Q1 Let $K_1, K_2, \ldots, K_n$ be subfields of K. The composite field of $K_1, K_2, \ldots, K_n$, denoted $K_1 K_2 \cdots K_n$, is defined to be the smallest subfield of K containing $K_1, K_2, \ldots, K_n$.

(a) Suppose that $K_j = F(S_j)$ for some $S_j \subseteq K$, $1 \leq j \leq n$. Show that $K_1 K_2 \cdots K_n = F(S_1 \cup S_2 \cup \cdots \cup S_n)$.

Proof. Denote $S = S_1 \cup \cdots \cup S_n \subseteq K$. For $j = 1, \ldots, n$, we have

$$K_j = F(S_j) \subseteq F(S) \subseteq K,$$

so $K_1 \cdots K_n \subseteq F(S)$.

On the other hand, for $j = 1, \ldots, n$, we have

$$S_j \subseteq F(S_j) = K_j \subseteq K_1 \cdots K_n,$$

so $S \subseteq K_1 \cdots K_n$. And, in particular,

$$F \subseteq F(S_1) = K_1 \subseteq K_1 \cdots K_n.$$

By definition, $F(S)$ is the smallest subfield of K containing F and S, so $F(S) \subseteq K_1 \cdots K_n$.

Hence, $K_1 \cdots K_n = F(S)$.

$\square$

(b) Let $K \subseteq \overline{F}$ be a finite separable field extension of F and $L \subseteq \overline{F}$ be the Galois closure of K over F. Suppose $\mathrm{Gal}(L/F) = \{\sigma_1, \ldots, \sigma_n\}$. Show that $L = \sigma_1(K)\sigma_2(K) \cdots \sigma_n(K)$.

Proof. By the primitive element theorem, K/F being a finite separable extension implies that $K = F(\alpha)$, for some $\alpha \in K$. Then, for any F-embedding $\varphi : K \to \overline{F}$, we have

$$\varphi(K) = \varphi(F(\alpha)) = F(\varphi(\alpha)).$$

Each $\sigma \in \mathrm{Gal}(L/F)$ can be restricted to an F-embedding $\sigma|_K : K \to \overline{F}$, so $\sigma(K) = F(\sigma(\alpha))$. Let $E = \sigma_1(K) \cdots \sigma_n(K)$, then applying part (a) to $S_j = \sigma_j(\alpha)$, we find

$$E = F(\sigma_1(\alpha)) \cdots F(\sigma_n(\alpha)) = F(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

We now claim that

$$\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/F).$$

Let $\tau \in \mathrm{Gal}(L/E)$ and $\sigma_j \in \mathrm{Gal}(L/F)$, then we immediately know $\sigma_j^{-1}\tau\sigma_j$ is an automorphism of L fixing F. To see that $\sigma_j^{-1}\tau\sigma_j$ also fixes E, it suffices to show that it fixes each $\sigma_i(\alpha)$, as they are the generators of E over F. Since both σ_i are both σ_j are elements in $\mathrm{Gal}(L/F)$, then so is $\sigma_j\sigma_i$, i.e., $\sigma_j\sigma_i = \sigma_k$ for some $1 \leq k \leq n$. Since τ fixes E and

$$\sigma_k(\alpha) \in \sigma_k(F(\alpha)) = \sigma_k(K) \subseteq E,$$

then in particular, τ fixes $\sigma_k(\alpha)$. We now derive

$$\sigma_j^{-1}\tau\sigma_j(\sigma_i(\alpha)) = \sigma_j^{-1}(\tau(\sigma_k(\alpha))) = \sigma_j^{-1}(\sigma_k(\alpha)) = \sigma_j^{-1}\sigma_j(\sigma_i(\alpha)) = \sigma_i(\alpha).$$

Hence, $\sigma_j^{-1}\tau\sigma_j$ fixes F and the generators of E over F, implying that it fixes E. That is, $\sigma_j^{-1}\tau\sigma_j \in \mathrm{Gal}(L/E)$, which tells us that $\mathrm{Gal}(L/E)$ is in fact a normal subgroup of $\mathrm{Gal}(L/F)$.

By the fundamental theorem, we conclude that E/F is a Galois subextension of L/F. Since $\mathrm{id}_L \in \mathrm{Gal}(L/F)$, then in particular, we know

$$K = \mathrm{id}_L(K) \subseteq \sigma_1(K)\cdots\sigma_n(K) = E.$$

That is, $K \subseteq E \subseteq L$ with E/F Galois. Since L/F is the Galois closure of K/F, then we must have

$$L = E = \sigma_1(K)\cdots\sigma_n(K).$$

$\square$

Q2 Problem 14.4.5 Let p be a prime and let F be a field. Let K be a Galois extension of F whose Galois group is a p-group (i.e., the degree $[K : F]$ is a power of p). Such an extension is called a *p-extension* (note that p-extensions are Galois by definition).

(a) Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.

Proof. Let $k, \ell \in \mathbb{Z}_{\geq 0}$ such that $[K : F] = p^k$ and $[L : K] = p^\ell$. In particular, L/F is a finite extension with $[L : F] = p^{k+\ell}$. Since L/K and K/F are both separable, then so is L/F.

Let E be the Galois closure of the finite separable extension L/F, and write

$$\mathrm{Gal}(E/F) = \{\sigma_1, \ldots, \sigma_n\}.$$

Applying Q1(b), we have

$$E = \sigma_1(L) \cdots \sigma_n(L).$$

Any $\sigma \in \mathrm{Gal}(E/F)$ restricts to an F-embedding $\sigma|_K : K \to \overline{F}$. Since K/F is Galois, it is normal, implying $\sigma(K) = K$. Then the field extension $\sigma(L)/\sigma(K) = \sigma(L)/K$ is isomorphic to the finite Galois extension L/K, so

$$\mathrm{Gal}(\sigma(L)/K) \cong \mathrm{Gal}(L/K).$$

Then $E/K = \sigma_1(L) \cdots \sigma_n(L)/K$ is a Galois extension with

$$\mathrm{Gal}(E/K) = \mathrm{Gal}(\sigma_1(L) \cdots \sigma_n(L)/K)$$

isomorphic to a subgroup of

$$\mathrm{Gal}(\sigma_1(L)/K) \times \cdots \times \mathrm{Gal}(\sigma_n(L)/K) \cong \mathrm{Gal}(L/K)^n.$$

(We have proven this result for composites of pairs of fields, and it easily generalizes to composites of finitely many fields.) In particular, $|\mathrm{Gal}(E/K)|$ divides $|\mathrm{Gal}(L/K)|^n = p^{\ell n}$, so $|\mathrm{Gal}(E/K)| = p^m$ for some nonnegative integer m. Therefore,

$$[E : F] = [E : K][K : F] = |\mathrm{Gal}(E/K)| p^k = p^{m+k},$$

meaning E/F is a p-extension of F.

$\square$

(b) Give an example to show that (a) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

Take $F = \mathbb{Q}$ and $K = L = \mathbb{Q}(\sqrt[3]{2})$. Then $[K : F] = 3$ and $[L : K] = 1 = 3^0$. And since K is Galois over itself, then L is trivially a 3-extension of K. However, the Galois closure of L over F is the splitting field of $x^3 - 2$, whose Galois group over F is isomorphic to S_3. Since $|S_3| = 6$, this could not be a 3-extension of F.

Q3 Problem 14.4.9 Suppose K/F is Galois with Galois group G and θ is a primitive element for K, i.e., $K = F(\theta)$. For any subgroup H of G, let $f(x) = \prod_{\sigma \in H}(x - \sigma(\theta))$. Show $f(x) \in E[x]$ where E is the fixed field of H in K, and that $f(x)$ is the minimal polynomial for θ over E. Prove that the coefficients of $f(x)$ generate E over F (these coefficients are the 'elementary symmetric functions' of the conjugates $\sigma(\theta)$ of θ for $\sigma \in H$, cf. Section 6).

Proof. Any automorphism of $K = F(\theta)$ fixing F is completely determined by the image of θ. Moreover, for any $\sigma \in \mathrm{Gal}(K/F)$,

$$K = \sigma(K) = \sigma(F(\theta)) = F(\sigma(\theta)).$$

This means that any automorphism of K fixing F is also completely determined by the image of $\sigma(\theta)$, for any $\sigma \in \mathrm{Gal}(K/F)$. In particular, for any $\sigma_1, \sigma_2, \tau \in \mathrm{Gal}(K/F)$,

$$\tau(\sigma_1(\theta)) = \tau(\sigma_2(\theta)) \implies \sigma_1(\theta) = \sigma_2(\theta) \implies \sigma_1 = \sigma_2.$$

In other words, each $\tau \in \mathrm{Gal}(K/F)$ is injective on the set $\{\sigma(\theta) \mid \sigma \in \mathrm{Gal}(K/F)\}$.

For any $\tau \in H$, we can extend τ to an automorphism of $K[x]$, acting on coefficients. Then

$$\tau(f(x)) = \prod_{\sigma \in H}(x - \tau(\sigma(\theta))) = \prod_{\sigma \in H}(x - \sigma(\theta)) = f(x),$$

where the second equality follows from the injectivity of τ, mentioned above, and the fact that $\tau\sigma \in H$ for all $\sigma \in H$, meaning τ is a bijection on the set $\{\sigma(\theta) : \sigma \in H\}$. This tells us that the coefficients of $f(x)$ are fixed under every $\tau \in H$, implying $f(x) \in K^H[x] = E[x]$.

Since $\mathrm{id}_K \in H$, then $(x - \theta) \mid f(x)$, implying $f(\theta) = 0$, so $m_{\theta,E}(x) \mid f(x)$. Clearly, $f(x)$ is monic, so it remains to show $f(x)$ is irreducible in $E[x]$. Suppose, for contradiction, that $f(x) = g(x)h(x)$ for some nonconstant $g(x), h(x) \in E[x]$. By the construction of $f(x)$, we can assume

$$g(x) = \prod_{j=1}^{k}(x - \sigma_j(\theta)) \quad \text{and} \quad h(x) = \prod_{j=k+1}^{n}(x - \sigma_j(\theta)),$$

for some $1 \leq k < n$, and where $H = \{\sigma_1, \ldots, \sigma_n\}$. Assume $\sigma_1 = \mathrm{id}_K$, so that θ is a root of $g(x)$, but not of $h(x)$. Since $h(x) \in E[x] = K^H[x]$ and $\sigma_{k+1}^{-1} \in H$, then we must have

$$h(x) = \sigma_{k+1}^{-1}(h(x)) = (x - \theta)\prod_{j=k+2}^{n}(x - \sigma_{k+1}^{-1}\sigma_j(\theta)).$$

However, this would imply that $f(x)$ has θ as a double root, which is contradiction. Hence, $f(x)$ is irreducible in $E[x]$, and we conclude that $f(x) = m_{\theta,E}(x)$.

Since $f(x) \in E[x]$, then the field generated by the coefficients of $f(x)$ over F is a subfield of E. Moreover, the minimal polynomial of θ over this field would still be $f(x)$, as θ is a root and it is irreducible over the possibly larger field of E. Therefore, the degree of K over this field would equal $\deg f(x) = [K : E]$, implying that the field generated by the coefficients of $f(x)$ over F is precisely E.

□

Q4 Problem 14.7.12 Let L be the Galois closure of the finite extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$. For any prime p dividing the order of $\mathrm{Gal}(L/\mathbb{Q})$ prove there is a subfield F of L with $[L:F]=p$ and $L=F(\alpha)$.
(Hint: One can use Cauchy's Theorem: If G is a finite group, p is a prime number and $p \mid |G|$, then G has a subgroup of order p.)

Proof. By Cauchy's theorem, there exists a subgroup $H \leq \mathrm{Gal}(L/\mathbb{Q})$ of order p. Suppose $\mathrm{Gal}(L/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$, then applying Q1(b), we find

$$L = \sigma_1(\mathbb{Q}(\alpha)) \cdots \sigma_n(\mathbb{Q}(\alpha)) = \mathbb{Q}(\sigma_1(\alpha)) \cdots \mathbb{Q}(\sigma_n(\alpha)) = \mathbb{Q}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)).$$

This means that any automorphism of L fixing $\mathbb{Q}$ is completely determined by its image of the generators $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. Therefore, choosing $\tau \in H \setminus \{\mathrm{id}_L\}$ (which exists since $|H| = p \geq 2$), we know there must be some $\sigma \in \mathrm{Gal}(L/F)$ such that $\tau\sigma(\alpha) \neq \sigma(\alpha)$. In which case, $\sigma^{-1}\tau\sigma(\alpha) \neq \alpha$, meaning α is not fixed by the conjugate subgroup $\sigma^{-1}H\sigma \leq \mathrm{Gal}(L/\mathbb{Q})$.

Define $F = L^{\sigma^{-1}H\sigma} \subseteq L$, then by construction, $\alpha \notin F$. Since conjugation by σ is an injective endomorphism on $\mathrm{Gal}(L/\mathbb{Q})$, we deduce

$$[L:F] = [L : L^{\sigma^{-1}H\sigma}] = |\sigma^{-1}H\sigma| = |H| = p.$$

Since p is prime, then L and F are the only subfields of L containing F. Since $\alpha \notin F$, then $F(\alpha)$ is a nontrivial field extension of F contained in L, implying $F(\alpha) = L$.

$\square$

Q5 Let F be a field and n be a positive integer. Suppose that $\mathrm{ch}(F) = 0$ or $\mathrm{ch}(F) \nmid n$ and $x^n - 1$ splits completely over F. Denote by $\sqrt[n]{a}$ a root in $\overline{F}$ of $x^n - a \in F[x]$. Let $m = [F(\sqrt[n]{a}) : F]$. Show that m is the smallest positive integer such that $(\sqrt[n]{a})^m \in F$.

Proof. The hypothesis on F is precisely the conditions for $\mathrm{Gal}(F(\sqrt[n]{a})/F) \cong \mathbb{Z}/m\mathbb{Z}$. Suppose the Galois group is generated by some σ, so that

$$\mathrm{Gal}(F(\sqrt[n]{a})/F) = \langle \sigma \rangle = \{\mathrm{id}_{F(\sqrt[n]{a})}, \sigma, \sigma^2, \ldots, \sigma^{m-1}\},$$

where $\mathrm{id}_{F(\sqrt[n]{a})} = \sigma^m$, since $|\sigma| = m$. Any automorphism of $F(\sqrt[n]{a})$ fixing F is completely determined by the image of $\sqrt[n]{a}$, which must be mapped to some other root of $x^n - a$. Suppose $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^r$, where $\zeta_n \in F$ is a primitive n-th root of unity and r is a nonnegative integer, so for all integers k,

$$\sigma^k(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^{rk}.$$

In particular, $\sigma^m = \mathrm{id}_{F(\sqrt[n]{a})}$ implies $\zeta_n^{rm} = 1$, i.e., that ζ_n^r is an m-th root of unity. Moreover, for $1 \le k < m$, the fact that $\sigma^k \neq \mathrm{id}_{F(\sqrt[n]{a})}$ means $\zeta_n^{rk} \neq 1$. From this, we deduce that ζ_n^r is in fact a primitive m-th root of unity, and denote it by ζ_m.

Applying Q3 to $\langle \sigma \rangle$ as a subgroup (of course, itself being the entire Galois group), the fixed field is

$$F(\sqrt[n]{a})^{\langle \sigma \rangle} = F(\sqrt[n]{a})^{\mathrm{Gal}(F(\sqrt[n]{a})/F)} = F,$$

and the minimal polynomial of $\sqrt[n]{a}$ over this fixed field is given by

$$m_{\sqrt[n]{a},F}(x) = \prod_{\tau \in \langle \sigma \rangle} (x - \sigma^k(\sqrt[n]{a})) = \prod_{k=0}^{m-1} (x - \sqrt[n]{a}\zeta_m^k) = x^m - \sqrt[n]{a}^m.$$

In particular, this implies $\sqrt[n]{a}^m \in F$. Moreover, $\sqrt[n]{a}^k \notin F$ for any positive integer $k < m$. Otherwise, $x^k - \sqrt[n]{a}^k$ would be a polynomial in $F[x]$ with $\sqrt[n]{a}$ as a root, but having a strictly smaller degree than the minimal polynomial of $\sqrt[n]{a}$ over F.

$\square$