Problem 1 [14.1.7]

(a) Prove that any $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma(a) < \sigma(b)$ for every $a, b \in \mathbb{R}$.

(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$ for every positive integer $m$. Conclude that $\sigma$ is a continuous map on $\mathbb{R}$.

(c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$, and let $a, b \in \mathbb{R}$ be arbitrary real numbers.

(a) Obviously, $\sigma(a^2) = (\sigma(a))^2$ so $\sigma$ takes positive reals to positive reals. If $a < b$ then since $\mathbb{Q}$ is dense in $\mathbb{R}$ there exists $u \in \mathbb{Q}$ such that $a < u < b$. We obtain

$$u = \sigma(u) = \sigma(u - a + a) = \sigma(u - a) + \sigma(a) > \sigma(a),$$

and similarly $u < \sigma(b)$, yielding $\sigma(a) < u < \sigma(b)$.

(b) Suppose that $|a - b| < \frac{1}{m}$, for some $m \in \mathbb{Z}$. In view of (a), we get

$$-\frac{1}{m} = \sigma \left( -\frac{1}{m} \right) < \sigma(a - b) = \sigma(a) - \sigma(b) < \frac{1}{m},$$

By definition $\sigma$ is continuous if for any $\epsilon > 0$, $\exists \, \delta > 0$ such that $|\sigma(x) - \sigma(y)| < \epsilon$, whenever $|x - y| < \delta$. Now fixing $\epsilon > 0$, let $\delta = \frac{1}{m} < \epsilon$, for some $m \in \mathbb{Z}$. If $|x - y| < \delta$, then by the above

$$|\sigma(x) - \sigma(y)| < \frac{1}{m} < \epsilon,$$

showing that $\sigma$ is continuous.

(c) Let $x \in \mathbb{R}$ and $\epsilon > 0$. Since $\sigma$ is continuous $\exists \, \delta > 0$ such that $|\sigma(x) - \sigma(y)| < \frac{\epsilon}{2}$, whenever $|x - y| < \delta$. Set $\rho = \min(\frac{\epsilon}{2}, \delta)$ and let $a \in \mathbb{Q}$ such that $|x - a| < \rho$. Then

$$|\sigma(x) - x| = |\sigma(x) - a + (a - x)|$$

$$\leq |\sigma(x) - \sigma(a)| + |a - x|$$

$$< \frac{\epsilon}{2} + \rho \leq \epsilon,$$

implying that $\sigma(x) = x$.

Consequently, the only automorphism of $\mathbb{R}$ fixing $\mathbb{Q}$ is just the identity.
Problem 2 [14.1.8] Prove that the automorphisms of the rational function field $k(t)$ which fix $k$ are precisely the fractional linear transformations determined by $t \mapsto \frac{at+b}{ct+d}$ for $a, b, c, d \in k$, $ad - bc \neq 0$.

Proof. Let $\phi : k(t) \to k(t)$ be defined by $\phi(f(t)) = f\left(\frac{at+b}{ct+d}\right)$, for $f(t) \in k(t)$.

If $f, g \in k(t)$ then

$$\phi((f + g)(t)) = (f + g)\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right) + g\left(\frac{at+b}{ct+d}\right) = \phi(f(t)) + \phi(g(t)),$$

$$\phi((fg)(t)) = (fg)\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right)g\left(\frac{at+b}{ct+d}\right) = \phi(f(t))\phi(g(t)),$$

so $\phi$ is a homomorphism.

Assume $\phi((f(t)) = \phi(g(t))$ for some $f(t), g(t) \in k(t)$. Then

$$f\left(\frac{at+b}{ct+d}\right) = g\left(\frac{at+b}{ct+d}\right) \iff f = g \text{ in } k\left(\frac{at+b}{ct+d}\right).$$

By [13.2.18] we infer that

$$\left[k(t) : k\left(\frac{at+b}{ct+d}\right)\right] = \max(\deg(at+b), \deg(ct+d)) = 1,$$

so $k(t) = k\left(\frac{at+b}{ct+d}\right)$ and thus $f = g$ in $k(t)$, showing that $\phi$ is injective. Moreover, the above implies that $\text{Im}(\phi) = k\left(\frac{at+b}{ct+d}\right) = k(t)$, so $\phi$ is surjective. In conclusion, $\phi$ is an automorphism. It remains to see that $\phi$ fixes the constant functions, which are precisely the elements of $k$, hence $\phi$ fixes $k$.

Conversely, let $\phi$ be an automorphism of $k(t)$ fixing $k$, and $f(t) = \sum_{i=1}^{m} a_i t^{i} \in k(t)$. Observe that

$$\phi(f(t)) = \frac{\phi(\sum_{i=1}^{m} a_i t^{i})}{\phi(\sum_{i=1}^{m} b_i t^{i})} = \sum_{i=1}^{m} a_i \phi(t^{i}) = f(h(t)),$$

where $h(t) = \frac{P(t)}{Q(t)}$ and $P, Q$ are relatively prime over $k$.

Now $\text{Im}(\phi) = k(h(t)) = k\left(\frac{P(t)}{Q(t)}\right)$, and since $\phi$ is an automorphism $\text{Im}(\phi) = k(t)$. Hence by [13.2.18],

$$\max(\deg(P(t)), \deg(Q(t))) = [k(t) : k(h(t))] = 1,$$

proving that $P(t) = at+b$ and $Q(t) = ct+d$, for some $a, b, c, d \in k$. Finally, note that if $c = 0$ then $a \neq 0$ (and clearly $d \neq 0$), for otherwise $P$ and $Q$ would be constants, and not relatively prime. Similarly, if $c \neq 0$ then $\frac{ad}{c} \neq b$, for otherwise $at+b = \frac{a}{c}(ct+d)$. In either case, $ad - bc \neq 0$. Therefore, the automorphisms of the rational function field $k(t)$ that fix $k$ are precisely the fractional linear transformations.

\[\square\]

Problem 3 [14.2.13] Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.
Proof. Let \( f \) be a cubic with a splitting field \( K \) over \( \mathbb{Q} \), such that \( G := Gal(K/\mathbb{Q}) \) is the cyclic group of order 3. If \( f \) has only one real root, then the remaining two form a pair of conjugates. Now, complex conjugation \( \tau \) fixes \( \mathbb{Q} \), so \( \tau \in G \). However the order of \( \tau \) is 2, which does not divide \( |G| = 3 \), leading to a contradiction. \( \square \)

Problem 4. If \( \alpha \) is a complex root of \( x^6 + x^3 + 1 \) find all field homomorphisms \( \phi : \mathbb{Q}(\alpha) \to \mathbb{C} \).

Proof. Any field homomorphism will map the identity to 0 or to 1, so it will either be the zero homomorphism or it will fix \( \mathbb{Q} \). Thus it’s enough to find all homomorphisms \( \sigma \) fixing \( \mathbb{Q} \). Now \( \alpha^6 + \alpha^3 + 1 = 0 \) implies that \( \sigma(\alpha)^6 + \sigma(\alpha)^3 + 1 = 0 \), showing that any homomorphism sends \( \alpha \) to another root of \( x^6 + x^3 + 1 \). Since \( x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) \), the roots of \( x^6 + x^3 + 1 \) are just \( \{ \omega_k = e^{2\pi i k/9} \mid k = 1, 2, 4, 5, 7, 8 \} \). Note that each automorphism is determined by where \( \omega_1 \) gets sent to. For instance, if \( \sigma(\omega_1) = \omega_2 \), then \( \sigma(\omega_2) = \omega_4, \sigma(\omega_4) = \omega_8, \sigma(\omega_5) = \omega_1, \sigma(\omega_7) = \omega_5 \) and \( \sigma(\omega_8) = \omega_7 \). Thus the possible homomorphisms are just the ones mapping \( \omega_1 \) to \( \omega_k \), for \( k = 1, 2, 4, 5, 7, 8 \). \( \square \)

Problem 5. Let \( d > 0 \) be a square-free integer. Show that \( \mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}) \) is Galois and determine its Galois group explicitly. Show that \( Gal(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})) \) is isomorphic to the dihedral group with 8 elements by giving an explicit isomorphism.

Proof. Note that \( Aut(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})) \) is determined by the action on the generators \( \theta = \sqrt[8]{d} \) and \( i \). Consider

\[
\begin{align*}
  r : \sqrt[8]{d} &\mapsto \zeta^6 \sqrt[8]{d} \\
  i &\mapsto i
\end{align*}
\]

and

\[
\begin{align*}
  s : \sqrt[8]{d} &\mapsto -\sqrt[8]{d} \\
  i &\mapsto -i
\end{align*}
\]

Then it is not hard to see that any automorphism generated by \( r \) and \( s \) fixes \( \mathbb{Q}(\sqrt{d}) \). Moreover, \( \mathbb{Q}(\sqrt[8]{d}, i) \) is an extension of degree 8 over \( \mathbb{Q}(\sqrt{d}) \). Note that \( r^4 = s^2 = 1 \) and \( rsr = s \), which is a presentation of the dihedral group. Therefore

\[
8 = |D_8| = |r, s |^2 = 1, rsr = s > |Aut(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}))| \leq |\mathbb{Q}(\sqrt[8]{d}, i) : \mathbb{Q}(\sqrt{d})| = 8,
\]

showing that \( \mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d}) \) is Galois, and \( Gal(\mathbb{Q}(\sqrt[8]{d}, i)/\mathbb{Q}(\sqrt{d})) = D_8 \). \( \square \)