Problem 1: Let $F$ be a field and let $F[x_1,\ldots,x_n]^{S_n}$ be the set of symmetric polynomials with coefficients in $F$ over the variable set $\{x_1,\ldots,x_n\}$. We may regard $F[x_1,\ldots,x_n]^{S_n}$ as an infinite-dimensional $F$-vector space. Find two different $F$-bases for $F[x_1,\ldots,x_n]^{S_n}$.

Solution: Consider the action of $S_n$ on the set $M_n$ of monomials in $F[x_1,\ldots,x_n]$. One $F$-basis is given by the sums of the monomials in the orbits of the action of $S_n$ on $M_n$. Each orbit of this action has a unique representative of the form $x_1^{a_1}\cdots x_n^{a_n}$ with $a_1\geq\cdots\geq a_n$. We see that

$$\left\{ \sum_{\text{sort}(b_1,\ldots,b_n)=(a_1,\ldots,a_n)} x_1^{b_1}\cdots x_n^{b_n} : a_1\geq\cdots\geq a_n \geq 0 \right\}$$

is an $F$-basis for $F[x_1,\ldots,x_n]^{S_n}$. Here $\text{sort}(b_1,\ldots,b_n)$ is the integer sequence $(b_1,\ldots,b_n)$ sorted into weakly decreasing order.

The Fundamental Theorem of Symmetric Polynomials states that any element $f \in F[x_1,\ldots,x_n]^{S_n}$ may be written uniquely as a polynomial in the elementary symmetric polynomials $s_1,\ldots,s_n$ with coefficients in $F$. It follows that

$$\{s_1^{b_1}s_2^{b_2}\cdots s_n^{b_n} : b_1,b_2,\ldots,b_n \geq 0 \}$$

is another $F$-basis for $F[x_1,\ldots,x_n]^{S_n}$.

Problem 2: Determine the splitting fields of the following polynomials over $\mathbb{Q}$:

$$f(x) = x^3 - 2, \quad g(x) = x^4 - 1, \quad h(x) = x^4 + 1.$$ 

Solution: Let $\alpha = 2^{1/3}$ be the real cube root of 2 and let $\omega = \exp(2\pi i/3)$. The roots of $f(x)$ are $\alpha,\omega\alpha,\omega^2\alpha$. It follows that the splitting field for $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha,\omega\alpha,\omega^2\alpha) = \mathbb{Q}(\alpha,\omega)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ (since $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein) and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ (since $\omega \notin \mathbb{Q}$ and $\omega$ is a root of $x^2 + x + 1$) and $\gcd(3,2) = 1$ we have $[\mathbb{Q}(\alpha,\omega) : \mathbb{Q}] = 6$.

The roots of $g(x)$ are $1,i,-1,-i$. It follows that the splitting field for $g(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$. The degree of this splitting field over $\mathbb{Q}$ is $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Let $\beta = 1/\sqrt{2}$. The roots of $h(x)$ are $\pm\beta\pm\beta i$. It follows that the splitting field for $h(x)$ over $\mathbb{Q}$ is

$$\mathbb{Q}(\beta + \beta i,\beta - \beta i,-\beta + \beta i,-\beta - \beta i) = \mathbb{Q}(\sqrt{2},i).$$

Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$ and $i \notin \mathbb{Q}(\sqrt{2})$ (since every element of $\mathbb{Q}(\sqrt{2})$ is real) we have $[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}] = 4$.

Problem 3: Let $F$ be a field and let $f(x) \in F[x]$ be a monic polynomial of degree $n$. Let $K$ be a splitting field for $f$ over $F$. Prove that the degree $[K : F]$ divides $n$!
By the Fixed Field Theorem, we know that we will use this throughout. This gives a maximum of $3 \cdot 2 = 6$ choices for $\sigma$, all of which must give well defined automorphisms of $Q(\alpha, \omega)$.

**Problem 4:** Let $\alpha = 2^{1/3}$ be the real cube root of 2 and let $\omega = \exp(2\pi i / 3)$. Determine all automorphisms of the fields $Q(\alpha)$ and $Q(\alpha, \omega)$.

**Solution:** Consider the polynomial $f(x) = x^3 - 2 \in Q[x]$. Then $f(x)$ has roots $\alpha, \omega\alpha, \omega^2\alpha$. Let $\sigma$ be an automorphism of $Q(\alpha)$. Then $\sigma$ fixes $Q$, and so permutes the roots of $f(x)$. Since $\sigma$ is determined by $\sigma(\alpha)$ and neither of the roots $\omega\alpha, \omega^2\alpha$ lie in $Q(\alpha)$ (since every element of $Q(\alpha)$ is real), we see that $\sigma$ is the identity map.

We have seen in Problem 2 that $Q(\alpha, \omega)$ is the splitting field for $f(x)$ over $Q$ and that $[Q(\alpha, \omega) : Q] = 6$. It follows that the group

$$\text{Aut}(Q(\alpha, \omega)) = G(Q(\alpha, \omega)/Q)$$

has size 6. Let $\sigma$ be an automorphism of $Q(\alpha, \omega)$, so that $\sigma$ fixes $Q$ and is determined by the values $\sigma(\alpha)$ and $\sigma(\omega)$. Since $\sigma$ permutes the roots of $f(x)$ we must have $\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}$. Since $\sigma$ permutes the roots of $x^2 + x + 1$ we have $\sigma(\omega) \in \{\omega, \omega^2\}$. This gives a maximum of $3 \cdot 2 = 6$ choices for $\sigma$, all of which must give well defined automorphisms of $Q(\alpha, \omega)$.

**Problem 5:** For each of the following sets of automorphisms of the field $C(t)$, determine the group of automorphisms $G$ which they generate and describe the fixed field $C(t)^G$ explicitly.

1. $\sigma(t) = t^{-1}$,
2. $\sigma(t) = it$,
3. $\sigma(t) = -t$, $\tau(t) = t^{-1}$,
4. $\sigma(t) = \omega t$, $\tau(t) = t^{-1}$, where $\omega = \exp(2\pi i / 3)$.

**Solution:** By the Fixed Field Theorem, we know that $C(t)$ has degree $|G|$ over $C(t)^G$; we will use this throughout.

1. The automorphism $\sigma$ generates a group $G$ of order 2, so that $[C(t) : C(t)^G] = 2$. We have $\sigma(t + t^{-1}) = t^{-1} + t$, so that $\mathbb{C}(t + t^{-1}) \subseteq C(t)^G$. Observe that $t$ is a
root of the quadratic polynomial
\[ x^2 - (t + t^{-1})x + 1 \in \mathbb{C}(t + t^{-1})[x], \]
so that \([\mathbb{C}(t) : \mathbb{C}(t + t^{-1})] \leq 2\). Combined with the previous observation and the Fixed Field Theorem, we see that \(\mathbb{C}(t)^G = \mathbb{C}(t + t^{-1})\) (and that \([\mathbb{C}(t) : \mathbb{C}(t + t^{-1})] = 2\).

(2) The automorphism \(\sigma\) generates a group \(G\) which is cyclic of order 4, so that \([\mathbb{C}(t) : \mathbb{C}(t)^G] = 4\). We have \(\sigma(t^4) = (it)^4 = t^4\), so that \(\mathbb{C}(t^4) \subseteq \mathbb{C}(t)^G\). Observe that \(t\) is a root of the quartic polynomial
\[ x^4 - t^4 \in \mathbb{C}(t^4)[x], \]
so that \([\mathbb{C}(t) : \mathbb{C}(t^4)] \leq 4\). As above, it follows that \(\mathbb{C}(t)^G = \mathbb{C}(t^4)\).

(3) Both of the automorphisms \(\sigma\) and \(\tau\) have order 2; they satisfy \(\sigma \tau = \tau \sigma\), so that they group \(G\) they generate is isomorphic to the product \(C_2 \times C_2\); the degree of \(\mathbb{C}(t)\) over \(\mathbb{C}(t)^G\) is 4. It is clear that \(t^2 + t^{-2} \in \mathbb{C}(t)^G\). Moreover, \(t\) is a root of the quartic polynomial
\[ x^4 - (t^2 + t^{-2})x^2 + 1 \in \mathbb{C}(t^2 + t^{-2})[x], \]
so that \([\mathbb{C}(t) : \mathbb{C}(t^2 + t^{-2})] \leq 4\). As above, it follows that \(\mathbb{C}(t)^G = \mathbb{C}(t^2 + t^{-2})\).

(4) The automorphism \(\sigma\) has order 3 and the automorphism \(\tau\) has order 2. We have \(\sigma(\tau(t)) = \sigma(t^{-1}) = \sigma(t)^{-1} = \omega^{-1}t^{-1}\), so that \(\tau(\sigma(\tau(t))) = \tau(\omega^{-1}t^{-1}) = \tau(\omega^{-1})\tau(t^{-1}) = \omega^{-1}t\) and \(\tau \sigma \tau = \sigma^{-1}\). It follows that \(\tau\) and \(\sigma\) generate a copy of the symmetric group \(S_3\) (of order 6).

We see that \(t^3 + t^{-3} \in \mathbb{C}(t)^G\). Moreover, \(t\) is a root of the sextic polynomial
\[ x^6 - (t^3 + t^{-3})x^3 + 1 \in \mathbb{C}(t^3 + t^{-3})[x], \]
so that \([\mathbb{C}(t) : \mathbb{C}(t^3 + t^{-3})] \leq 6\). As above, it follows that \(\mathbb{C}(t)^G = \mathbb{C}(t^3 + t^{-3})\).

**Problem 6:** Let \(f(x) = (x^2 - 2x - 1)(x^2 - 2x - 7) \in \mathbb{Q}[x]\). Let \(K\) be the splitting field for \(f(x)\) over \(\mathbb{Q}\). Determine all automorphisms of \(K\).

**Solution:** Let \(g(x) = x^2 - 2x + 1\) and \(h(x) = x^2 - 2x - 7\). Applying the quadratic formula, we see that the roots of \(g(x)\) are \((2 \pm \sqrt{8})/2 = 1 \pm \sqrt{2}\) and the roots of \(h(x)\) are \((2 \pm \sqrt{32})/2 = 1 \pm 2\sqrt{2}\). It follows that
\[ K = \mathbb{Q}(1 + \sqrt{2}, 1 - \sqrt{2}, 1 + 2\sqrt{2}, 1 - 2\sqrt{2}) = \mathbb{Q}(\sqrt{2}). \]

In particular, we have \([K : \mathbb{Q}] = 2\). There is only one nontrivial automorphism of \(K\); it is given by \(a + b\sqrt{2} \mapsto a - b\sqrt{2}\) for \(a, b \in \mathbb{Q}\).

**Problem 7:** (Optional - not to be handed in.) **Tensor products I.** Let \(R\) be a ring (not necessarily commutative), let \(M\) be a right \(R\)-module, \(^1\) and let \(N\) be a left \(R\)-module. Let \(\mathbb{Z}[M \times N]\) be the free abelian group with basis given by the set \(M \times N\). The tensor product \(M \otimes_R N\) is the abelian group
\[ M \otimes_R N := \mathbb{Z}[M \times N]/I, \]

\(^1\) That is, we have a map \(M \times R \to M\) such that \(m \cdot 1 = m\), \(m \cdot (r_1r_2) = (m \cdot r_1) \cdot r_2\), and \((m_1 + m_2) \cdot r = m_1 \cdot r + m_2 \cdot r\) always.
where $I$ is the subgroup of $\mathbb{Z}[M \times N]$ generated by all elements of the form

\[
(m \cdot r, n) - (m, r \cdot n)
\]
\[
(m + m', n) - (m, n) - (m', n)
\]
\[
(m, n + n') - (m, n) - (m, n')
\]

for $m, m' \in M, n, n' \in N$, and $r \in R$. Let $m \otimes n$ be the image of $(m, n)$ in $M \otimes_R N$ for $m \in M$ and $n \in N$. We have by construction the Universal Property of the Tensor Product:

for any abelian group $A$ and any map of sets $\phi : M \times N \to A$ which satisfies $\phi(m \cdot r, n) = \phi(m, r \cdot n), \phi(m + m', n) = \phi(m, n) + \phi(m', n)$, and $\phi(m, n + n') = \phi(m, n) + \phi(m, n')$ always, we have a unique well-defined homomorphism of abelian groups $\Phi : M \otimes_R N \to A$ determined by $\Phi : m \otimes n \mapsto \phi(m, n)$.

Suppose that $S$ is another ring and $M$ is an $(S,R)$-bimodule. \footnote{That is, $M$ is a left $S$-module, a right $R$-module, and we have $s \cdot (m \cdot r) = r \cdot (m \cdot s)$ for all $s \in S, m \in M, r \in R$.} Show that the map $S \times (M \otimes_R N) \to (M \otimes_R N)$ determined by $s \cdot (m \otimes n) := (s \cdot m) \otimes n$ gives $M \otimes_R N$ the (well defined) structure of a left $S$-module.

**Problem 8:** (Optional - not to be handed in.) **Tensor Products II.** Let $K/F$ be a field extension and let $V$ be an $F$-vector space. Explain how the tensor product $K \otimes_F V$ is a $K$-vector space.

Let $V$ and $W$ be vector spaces over some field $F$. Explain how the tensor product $V \otimes_F W$ is an $F$-vector space.

**Problem 9:** (Optional - not to be handed in.) **Tensor Products III.** Let $F$ be a field and let $V$ and $W$ be $F$-algebras. Prove that the tensor product $V \otimes_F W$ has an $F$-algebra structure determined by

\[
(v \otimes w) \cdot (v' \otimes w') := (v \cdot v') \otimes (w \cdot w')
\]

for all $v, v' \in V$ and $w, w' \in W$. To what familiar $F$-algebra is the tensor product $F[x] \otimes_F F[y]$ isomorphic (where $x$ and $y$ are variables)?

**Problem 10:** (Optional - not to be handed in.) **Tensor Products IV.** Let $G$ and $H$ be groups and let $F$ be a field. Let $V$ be a $G$-module over $F$ and let $W$ be an $H$-module over $F$. Prove that the $F$-vector space $V \otimes_F W$ is a $G \times H$-module according to the rule

\[
(g, h) \cdot (v \otimes w) := (g \cdot v) \otimes (h \cdot w)
\]

for all $g \in G, h \in H, v \in V, w \in W$. 