prove or give a counterexample.

Solution Consider the tower:

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ \mid 2 \\ \mathbb{Q}(\sqrt{2}) \\ \mid 2 \\ \mathbb{Q} \end{array}$$

$\mathbb{Q}(\sqrt{2})$ is the splitting field of x^2-2 over $\mathbb{Q}$, so it is a normal extension of $\mathbb{Q}$ of degree 2, since x^2-2 is irreducible by Eisenstein. Similarly, $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field of $x^2-\sqrt{2}$, so it is a normal extension of $\mathbb{Q}(\sqrt{2})$. $\{1, \sqrt[4]{2}\}$ is a basis for this extension. It is certainly linearly independent, since $\sqrt[4]{2}$ is not a power of $\sqrt{2}$, and they span by definition. Thus, this extension has degree 2 also. Thus,

$$\left[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})\right]\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 4$$

Thus, $\sqrt[4]{2}$ is a root of x^4-2 which lies in $\mathbb{Q}(\sqrt[4]{2})$. But by Problem 10(c), a splitting field of this polynomial has degree 8, which means that x^4-2 cannot split in $\mathbb{Q}(\sqrt[4]{2})$, so the extension is not normal over $\mathbb{Q}$.

---

37 Suppose that K/F is Galois with Galois group $\mathrm{Gal}(K/F) \simeq S_n$. Show that K is the splitting field of an irreducible polynomial in $F[t]$ of degree n over F.

Solution Let $S_{n-1} \simeq G_i \leq S_n$ be the subgroup of S_n which fixes i. By the Galois correspondence theorem, G_i fixes a subfield $F_i \leq K$. Moreover, we have that $[F_i : F] = [\mathrm{Gal}(K/F) : \mathrm{Gal}(K/F_i)] = [S_n : S_{n-1}] = n$.

Because K/F is separable, F_i/F is separable also, so by the primitive element theorem, there exists $\alpha_1 \in F_1$ so that $F_1 = F(\alpha_1)$. Now let Then the stabilizer of α_i is precisely G_i: It's clear that $\mathrm{stab}(\alpha_i) \supseteq G_i$, since G_i fixes $F_i \ni \alpha_i$. Conversely, if $\sigma \in S_n$ fixes α_i, then σ fixes F_i, and so $\sigma \in G_i$, by the Galois correspondence theorem.

Now, consider $F(\alpha_1, \ldots, \alpha_n)$, which is a subfield of K. By the Galois correspondence theorem again, $F(\alpha_1, \ldots, \alpha_n)$ corresponds to a subgroup G of S_n. G must fix $\alpha_1, \ldots, \alpha_n$, so

$$G \subseteq \bigcap_{i=1}^{n} \mathrm{stab}(\alpha_i) = \bigcap_{i=1}^{n} G_i = \{e\},$$

since the only permutation which fixes every element in S_n is the identity. Thus, G fixes every element in K, which means that $K = F(\alpha_1, \ldots, \alpha_n)$.

Lastly, note that $m_F(\alpha_1)$ has degree n since $[F_i : F] = n$. If $\sigma \colon \alpha_1 \mapsto \alpha_i$, then

$$\sigma(m_F(\alpha_1)(\alpha_1)) = m_F(\alpha_1)(\alpha_i) = 0,$$

which means that the n roots of $m_F(\alpha_1)$ are precisely $\alpha_1, \ldots, \alpha_n$. Thus, K is precisely the splitting field of $m_F(\alpha_1)$, which is irreducible by definition, and has degree n.

38 Let K be a splitting field of $f \in \mathbb{Q}[t]$. Find K, $\operatorname{Gal}(K/F)$ and all intermediate fields if:

a. $f = t^4 - t^2 - 6$.

b. $f = t^3 - 3$.

Solution a. We can factor the polynomial as $(t^2-3)(t^2+2)$. Thus, $K = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$. $t^2 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein, so it is the minimal polynomial of $\sqrt{3}$ and hence $\left[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}\right] = 2$. $t^2 + 2$ is still irreducible over $\mathbb{Q}(\sqrt{3})$, since $i\sqrt{2} \in \mathbb{C}$, so $\left[\mathbb{Q}(\sqrt{3}, i\sqrt{2}) : \mathbb{Q}(\sqrt{3})\right] = 2$. Thus, $[K : F] = 4$, and because f has no repeated roots, $|\operatorname{Gal}(K/F)| = 4$.

If $\sigma\colon i\sqrt{2} \mapsto -i\sqrt{2}$ and $\tau\colon \sqrt{3} \mapsto -\sqrt{3}$, then $\operatorname{Gal}(K/F) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$.

The subgroups of $\operatorname{Gal}(K/F)$ are $\{\mathrm{id}, \sigma\}$, $\{\mathrm{id}, \tau\}$, $\{\mathrm{id}, \sigma\tau\}$. These correspond to the subfields $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i\sqrt{2})$, and $\mathbb{Q}(i\sqrt{6})$, respectively.

b. By Eisenstein with $p = 3$, f is irreducible. If $\zeta = e^{2\pi i/3}$, then

$$\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{and} \quad \zeta^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2},$$

so the splitting field of f is $K = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$. We also have that $\left[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}\right] = 3$, since the minimal polynomial of $\sqrt[3]{3}$ is f. The minimal polynomial of $i\sqrt{3}$ is $t^2 + 3$, which is also irreducible by Eisenstein, so $\left[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}\right] = 2$. Since 3 and 2 are coprime, by Problem 2, $[K : F] = 3 \cdot 2 = 6$. f has no repeated roots, so $[K : F] = |\operatorname{Gal}(K/F)| = 6$.

Let $\sigma\colon \sqrt[3]{3} \mapsto \zeta\sqrt[3]{3}$ and $\tau\colon \zeta \mapsto \zeta^2$. Then the order of σ is 3 and the order of τ is 2, since $\sigma^3(\sqrt[3]{3}) = \zeta^3\sqrt[3]{3} = \sqrt[3]{3}$, and $\tau^2(\zeta) = \zeta^4 = \zeta$. Thus, $\operatorname{Gal}(K/F) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} \simeq S_3$.

Subgroups of order 2:

Here, the subgroups are $\{\mathrm{id}, \tau\}$, $\{\mathrm{id}, \sigma\tau\}$, and $\{\mathrm{id}, \sigma^2\tau\}$, by a simple check. These correspond to $\mathbb{Q}(\sqrt[3]{3})$, $\mathbb{Q}(\zeta\sqrt[3]{3})$, $\mathbb{Q}(\zeta^2\sqrt[3]{3})$, respectively.

Subgroups of order 3:

This is just $\{\mathrm{id}, \sigma, \sigma^2\}$, which corresponds to $\mathbb{Q}(\zeta)$.

There are no subgroups of order 4 or 5, since they don't divide 6, so these are all the non-trivial subfields.

---

39 Suppose that L/F is a finite Galois extension and $L/K/F$ an intermediate field. Show that $\operatorname{Gal}(K/F) = N_{\operatorname{Gal}(L/F)}(\operatorname{Gal}(L/K))/\operatorname{Gal}(L/K)$, where $N_{\operatorname{Gal}(L/F)}(\operatorname{Gal}(L/K))$ is the normalizer of $\operatorname{Gal}(L/K)$ in $\operatorname{Gal}(L/K)$.

Solution Define $\varphi\colon N_{\operatorname{Gal}(L/F)}(\operatorname{Gal}(L/K)) \to \operatorname{Gal}(K/F)$ as follows: $\sigma \mapsto \sigma|_K$.

This is well-defined: If σ fixes K, then $\sigma|_K$ certainly fixes F. Also, its kernel is

$$\ker\varphi = \{\sigma \mid \sigma|_K = \mathrm{id}\} = \operatorname{Gal} L/K.$$

Thus, if we can show that φ is onto, then we are done, by the first isomorphism theorem.

Let $\sigma \in \operatorname{Gal}(K/F)$. Because $L/K/F$ is finite, there exists $\alpha \in L$ so that $L = K(\alpha)$. If we write $x = a + b\alpha$ for $a, b \in K$, then set $\tau(x) = a + \sigma(b)\alpha$. This clearly defines a homomorphism on L which fixes K. Moreover, if $\upsilon \in \operatorname{Gal}(L/K)$, then $\tau\upsilon\tau^{-1}$ fixes $\tau(K) = K$, and so $\tau\upsilon\tau^{-1} \in \operatorname{Gal}(L/K)$ also. Thus, $\tau \in N_{\operatorname{Gal}(L/F)}(\operatorname{Gal}(L/K))$, and $\varphi(\tau) = \sigma$, by construction. Hence, φ is onto, as desired.

40 Suppose that K/F is Galois. Let $F \subseteq k \subseteq K$ and L be the smallest subfield of K containing k such that L/F is normal. Show that

$$\mathrm{Gal}(K/L) = \bigcap_{\sigma \in \mathrm{Gal}(K/F)} \sigma \, \mathrm{Gal}(K/k) \sigma^{-1}.$$

Solution Since L/F is normal, $\mathrm{Gal}(L/F)$ is a normal subgroup of $\mathrm{Gal}(K/F)$ by the Galois correspondence theorem. Since L is the smallest field of K containing k, $\mathrm{Gal}(L/F)$ is the largest subgroup containing $\mathrm{Gal}(K/k)$ as a normal subgroup, so $\mathrm{Gal}(L/F)$ is the normalizer of $\mathrm{Gal}(K/k)$ in $\mathrm{Gal}(K/F)$.

If we let G be the right-hand side, then

$$\begin{aligned} G &= \{\tau \in \mathrm{Gal}(K/F) \mid \sigma\tau\sigma^{-1} \in \mathrm{Gal}(K/F)\} \cap \bigcap_{\sigma \in \mathrm{Gal}(K/F)\setminus\{\mathrm{id}\}} \{\tau \in \mathrm{Gal}(K/F) \mid \sigma\tau\sigma^{-1} \in G\} \\ &= \{\tau \in \mathrm{Gal}(K/F) \mid \sigma\tau\sigma^{-1} \in \mathrm{Gal}(K/F) \ \forall \sigma \in \mathrm{Gal}(K/F)\} \\ &= N_{\mathrm{Gal}(K/F)}(\mathrm{Gal}(K/k)) \\ &= \mathrm{Gal}(K/L). \end{aligned}$$

---

41 Suppose that K/F is Galois and $p^r \mid [K:F]$, but $p^{r+1} \nmid [K:F]$. Show that there exist fields L_i, $1 \leq i \leq r$, satisfying $F \subseteq L_r < L_{r-1} < \cdots < L_1 < L_0 = K$ such that L_i/L_{i+1} is normal, $[L_i : L_{i+1}] = p$, and $p \nmid [L_r : F]$.

Solution Since K/F is Galois, $p^r \mid [K:F] = |\mathrm{Gal}(K/F)|$, so by repeated use of Cauchy's theorem, we get normal subgroups $\mathrm{Gal}(K/F) = G_0 > G_1 > \cdots > G_r = \{e\}$ with $|G_i| = p^{r-i}$. By the Galois correspondence theorem, these all correspond to subfields $F = L_r < \cdots < L_1 < L_0 = K$ with $\mathrm{Gal}(L_i/F) \simeq G_i$ and we also get

$$p = |G_i/G_{i+1}| = |\mathrm{Gal}(K/L_{i+1})/\mathrm{Gal}(K/L_i)| = [L_i : L_{i+1}].$$

p does not divide $[L_r : F] = |\mathrm{Gal}(L_r/F)| = |G_0| = 1$, by construction.

From group theory, p-subgroups of p-groups are normal, so $G_{i+1} \triangleleft G_i$ and hence by the fundamental theorem of Galois theorem, L_i/L_{i+1} is normal.

---

48 Let f be an irreducible quartic over a field K of characteristic zero, G the Galois group of f, and u a root of f. Show that there is no field properly between K and $K(u)$ if and only if $G = A_4$ or $G = S_4$.

Solution "$\Longleftarrow$"

Let $G = A_4$ or $G = S_4$.

Since f is irreducible, $[K(u) : K] = 4$. Thus, any field L with $K < L < K(u)$ must satisfy $[L : K] = 2$, by the dimension formula. Also, $L(u) = K(u)$: "$\subseteq$" comes from $L < K$, and "$\supseteq$" is clear.

By Galois correspondence, L/K is associated to a subgroup H of G, and $2 = [L : K] = [G : H]$. If $G = A_4$, then $H = 6$, but A_4 does not have a subgroup of order 6. On the other hand, if $G = S_4$, then $H = A_4$. Now consider $K(u)/L$, which has a subgroup H_1 of index 2 in $\mathrm{Gal}(K/L)$, by the same argument as the above. But this means that $H_1 \leq H = A_4$ and $|H_1| = 6$, which is impossible as before.

"$\Longrightarrow$"

Since f is irreducible, $G \leq S_4$ is a transitive group, and recall that the transitive subgroups of S_4 are S_4, A_4, D_4, $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Suppose $G \neq A_4$ and $G \neq S_4$. Since f is irreducible, $[K(u) : K] = 4$, so $|G| \geq 4$ and so $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or D_4. Moreover, by the Galois correspondence theorem, $K(u)/K$ is associated with a subgroup H of order 4.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ have order 4, which means that $K(u)$ would be the splitting field of f. But these both have $\mathbb{Z}/2\mathbb{Z}$ as a subgroup, which gives an intermediate field, which is impossible.

On the other hand, if $G = D_4$, then $H = \mathbb{Z}/4\mathbb{Z}$, which is impossible as before.

50 Let K/F be a finite extension. Suppose that F has no nontrivial extensions of odd degree and K has no extensions of degree two. Show that F is perfect and K is algebraically closed.

Solution Since F has no non-trivial extensions of odd degree, any extension of F must have degree a power of 2. Indeed, if L is an extension which is not a power of 2, then $\mathrm{Gal}(L/F)$ has a Sylow-2 subgroup P, which has odd index. Then by the Galois correspondence theorem, $\left[K^P : F\right] = [\mathrm{Gal}(L)F : P]$ which is odd; a contradiction.

In particular, $[K : F] = 2^n$ for some $n \geq 1$.

Suppose K is not algebraically closed, so that there exists a polynomial $f \in K[t]$ with no roots in K, and consider its splitting field L, which is Galois. L is a non-trivial extension of F, so $[L : F] = 2^m$ for some $m \geq 1$. If L is a non-trivial extension of K, then $2 \mid [L : K] = |\mathrm{Gal}(L/F)|$, which means that K would have an extension of 2, by combining Cauchy's theorem and the fundamental theorem of Galois theory. Thus, $L = K$, which means that f split in K, a contradiction.