Proposition. Let $K$ be the splitting field of the separable polynomial $(x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$. Then $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the set of all of subfields of $K$ containing $\mathbb{Q}$ is

$$S = \{1, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{3}, \sqrt{5}), K\}.$$

Proof. It follows that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5})$. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over $\mathbb{Q}$ by Example 4 of §14.1 in [1]; since $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\sqrt{5}$ is a root of $x^2 - 5$, the degree of $\mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5})$ over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is equal to 2; therefore

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = (2)(4) = 8.$$

Hence, by Theorem 14 of §14.2 in [1], $\# \text{Gal}(K/\mathbb{Q}) = 8$.

Any automorphism $\sigma \in \text{Gal}(K/\mathbb{Q})$ must map the generators $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$ to a root of their respective minimal polynomials. Thus, because $\sigma$ is defined by where it maps the generators $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$, we may characterize $\sigma$ by

$$\sigma : \begin{cases} 
\sqrt{2} \mapsto \pm \sqrt{2} \\
\sqrt{3} \mapsto \pm \sqrt{3} \\
\sqrt{5} \mapsto \pm \sqrt{5}.
\end{cases}$$

Since $\# \text{Gal}(K/\mathbb{Q}) = 8$, these eight distinct possibilities must be elements of $\text{Gal}(K/\mathbb{Q})$. Furthermore, for $\sigma_1, \sigma_2, \sigma_3 \in \text{Gal}(K/\mathbb{Q})$ such that

$$\sigma_1 : \begin{cases} 
\sqrt{2} \mapsto -\sqrt{2} \\
\sqrt{3} \mapsto \sqrt{3} \\
\sqrt{5} \mapsto \sqrt{5}
\end{cases}, \quad \sigma_2 : \begin{cases} 
\sqrt{2} \mapsto \sqrt{2} \\
\sqrt{3} \mapsto -\sqrt{3} \\
\sqrt{5} \mapsto \sqrt{5}
\end{cases} \quad \text{and} \quad \sigma_3 : \begin{cases} 
\sqrt{2} \mapsto \sqrt{2} \\
\sqrt{3} \mapsto \sqrt{3} \\
\sqrt{5} \mapsto -\sqrt{5}
\end{cases},$$

it follows that

$$\text{Gal}(K/\mathbb{Q}) \cong \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The subgroups $\langle \sigma_1 \rangle$, $\langle \sigma_2 \rangle$ and $\langle \sigma_3 \rangle$ each fix two of the three generators of $K$ and, so, have fixed fields $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, respectively. Similarly, the subgroups $\langle \sigma_1, \sigma_2 \rangle$, $\langle \sigma_2, \sigma_3 \rangle$ and $\langle \sigma_1, \sigma_3 \rangle$ fix the fields $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, respectively. The identity element 1 $\in \text{Gal}(K/\mathbb{Q})$ fixes all of $K$ and $\langle \sigma_1, \sigma_2, \sigma_3 \rangle$ fixes only $\mathbb{Q}$. These eight subfields of $K$ exhaust the possibilities by the bijective correspondence of Theorem 14 of §14.2 in [1] to complete the proof. \qed

Date: 06/01/2011.
6.

**Proposition.** Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i), F_2 = \mathbb{Q}(\sqrt{2})$ and $F_1 = \mathbb{Q}(\sqrt{-2})$. Then Gal($K/F_1) \cong Z_8$, Gal($K/F_2) \cong D_8$ and Gal($K/F_3) \cong Q_8$.

**Proof.** Let $\zeta$ be a primitive eighth root of unity. By the discussion in §14.2 of [1],

Gal($\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}$) = $\langle \sigma, \tau : \sigma^8 = \tau^2 = 1, \sigma \tau = \tau \sigma^3 \rangle$

for the automorphisms $\sigma$ and $\tau$ of $K$ such that

$$
\sigma : \begin{cases}
\sqrt[8]{2} \mapsto \zeta \sqrt[8]{2} \\
i \mapsto i \\
\zeta \mapsto \zeta^5
\end{cases}
$$

and

$$
\tau : \begin{cases}
\sqrt[8]{2} \mapsto -\sqrt[8]{2} \\
i \mapsto -i \\
\zeta \mapsto \zeta^7
\end{cases}
$$

From these relations, it follows that $F_1$ is the fixed field of $H_1 = \langle \sigma \rangle$, $F_2$ is the fixed field of $H_2 = \langle \sigma^2, \tau \rangle$ and $F_3$ is the fixed field of $H_3 = \langle \sigma^2, \tau \sigma^2 \rangle$; therefore, by Corollary 11 of §14.2 in [1], Gal($K/F_i) = H_i$ for all $i \in \{1, 2, 3\}$.

Also by the relations in (1), $\sigma^8 = 1$ and so $H_1$ is a group of order 8 containing an element of order 8. Thus $H_1$ is isomorphic to the cyclic group $Z_8$. Similarly, we have the equations $(\sigma^2)^4 = 1, \tau^2 = 1$ and $\sigma^2 \tau = \sigma(\sigma \tau) = \sigma(\tau \sigma^3) = \tau \sigma^{-1}$. Hence

$$H_2 = \langle \sigma^2, \tau : (\sigma^2)^4 = \tau^2 = 1, \sigma \tau = \tau \sigma^{-1} \rangle.$$

Since these generators and relations uniquely define the dihedral group of order 8, $H_2 \cong D_8$. Lastly, the relations in (1) also imply that $(\sigma^2)^4 = 1, (\tau \sigma^3)^4 = 1, \sigma^2 (\tau \sigma^3) = (\tau \sigma^3)^{-1} \sigma^2$ and $(\sigma^2)^2 = \sigma^4 = (\tau \sigma^3)^2$, we find that

$$H_3 = \langle \sigma^2, \tau \sigma^3 : (\sigma^2)^4 = (\tau \sigma^3)^4 = 1, \sigma^2 (\tau \sigma^3) = (\tau \sigma^3)^{-1} \sigma^2, (\sigma^2)^2 = (\tau \sigma^3)^2 \rangle.$$

Therefore $H_3 \cong Q_8$. \hfill \Box

10.

**Proposition.** Let $K$ be the splitting field over $\mathbb{Q}$ of $x^8 - 3 \in \mathbb{Q}[x]$ and let $\zeta$ be a primitive eighth root of unity. The Galois group Gal($K/\mathbb{Q}$) is the group of automorphisms $\sigma_{a,b} : K \to K$ indexed by $(a, b) \in (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^*$, where $\sigma_{a,b}$ fixes $\mathbb{Q}$ and

$$\sigma_{a,b} : \begin{cases}
\sqrt[8]{3} \mapsto \zeta^a \sqrt[8]{3} \\
\zeta \mapsto \zeta^b
\end{cases}
$$

This identification yields an isomorphism

Gal($K/\mathbb{Q}$) $\cong (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^*$ (semi-direct product),

where the multiplicative group $(\mathbb{Z}/8\mathbb{Z})^*$ acts on the additive group $\mathbb{Z}/8\mathbb{Z}$ by multiplication.

**Proof.** The eight distinct roots of $x^8 - 3$ are given by $\zeta^a \sqrt[8]{3}$ for $a \in \{0, 1, \ldots, 7\}$. Thus $K = \mathbb{Q}(\zeta, \sqrt[8]{3})$. Note that by the discussion in §14.2 of [1], $Q(\zeta) = Q(\sqrt[8]{2}, i)$. We claim that $\sqrt[8]{2} \not\in Q(\sqrt[8]{3})$. Granting this, we see that

$$|Q(\sqrt[8]{2}, \sqrt[8]{3}) : \mathbb{Q}| = 2 \cdot |Q(\sqrt[8]{3}) : \mathbb{Q}| = 16.$$

Then since $i$ cannot be embedded in $\mathbb{R}$, we have that $K$ is the degree 2 extension of $Q(\sqrt[8]{2}, \sqrt[8]{3})$ obtained by adjoining $i$, and hence $|K : \mathbb{Q}| = 2 \cdot 16 = 32$.

There are various ways to prove the claim that $\sqrt[8]{2} \not\in Q(\sqrt[8]{3})$; perhaps simplest is to use Eisenstein’s criterion with the polynomial $x^8 - 3$ over the ring $\mathbb{Z}[\sqrt[8]{2}]$ with the maximal ideal $(3)$; this shows that the polynomial is irreducible over the UPD $\mathbb{Z}[\sqrt[8]{2}]$, hence irreducible over $Q(\sqrt[8]{2})$ by Gauss’s Lemma, and hence $|Q(\sqrt[8]{2}, \sqrt[8]{3}) : \mathbb{Q}| = 16$, proving the claim.

For any $\sigma \in$ Gal($K/\mathbb{Q}$), the generators $\sqrt[8]{3}$ and $\zeta$ must be sent to roots of their respective minimal polynomials. That is, $\sigma$ is of the form $\sigma_{a,b}$ as in (2). Since there are exactly 32 pairs $(a, b)$ and $|K : \mathbb{Q}| = 32$, we see that each $\sigma_{a,b}$ does indeed yield an element of Gal($K/\mathbb{Q}$).
It remains to determine the group structure of \( \text{Gal}(K/\mathbb{Q}) \). We calculate that
\[
\sigma_{a,b} \circ \sigma_{c,d}(\sqrt[3]{3}) = \sigma_{a,b}(\zeta \sqrt[3]{3}) = \zeta^{a+bc} \sqrt[3]{3},
\]
\[
\sigma_{a,b} \circ \sigma_{c,d}(\zeta) = \sigma_{a,b}(\zeta^d) = \zeta^{bd}.
\]
Therefore \( \sigma_{a,b} \circ \sigma_{c,d} = \sigma_{a+bc,bd} \), which gives the semi-direct product as desired:
\[
\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/8\mathbb{Z}).
\]
\[\square\]

12. **Proposition.** Let \( K \) be the splitting field over \( \mathbb{Q} \) of \( x^4 - 14x^2 + 9 \in \mathbb{Q}[x] \) and let \( \alpha_1 = \sqrt{7 + 2\sqrt{10}} \). Then \( K = \mathbb{Q}(\alpha_1) \), and \( \text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \), the Klein 4-group.

**Proof.** Let \( \alpha_2 = \sqrt{7 - 2\sqrt{10}} \). A straightforward computation using the quadratic formula shows that \( \pm \alpha_1 \) and \( \pm \alpha_2 \) are the distinct roots of \( x^4 - 14x^2 + 9 \). So \( K = \mathbb{Q}(\alpha_1, \alpha_2) \). Since \( \alpha_1\alpha_2 = \sqrt{49 - 40} = 3 \), we see that \( \alpha_2 \in \mathbb{Q}(\alpha_1) \); so in fact \( K = \mathbb{Q}(\alpha_1) \).

We claim that \( [K : \mathbb{Q}] = 4 \), i.e. that \( x^4 - 14x^2 + 9 \) is irreducible. One can prove this directly by exploring the possible factorizations (the factorizations will be of the form \( (x^2 + ax \pm 3)(x^2 - ax \pm 3) \) or the same with \( (3, 3) \) replaced by \( (1, 9) \); now solve for \( a \) and show that \( a \) is not rational). Here is an alternate method. Since we know how the polynomial factors in \( K \), and neither \( \alpha_1 \) nor \( \alpha_2 \) is rational, a factorization occurs only if \( (x + \alpha_1)(x \pm \alpha_2) \) has rational coefficients. The constant term is indeed rational (namely, \( \pm 3 \)), but the \( x \) coefficient is \( \alpha_1 \pm \alpha_2 \), and we calculate
\[
(\alpha_1 + \alpha_2)^2 = 20, \quad (\alpha_1 - \alpha_2)^2 = 8,
\]
so in particular neither of \( \alpha_1 \pm \alpha_2 \) is rational.

In any case, regardless of which method we chose, we see that the polynomial is irreducible and \( [K : \mathbb{Q}] = 4 \). To figure out the structure of the Galois group, one method is to note that by our calculations above, we see that \( K \) contains \( \sqrt{20} = 2\sqrt{5} \) and \( \sqrt{8} = 2\sqrt{2} \), and also it clearly contains \( \alpha_1^2 = 7 + 2\sqrt{10} \). Hence \( K = \mathbb{Q}(\sqrt{2}, \sqrt{5}) \) is a biquadratic extension with Galois group \( (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \).

Another way to see this if we did not do the calculation above with \( (\alpha_1 \pm \alpha_2)^2 \) is to directly write down the automorphisms. We know that \( \text{Gal}(K/\mathbb{Q}) \) acts transitively on the roots, so the Galois elements are determined by the possible images of \( \alpha_1 \); we have the identity and the elements:
\[
\sigma_1(\alpha_1) = \alpha_2; \quad \sigma_2(\alpha_1) = -\alpha_1; \quad \sigma_3(\alpha_1) = -\alpha_2.
\]
Since \( \alpha_2 = 3/\alpha_1 \), it is easy to compute the action of these automorphisms on \( \alpha_2 \):
\[
\sigma_1(\alpha_2) = \alpha_1; \quad \sigma_2(\alpha_2) = -\alpha_2; \quad \sigma_3(\alpha_2) = -\alpha_1.
\]
With these formulas it is easy to check that \( \sigma_i^2 = 1 \) for each \( i = 1, 2, 3 \). Hence \( \text{Gal}(K/\mathbb{Q}) \) is the Klein 4-group.
\[\square\]

17. This is similar to the proof of the next exercise.

18. **With notation as in the previous problem define the trace of \( \alpha \) from \( K \) to \( F \) to be**
\[
T_{\text{Tr}_{K/F}}(\alpha) = \sum_{\sigma} \sigma(\alpha),
\]
**a sum of Galois conjugates of \( \alpha \).**

(a) **Prove that** \( T_{\text{Tr}_{K/F}}(\alpha) \in F \).

**Proof.** The sum here is taken as follows. Let \( L \) be a Galois extension of \( F \) containing \( K \), and write \( G = \text{Gal}(L/F) \). Let \( H \subset G \) be the subgroup corresponding to \( K \). Then the sum runs over representatives \( \sigma \) for the left cosets of \( H \) in \( G \). These \( \sigma \) are the embeddings of \( K \) in \( L \) (equivalently, of \( K \) in \( F \)) by the Fundamental Theorem of Galois Theory.

To begin, note that the trace is well-defined, i.e. \( \sigma(\alpha) \) depends only on the left \( H \)-coset of \( \sigma \). Since \( H \) fixes \( K \) we see that if \( \sigma H = \tau H \), then \( \tau^{-1} \sigma(\alpha) = \h(\alpha) = \alpha \) for some \( h \in H \). Therefore, \( \sigma(\alpha) = \tau(\alpha) \).
To see that $\text{Tr}_{K/F}(\alpha) \in F$, let $S$ be a set of coset representatives for $H$, and notice that if $\tau \in \text{Gal}(L/F)$ then $\tau S$ is still a set of coset representatives for $H$. In other words, the action of $G$ by left multiplication simply permutes the left $H$-cosets. It follows that $\tau(\text{Tr}_{K/F}(\alpha)) = \text{Tr}_{K/F}(\alpha)$ for all $\tau \in \text{Gal}(L/F)$, and since the only elements fixed by all the automorphisms of $L/F$ are those in $F$, we have $\text{Tr}_{K/F}(\alpha) \in F$. \hfill $\Box$

(b) Prove that $\text{Tr}_{K/F}(\alpha + \beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta)$, so that the trace is an additive map from $K$ to $F$.

Proof. By the definition of trace,

$$\text{Tr}_{K/F}(\alpha + \beta) = \sum_{\sigma} \sigma(\alpha + \beta)$$

$$= \sum_{\sigma} (\sigma(\alpha) + \sigma(\beta))$$

$$= \sum_{\sigma} \sigma(\alpha) + \sum_{\sigma} \sigma(\beta)$$

$$= \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta),$$

so the trace map is additive. \hfill $\Box$

(c) Let $K = F(\sqrt{D})$ be a quadratic extension of $F$. Show that $\text{Tr}_{K/F}(a + b\sqrt{D}) = 2a$.

Proof. The quadratic extension $K/F$ is a Galois extension with $\text{Gal}(K/F) = \{1, \sigma\}$, where $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$. As such,

$$\text{Tr}_{K/F}(a + b\sqrt{D}) = a + \sqrt{D} + \sigma(a + b\sqrt{D})$$

$$= a + b\sqrt{D} + a - b\sqrt{D}$$

$$= 2a.$$ \hfill $\Box$

(d) Let $m_\alpha(x)$ be as in the previous problem. Prove that $\text{Tr}_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$.

Proof. Begin by noticing that

$$\prod_{\sigma}(x - \sigma(\alpha)) = x^n - (\sum_{\sigma} \sigma(\alpha))x^{n-1} + \cdots$$

$$= x^n - \text{Tr}_{K/F}(\alpha)x^{n-1} + \cdots.$$

Also,

$$(m_\alpha(x))^\frac{1}{d} = (x^d + a_{d-1}x^{d-1} + \cdots + a_0)^\frac{1}{d}$$

$$= x^n + \frac{n}{d}a_{d-1}x^{n-1} + \cdots + a_0^\frac{1}{d}.$$

In the following problem we prove that $\prod_{\sigma}(x - \sigma(\alpha)) = (m_\alpha(x))^\frac{1}{d}$, so equating the two $x^{n-1}$ terms gives the desired result. \hfill $\Box$

20. With notation as in the previous problems (beginning with 17) show more generally that $\prod_{\sigma}(x - \sigma(\alpha)) = (m_\alpha(x))^\frac{1}{d}$.

Proof. Let $f(x) = \prod_{\sigma}(x - \sigma(\alpha))$. Let $H' \subset G$ be the subgroup corresponding to $F(\alpha)$, and observe that it follows from $F \subseteq F(\alpha) \subseteq K$ that $H \subset H'$. We have the following diagram of fields, with certain extensions labelled by their Galois groups:
Now we claim that
\[ m_\alpha(x) = \prod_{\tau \in H'} (x - \tau(\alpha)), \]
where the product runs over the left cosets of $H'$ in $G$. Indeed, it is clear that $\alpha$ is a root of the product on the right (taking $\tau = 1$), and that this product is in $F[x]$ by the argument of #19 part (a). Since $\deg m_\alpha = [F(\alpha) : F] = [G : H']$, we have the desired equality.

Let’s return to the product $f(x) = \prod_\sigma (x - \sigma(\alpha))$, with the product running over all left $H$-cosets. We have that
\[ \sigma(\alpha) = \tau(\alpha) \iff \tau^{-1} \sigma \in H' \iff \sigma H' = \tau H'. \]
Since $H \subset H'$, each left $H'$-coset is a disjoint union of left $H$-cosets. The number of $H$-cosets in this disjoint union is
\[ [H' : H] = [G : H]/[G : H'] = n/d, \]
where $n = [K : F]$ and $d = [F(\alpha) : F] = \deg m_\alpha$.

Therefore, in the product defining $f(x)$, each distinct root $\sigma(\alpha)$ is repeated $\frac{n}{d}$ times, and hence $f(x) = (m_\alpha(x))^\frac{n}{d}$ as desired. □

References