Homework 5
Solutions

Problem 1 [14.2.3] Determine the Galois group of \((x^2 - 2)(x^2 - 3)(x^2 - 5)\). Determine all the subfields of the splitting field of this polynomial.

Solution. It is easy to see that \(K = \mathbb{Q} (\sqrt{2}, \sqrt{3}, \sqrt{5})\) is the splitting field of the polynomial \(f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)\) over \(\mathbb{Q}\). Moreover \(\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}\) is a \(\mathbb{Q}\)-basis for \(K\) and thus \([K : \mathbb{Q}] = 8\). So if \(G = \text{Gal}(K/\mathbb{Q})\) then \(|G| = 8\).

Consider the following automorphisms (of order 2 in \(G\))

\[
\begin{align*}
\sigma_2 &: \begin{cases}
\sqrt{2} \mapsto -\sqrt{2} \\
\sqrt{3} \mapsto \sqrt{3} \\
\sqrt{5} \mapsto \sqrt{5}
\end{cases} \\
\sigma_3 &: \begin{cases}
\sqrt{2} \mapsto \sqrt{2} \\
\sqrt{3} \mapsto -\sqrt{3} \\
\sqrt{5} \mapsto \sqrt{5}
\end{cases} \\
\sigma_5 &: \begin{cases}
\sqrt{2} \mapsto \sqrt{2} \\
\sqrt{3} \mapsto \sqrt{3} \\
\sqrt{5} \mapsto -\sqrt{5}
\end{cases}
\end{align*}
\]

then obviously

\(G = \langle \sigma_2, \sigma_3, \sigma_5 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\).

Notice that \(G\) is abelian, implying that all of its subgroups are normal. Now by the Fundamental Theorem of Galois theory, every normal subgroup \(H \leq G\) corresponds to a subfield \(K^H\), which is a splitting field over \(\mathbb{Q}\). Since \(|H|\) divides 8, we distinguish 4 cases:

- \(|H| = 1\), then clearly \(K^H = K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})\).
- \(|H| = 2\), then \(H\) contains the identity and an element of order 2, so it can be any of the following 7 groups: \(\{1, \sigma_2\}, \{1, \sigma_3\}, \{1, \sigma_5\}, \{1, \sigma_2\sigma_3\}, \{1, \sigma_3\sigma_5\}, \{1, \sigma_2\sigma_3\sigma_5\}\) by looking at the action on the basis elements we find that the corresponding fixed subfields of the above groups are \(\mathbb{Q}(\sqrt{3}, \sqrt{5})\), \(\mathbb{Q}(\sqrt{2}, \sqrt{5})\), \(\mathbb{Q}(\sqrt{2}, \sqrt{3})\), \(\mathbb{Q}(\sqrt{5}, \sqrt{6})\), \(\mathbb{Q}(\sqrt{2}, \sqrt{15})\), \(\mathbb{Q}(\sqrt{3}, \sqrt{10})\), \(\mathbb{Q}(\sqrt{6}, \sqrt{10})\).
- \(|H| = 4\), then \(H\) contains the identity, two distinct elements of order 2, and their product so it can be any of the following 7 groups: \(\{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\}, \{1, \sigma_3, \sigma_5, \sigma_3\sigma_5\}, \{1, \sigma_2, \sigma_5, \sigma_2\sigma_5\}, \{1, \sigma_3, \sigma_2\sigma_3, \sigma_2\sigma_3\sigma_5\}, \{1, \sigma_5, \sigma_2\sigma_3, \sigma_2\sigma_3\sigma_5\}, \{1, \sigma_2\sigma_3, \sigma_3\sigma_5, \sigma_5\sigma_2\}\) by looking at the action on the basis elements we find that the corresponding fixed subfields are \(\mathbb{Q}(\sqrt{5})\), \(\mathbb{Q}(\sqrt{3})\), \(\mathbb{Q}(\sqrt{15})\), \(\mathbb{Q}(\sqrt{10})\), \(\mathbb{Q}(\sqrt{6})\), \(\mathbb{Q}(\sqrt{30})\).
- \(|H| = 8\), then \(K^H = \mathbb{Q}\).
Problem 2 [14.2.16]
(a) Prove that \(x^4 - 2x^2 - 2\) is irreducible over \(\mathbb{Q}\).
(b) Show that the roots of this quartic are
\[\alpha_1 = \sqrt{1 + \sqrt{3}}, \quad \alpha_2 = \sqrt{1 - \sqrt{3}}, \quad \alpha_3 = -\sqrt{1 + \sqrt{3}}, \quad \alpha_4 = -\sqrt{1 - \sqrt{3}}.\]
(c) Let \(K_1 = \mathbb{Q}(\alpha_1)\) and \(K_2 = \mathbb{Q}(\alpha_2)\). Show that \(K_1 \neq K_2\) and \(K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F\).
(d) Prove that \(K_1, K_2\) and \(K_1K_2\) are Galois over \(F\) with \(\text{Gal}(K_1K_2/F)\) the Klein 4-group. Write out the elements of \(\text{Gal}(K_1K_2/F)\) explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of \(K_1K_2\) containing \(F\).
(e) Prove that the splitting field of \(x^4 - 2x^2 - 2\) over \(\mathbb{Q}\) is of degree 8 with dihedral Galois group.

Proof. (a) The polynomial \(x^4 - 2x^2 - 2\) is irreducible by Eisenstein’s criterion for \(p = 2\).
(b) Note that \((\pm \sqrt{1 \pm \sqrt{3}})^4 - 2(\pm \sqrt{1 \pm \sqrt{3}})^2 - 2 = (4 \pm 2\sqrt{3}) - 2(1 \pm \sqrt{3}) - 2 = 0\).
(c) Observe that \(\alpha_1\) is real, while and \(\alpha_2\) is complex, so \(K_1 \neq K_2\). Now \(F \subseteq K_1 \cap K_2\). \(K_1, K_2\) are each of degree 4, and they’re not equal, so \(2 \leq |K_1 \cap K_2 : \mathbb{Q}| < 4\). Therefore \(K_1 \cap K_2 = F\).
(d) We have the following factorization
\[x^4 - 2x^2 - 2 = (x^2 - 1 - \sqrt{3})(x^2 - 1 + \sqrt{3}) \in \mathbb{F}[x],\]
and clearly \(K_1\) is the splitting field of \(x^2 - 1 - \sqrt{3} \in \mathbb{F}[x]\) so \(K_1/F\) is Galois. Similarly, \(K_2/F\) is also Galois.
Now \(K_1K_2\) is the splitting field of the polynomial \(x^4 - 2x^2 - 2\) over \(F\) and \(\text{Gal}(K_1K_2/F)\) is generated by
\[\tau : \begin{cases} \alpha_1 \mapsto \alpha_1 \\ \alpha_2 \mapsto \alpha_4 \end{cases}, \quad \sigma : \begin{cases} \alpha_1 \mapsto \alpha_3 \\ \alpha_2 \mapsto \alpha_2 \end{cases}\]
so it has the structure of the Klein 4-group. The subgroup \(\{1, \tau\}\) corresponds to the fixed field \(K_1\), \(\{1, \sigma\}\) corresponds to \(K_2\), \(\{1, \sigma \tau\}\) corresponds to \(F(\sqrt{-2})\), the identity subgroup corresponds to \(K_1K_2\), and \(\{1, \sigma, \tau, \sigma \tau\}\) corresponds to \(F\).
(e) Since \(K_1K_2\) is the splitting field of \(x^4 - 2x^2 - 2\) over \(\mathbb{Q}\) we obtain \(|K_1K_2 : \mathbb{Q}| = |K_1K_2 : F|[F : \mathbb{Q}]| = 4 \cdot 2 = 8\) so \(G = \text{Gal}(K_1K_2/\mathbb{Q})\) is of order 8. From the previous part, we see that \(G\) has at least 3 subgroups of order 2. Also, \(G\) is not abelian. Since the only nonabelian subgroups of order 8 are \(D_8\) and \(Q_8\), we conclude that \(G\) must be the dihedral group.

Problem 3 [14.2.17] Let \(K/F\) be any finite extension and let \(\alpha \in K\). Let \(L\) be a Galois extension of \(F\) containing \(K\) and let \(H \leq \text{Gal}(L/F)\) be the subgroup corresponding to \(K\). Define the norm of \(\alpha\) from \(K\) to \(F\) to be
\[N_{K/F}(\alpha) = \prod \sigma(\alpha),\]
where the product is taken over all \(F\)-embeddings of \(K\) into an algebraic closure of \(F\) (so over a set of coset representatives for \(H\) in \(\text{Gal}(L/F)\) by the Fundamental Theorem of Galois Theory). This is a product of conjugates of \(\alpha\).
(a) Prove that $N_{K/F}(\alpha) \in F$.

(b) Prove that the norm is a multiplicative map.

(c) Let $K = F(\sqrt{D})$, prove that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.

(d) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over $F$. Let $n = [K : F]$. Prove that $d|n$, that there are $d$ distinct Galois conjugates of $\alpha$ which are all repeated $n/d$ times in the product above and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

Proof. (a) First we need to check that the product in the definition of the norm is well defined. Indeed, since $K$ is the fixed field of $H$, the elements of a coset $H \subset \text{Gal}(L/F)$ all correspond to the same embedding. So if $I$ and $J$ are two sets of coset representatives for $H$, then

$$\prod_{\sigma \in I} \sigma(\alpha) = \prod_{\sigma \in J} \sigma(\alpha),$$

showing that $N_{K/F}(\alpha)$ is well defined.

Now if $I$ is a set of coset representatives for $H$, then for any $\tau \in \text{Gal}(L/F)$, $\tau I$ is also a complete set of representatives, say $S$. This implies that

$$\tau N_{K/F}(\alpha) = \tau \prod_{\sigma \in I} \sigma(\alpha) = \prod_{\sigma \in I} \tau \sigma(\alpha) = \prod_{\sigma \in S} \sigma(\alpha) = N_{K/F}(\alpha).$$

In other words $N_{K/F}(\alpha)$ is fixed by $\text{Gal}(L/F)$, so it lies in $F$.

(b) Note that

$$N_{K/F}(\alpha\beta) = \prod_{\sigma} \sigma(\alpha\beta) = \prod_{\sigma} \sigma(\alpha) \prod_{\sigma} \sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).$$

(c) If $K = F(\sqrt{D})$ is a quadratic extension of $F$, then $K/F$ is necessarily Galois. In this case, the only non-identity element of $\text{Gal}(K/F)$ is the map $\sqrt{D} \mapsto -\sqrt{D}$. Hence

$$N_{K/F}(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$
Problem 4 [14.2.18] With the notation as in the previous problem, define the trace of \( \alpha \) from \( K \) to \( F \) to be
\[
\text{Tr}_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha),
\]
a sum of Galois conjugates of \( \alpha \).

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

(b) Prove that the trace is an additive map.

(c) Let \( K = F(\sqrt{D}) \), prove that \( \text{Tr}_{K/F}(a + b\sqrt{D}) = 2a \).

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

Proof. (a) This follows by the same reasoning as in the problem above.

(b) Notice that
\[
\text{Tr}_{K/F}(\alpha + \beta) = \sum_{\sigma} \sigma(\alpha + \beta) = \sum_{\sigma} \sigma(\alpha) + \sum_{\sigma} \sigma(\beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta).
\]

(c) In view of the previous problem
\[
\text{Tr}_{K/F}(a + b\sqrt{D}) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a.
\]

(d) As we saw in the previous problem, each of the \( d \) distinct Galois conjugates of \( K \) is repeated \( n/d \) times in the sum defining the trace. Hence
\[
\text{Tr}_{K/F}(\alpha) = \frac{n}{d} (\sum_{i=1}^{d} \alpha_i).
\]

Since \( \sum_{i=1}^{d} \alpha_i = -a_{d-1} \), it follows that \( \text{Tr}_{K/F}(\alpha) = -\frac{a}{d} a_{d-1} \).

Problem 5 [14.2.22] Suppose that \( K/F \) is a Galois extension and let \( \sigma \) be an element of the Galois group.

(a) Suppose \( \alpha \in K \) is of the form \( \alpha = \frac{\beta}{\sigma \beta} \) for some nonzero \( \beta \in K \). Prove that \( N_{K/F}(\alpha) = 1 \).

(b) Suppose \( \alpha \in K \) is of the form \( \alpha = \beta - \sigma \beta \) for some \( \beta \in K \). Prove that \( \text{Tr}_{K/F}(\alpha) = 0 \).

Proof. a) By the definition of the norm we have that for \( \beta \in K \) and \( \sigma \in G = \text{Gal}(K/F) \):
\[
N_{K/F}(\sigma \beta) = \prod_{\tau \in G} \tau(\sigma \beta) = \prod_{\rho \in G} \rho \beta = N_{K/F}(\beta).
\]
Thus if \( \alpha = \frac{\beta}{\sigma \beta} \) then \( N_{K/F}(\alpha) = \frac{N_{K/F}(\sigma \beta)}{N_{K/F}(\sigma \beta)} = 1 \).

b) Similarly, one has that \( \text{Tr}_{K/F}(\beta) = \text{Tr}_{K/F}(\sigma \beta) \). Hence, if \( \alpha = \beta - \sigma \beta \) then \( \text{Tr}_{K/F}(\alpha) = \text{Tr}_{K/F}(\beta) - \text{Tr}_{K/F}(\sigma \beta) = 0 \).