Section 14.2

Exercise 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.

Proof. Note that the splitting field of the polynomial is \(\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5})\) if we show that \(\sqrt{2} \notin \mathbb{Q}, \sqrt{3} \notin \mathbb{Q}(\sqrt{2})\) and \(\sqrt{5} \notin \mathbb{Q}(\sqrt{2})(\sqrt{3})\). We sketch the implication without being rigorous as the computations are straightforward.

1. \(\sqrt{2} \notin \mathbb{Q}\). Otherwise \(\sqrt{2}\) is a rational number; a contradiction.

2. \(\sqrt{3} \notin \mathbb{Q}(\sqrt{2})\). Otherwise \(\sqrt{3}\) has the form \(a + b\sqrt{2}\), with \(a, b \in \mathbb{Q}\). By taking the square, if follows that either \(a\) or \(b\) are equal to 0, otherwise \(\sqrt{2} \in \mathbb{Q}\). If \(a = 0\) then \(\sqrt{3}/\sqrt{2} \in \mathbb{Q}\); a contradiction. If \(b = 0\) then \(\sqrt{3} \in \mathbb{Q}\); again, a contradiction.

3. \(\sqrt{5} \notin \mathbb{Q}(\sqrt{2})(\sqrt{3})\). Otherwise, \(\sqrt{5}\) has the form \(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\), with \(a, b, c, d \in \mathbb{Q}\) [example 2, section 13.2 in Dummit and Foote]. By taking the square, we see that \(\sqrt{3} \in \mathbb{Q}(\sqrt{2})\) (a contradiction to the above statement) unless \(5\) has the form \(a' + b'\sqrt{2}\), with \(a', b' \in \mathbb{Q}\). Again a contradiction, since it implies \(\sqrt{2} \in \mathbb{Q}\).

Thus \(\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5})\) is the splitting field of the polynomial, and furthermore its degree extension is 8 (since the quadratic polynomials are minimal in the respective extensions). It follows that its Galois group is also of order 8.

Since roots of minimal polynomial are mapped to other roots of the same minimal polynomial, we have the following natural choices for automorphisms in the Galois group:

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

Note that these automorphisms are pairwise commutative and of order 2. Therefore our Galois group is isomorphic to \(\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2\). From here we check the structure of this group (via internet) and see that it contains the following proper subgroups, together with their corresponding subfields:
i) of order 2:
\[
\begin{align*}
\langle \sigma_2 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{3})(\sqrt{5}) \\
\langle \sigma_3 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{5}) \\
\langle \sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\
\langle \sigma_2\sigma_3 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{5})(\sqrt{6}) \\
\langle \sigma_2\sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{3})(\sqrt{10}) \\
\langle \sigma_3\sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{15}) \\
\langle \sigma_2\sigma_3\sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{6})(\sqrt{10})
\end{align*}
\]

ii) of order 4:
\[
\begin{align*}
\langle \sigma_2, \sigma_3 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{5}) \\
\langle \sigma_2, \sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{3}) \\
\langle \sigma_3, \sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{2}) \\
\langle \sigma_2, \sigma_3\sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{15}) \\
\langle \sigma_3, \sigma_2\sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{10}) \\
\langle \sigma_5, \sigma_2\sigma_3 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{6}) \\
\langle \sigma_2\sigma_3, \sigma_2\sigma_5 \rangle &\leftrightarrow \mathbb{Q}(\sqrt{30})
\end{align*}
\]

Exercise 11. Suppose \( f(x) \in \mathbb{Z}[x] \) is an irreducible quartic whose splitting field has Galois group \( S_4 \) over \( \mathbb{Q} \). Let \( \theta \) be a root of \( f(x) \) and set \( K = \mathbb{Q}(\theta) \). Prove that \( K \) is an extension of \( \mathbb{Q} \) of degree 4 which has no proper subfields. Are there any Galois extensions of \( \mathbb{Q} \) of degree 4 with no proper subfields?

Proof. Since \( f(x) \) is irreducible in \( \mathbb{Z}[x] \) it is also irreducible in \( \mathbb{Q}[x] \) then, by corollary 7 [Dummit and Foote, section 13.1] the extension \( K/\mathbb{Q} \) is of degree 4. Now, let \( J \) be the splitting field of \( f(x) \) and assume that a proper subfield \( L \subset K \) exists. By the Fundamental Theorem of Galois Theory \( J, K, L, \mathbb{Q} \) are in correspondence with subgroups of \( S_4 \). In particular, the extension \( K/L \) permutes the other 3 roots of \( f(x) \) therefore \( \text{Gal}(K/L) = S_3 \). It suffices to show that there are no proper subgroups between \( S_4 \) and \( S_3 \). Which we show by looking at the group lattice of \( S_4 \).

![Group structure of S4](image)

Figure 1: Group structure of \( S_4 \)

For the second part, if the Galois extension is of degree 4, then it is in correspondence to a group of order 4. By Cauchy theorem, this group must have a normal subgroup of order 2 and thus, such extension will always have a proper subfield. \( \square \)
Exercise 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

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

where the product is taken over all the embeddings of $K$ into an algebraic closure of $F$. This is a product of Galois conjugates of $\alpha$. In particular, if $K/F$ is Galois this is

$$\prod_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha).$$

i. Prove that $N_{K/F}(\alpha) \in F$.

ii. Prove that $N_{K/F}(\alpha \beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so that the norm is a multiplicative map from $K$ to $F$.

Proof. By definition

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

as desired. \qed

iii. Let $K = F(\sqrt{D})$ be a quadratic extension of $F$. Show that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.

Proof. Observe that $\sqrt{D}$ satisfies $x^2 - D = 0$, thus $x^2 - D$ splits in $K$ and therefore it is a Galois extension. Since $\sigma \in \text{Gal}(K/F)$ permutes the roots of irreducible polynomials we have that, either $\sigma$ is the trivial map, or $\sigma(\sqrt{D}) = -\sqrt{D}$. Thus

$$N_{K/F}(a + b\sqrt{D}) = \prod_{\sigma} \sigma(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$$

as desired. \qed

iv. Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$. Let $n = [K:F]$. Prove that $d$ divides $n$, 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. First, consider the field extensions $K/F$ and $F(\alpha)/F$. The latter is of degree $d$ from the minimal polynomial $m_\alpha(x)$. Then, by the basic property,

$$[K:F] = [K:F(\alpha)] [F(\alpha):F]$$

we see that $n = [K:F(\alpha)] d$. Thus $d$ divides $n$.

Now, since $K$ has degree $n$ over $F$, the order of $\text{Gal}(K/F)$ is $n$. Furthermore, $\sigma \in \text{Gal}(K/F)$
sends \( \alpha \) to a root of the minimal polynomial \( m_\alpha(x) \). We see that there are \( d \) distinct roots of \( m_\alpha(x) \), and thus \( \alpha \) is mapped to a different root \( n/d \) times. Then,

\[
N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \left( \prod_{i=1}^{d} \alpha_i \right)^{n/d}
\]

where \( \{\alpha_i\}_{i=1}^{d} \) is the set of roots of the minimal polynomial. Finally, the coefficient \( a_0 \) in \( m_\alpha(x) \) satisfies

\[
a_0 = (-1)^{d} \prod_{i=1}^{d} \alpha_i
\]

thus,

\[
N_{K/F}(\alpha) = (-1)^{n} a_0^{n/d}.
\]

**Exercise 18.** With 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 \( \alpha \).

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

ii. 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 definition

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

\[
= \sum_{\sigma} (\sigma(\alpha) + \sigma(\beta))
\]

\[
= \sum_{\sigma} \sigma(\alpha) + \sum_{\sigma} \sigma(\beta)
\]

\[= \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta)
\]

as we wanted. \( \square \)

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

**Proof.** Using the same reasoning as in Exercise 17, iii. we see that

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

\[= (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a.
\]

\( \square \)

iv. Let \( m_\alpha(x) \) be as in the previous problem. Prove that \( \text{Tr}_{K/F}(\alpha) = -\frac{n}{d}a_{d-1} \).
Proof. Analogous to part \( iv. \) in the previous exercise, \( \alpha \) is mapped to one of its conjugates \( n/d \) times. Therefore

\[
\text{Tr}_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha) = \frac{n}{d} \sum_{i=1}^{d} \alpha_i,
\]

where \( \{\alpha_i\}_{i=1}^{d} \) is the set of roots of \( m_\alpha(x) \). Now, observe that the coefficient \( a_{d-1} \) of \( m_\alpha(x) \) satisfies

\[-\sum_{i=1}^{d} \alpha_i = a_{d-1}\]

thus,

\[
\text{Tr}_{K/F}(\alpha) = -\frac{n}{d} a_{d-1}.
\]

Exercise 29. Let \( k \) be a field and let \( k(t) \) be the field of rational functions \( n \) variable \( t \). Define the maps \( \sigma \) and \( \tau \) form \( k(t) \) to itself by \( \sigma(f) = f(\frac{1}{1-t}) \) and \( \tau(f) = f(\frac{1}{t}) \) for \( f \in (t) \).

i. Prove that \( \sigma \) and \( \tau \) are automorphisms of \( k(t) \) and that the group \( G = \langle \sigma, \tau \rangle \) they generate is isomorphic to \( S_3 \).

\[
\text{Proof.} \text{ We prove this by means of exercise 8 [Section 14.1, Dummit and Foote]. The map } t \mapsto \frac{at+b}{ct+d} \text{ is an automorphism of the rational function field } k(t) \text{ whenever } a, b, c, d \in k \text{ and } ad-bc \neq 0. \text{ Clearly } \sigma \text{ and } \tau \text{ satisfy this condition. To prove that } G \cong S_3 \text{ it suffices to show that } \sigma^3 = \tau^2 = t \text{ (the identity map) and that } \tau \sigma \tau = \sigma^{-1} \text{ (this is the usual representation of } S_3 \text{ by generators). Clearly } \tau^2 = t, \text{ and furthermore,}
\]

\[
\sigma^2 = \frac{1}{1-t} - \frac{1}{1-\frac{1}{1-t}} = \frac{t-1}{t} = 1 - \frac{1}{t}
\]

then,

\[
\sigma^3 = 1 - \frac{1}{1-t} = 1 - (1-t) = t.
\]

It is left to show that \( \tau \sigma \tau = \sigma^{-1} \), or equivalently, \( \sigma \tau \sigma = t \). Observe that

\[
\sigma \tau = \frac{1}{1-t} = 1-t,
\]

\[
\tau \sigma = 1 - \frac{1}{1-t} \text{ and}
\]

\[
\sigma \tau \sigma = 1 - \frac{1}{1-t} = 1 - (1-t) = t
\]

as we wanted.

\[
\text{ii. Prove that the element } t = \frac{(t^2-t+1)^3}{t^2(t-1)^2} \text{ is fixed by all the elements of } G.
\]

\[
\text{Proof.} \text{ It suffices to check that the generators of } G \text{ fix } t. \text{ Observe that}
\]

\[
\sigma(t) = \frac{(\frac{1}{1-t})^2 - \frac{1}{1-\frac{1}{1-t}} + 1}{(\frac{1}{1-t})^2 (\frac{1}{1-t} - 1)^2} = \frac{\frac{1}{(1-t)^2} - \frac{1}{1-t} + 1}{\frac{1}{(1-t)^2} (\frac{1}{1-t} - 1)^2} = \frac{\frac{1}{(1-t)^2} - \frac{1}{1-t} + 1}{\frac{(1-t)^2}{(1-t)^2}} = \frac{(1-t)^3}{(1-t)^3} = \frac{(1-t)^3}{(1-t)^3} = \frac{(1-t)^3}{(1-t)^3} = \frac{(1-t)^3}{(1-t)^3}.
\]
as desired.\ Analogously,
\[
\tau(t) = \left(\frac{1}{2} \right)^3 - \left(\frac{1}{2} \right)^2 \left(\frac{1}{2} - t + 1\right) = \left(\frac{1-t}{t^2} \right)^3 \left(\frac{1}{2} \right)^2 = \left(\frac{1-t}{t^2} \right)^3 \left(\frac{1}{2} \right)^2 = \frac{(1-t+t^2)^3}{t^2(t-1)^2} = \frac{(1-t+t^2)^3}{t^2(t-1)^2}.
\]

Hence, \( t \) is fixed by \( G \). \( \square \)

iii. Prove that \( k(t) \) is precisely the fixed field of \( G \) in \( k(t) \).

**Proof.** We have shown in exercise 18 [Section 13.2, Dummit and Foote] that the degree of the extension
\[
k(t)/k \left(\frac{(t^2 - t + 1)^3}{t^2(t-1)^2}\right)
\]
is precisely \( \max\{\deg(t^2 - t + 1)^3, \deg t^2(t-1)^2\} = 6 \). Furthermore, let \( K \) be the fixed field described in ii., the previous part shows that \( [k(t) : K] = 6 \) as well. Then, by the basic property
\[
\left[ k(t) : k \left(\frac{(t^2 - t + 1)^3}{t^2(t-1)^2}\right) \right] = [k(t) : K] \left[ K : k \left(\frac{(t^2 - t + 1)^3}{t^2(t-1)^2}\right) \right],
\]
we have \( \left[ K : k \left(\frac{(t^2 - t + 1)^3}{t^2(t-1)^2}\right) \right] = 1 \) and therefore \( K = k \left(\frac{(t^2 - t + 1)^3}{t^2(t-1)^2}\right) \). \( \square \)

**Exercise 31.** Let \( K \) be a finite extension of degree \( n \) over \( F \). Let \( \alpha \) be an element of \( K \).

i. Prove that \( \alpha \) acting by left multiplication on \( K \) is an \( F \)-linear transformation \( T_\alpha \) of \( K \).

**Proof.** Let \( x, y \) be elements of \( K \) and \( c \) be an element of \( F \). Then, \( T_\alpha(c(x+y)) = T_\alpha(cx + cy) = \alpha(cx + cy) = \alpha cx + \alpha cy = c\alpha x + c\alpha y = cT_\alpha(x) + cT_\alpha(y) \). Thus, \( T_\alpha \) is \( F \)-linear. \( \square \)

ii. Prove that the minimal polynomial for \( \alpha \) over \( F \) is the same as the minimal polynomial for the linear transformation \( T_\alpha \).

**Proof.** Let \( m_\alpha(x) = \sum_{i=0}^{n} c_i x^i \) be the minimal polynomial of \( \alpha \) over \( F \). Then, by the linearity in part i. \( m_\alpha(T_\alpha) = \sum_{i=1}^{n} c_i (T_\alpha)^i \) is the map
\[
x \mapsto \left( \sum_{i=1}^{n} c_i (\alpha)^i \right) \cdot x
\]
where \( \sum_{i=1}^{n} c_i (\alpha)^i = m_\alpha(\alpha) = 0 \). Thus \( m_\alpha(T_\alpha) = 0 \), and furthermore, this polynomial is irreducible by definition. Thus \( m_\alpha(x) \) is the minimal polynomial of \( T_\alpha \). \( \square \)

iii. Prove that the trace \( \text{Tr}_{K/F}(\alpha) \) is the trace of the \( n \times n \) matrix defined by \( T_\alpha \). Prove that the norm \( \text{N}_{K/F}(\alpha) \) is the determinant of \( T_\alpha \).

**Proof.** Let \( f(x) \) be the characteristic polynomial of \( T_\alpha \) and \( m(x) \) be its minimal polynomial as in ii. Since the characteristic polynomial of \( T_\alpha \) divides some power of the minimal polynomial, and in our case, the minimal polynomial is irreducible it must hold that
\[
\deg m \bigg| \deg f.
\]
Therefore \( f \) is of the form \( f(x) = (m(x))^{\deg f/\deg m} \). We see the following
a) By Exercise 17 above we have
\[ N_{K/F}(\alpha) = (-1)^n c^{\deg f / \deg m} \]
which coincides with the constant coefficient in \( f(x) \), and hence with the determinant of \( T_a \).

b) By Exercise 18 above we have
\[ \text{Tr}_{K/F}(\alpha) = -d^{\deg f / \deg m} \]
which coincides with the negative of the coefficient of \( x^{\deg f - 1} \) in \( f(x) \), and hence with the trace of \( T_a \).

\[ \square \]

Section 14.3

Exercise 5. Exhibit an explicit isomorphism between the splitting fields of \( x^3 - x + 1 \) and \( x^3 - x - 1 \) over \( \mathbb{F}_3 \).

Construction. First we will show that \( \mathbb{F}_3 / \langle x^3 - x + 1 \rangle \) is the splitting field of \( f(x) = x^3 - x + 1 \). First, note that \( f(x) \) is irreducible, as it has no roots over \( \mathbb{F}_3 \), \( (f(0) = f(1) = f(2) = 1) \). By artificially adjoining a root of \( f(x) \), let it be \( \theta \), we get the extension \( \mathbb{F}_3(\theta) \) (isomorphic to \( \mathbb{F}_3 / \langle x^3 - x + 1 \rangle \)). Now, observe that \( f(\theta + z) \) evaluates to
\[
(\theta + z)^3 - (\theta + z) + 1 = \theta^3 + z^3 - \theta - z + 1 = (\theta^3 - \theta + 1) + (z^3 - z) = z^3 - z.
\]
With \( z^3 - z = 0 \) for all \( z \in \mathbb{F}_3 \). Thus \( \mathbb{F}_3(\alpha) \) contains all roots of \( f(x) \) and therefore it splits. By an analogous argument the splitting field of \( g(x) = x^3 - x - 1 \) is the field extension \( \mathbb{F}_3 / \langle x^3 - x - 1 \rangle \). Now consider the map
\[ \varphi : \mathbb{F}_3[x] \to \mathbb{F}_3[x] / \langle x^3 - x - 1 \rangle \]
given by the evaluation
\[ \varphi(h) = h(\theta) \]
with \( \theta \) as before. Since evaluation is a ring homomorphism it suffices to show that \( \ker \varphi = \langle x^3 - x + 1 \rangle \), so that by the first isomorphism theorem
\[ \mathbb{F}_3[x] / \langle x^3 - x + 1 \rangle \cong \mathbb{F}_3[x] / \langle x^3 - x - 1 \rangle. \]
Since \( \theta \) is a root of \( f \), we immediately see that \( \varphi(f) = f(\theta) = 0 \). Thus \( \langle f \rangle \subset \ker \varphi \). Conversely, take \( h \in \ker \varphi \), therefore \( h(\theta) = 0 \). Since \( f \) is irreducible, it is also the minimal polynomial of \( \theta \) in \( \mathbb{F}_3 \). Therefore \( f \) divides \( h \), and hence \( h \in \langle f \rangle \). It follows that \( \ker \varphi = \langle f \rangle \) and the construction of the isomorphism is complete.

Exercise 10. Prove that \( n \) divides \( \varphi(p^n - 1) \). [Observe that \( \varphi(p^n - 1) \) is the order of the group of automorphisms of a cyclic group of order \( p^n - 1 \)]

Proof. Consider \( G = (\mathbb{Z} / (p^n - 1)\mathbb{Z})^\times \); the group of units of integers modulo \( p^n - 1 \). The order of \( G \) is \( \varphi(p^n - 1) \). Note that \( p \in G \) as it is relatively prime to \( p^n - 1 \). Now we inspect the order of \( p \) in \( G \). Clearly \( p^n \equiv 1 \mod (p^n - 1) \), and by construction, \( n \) is the smallest number for which this is true. Thus, the order of \( p \) in \( G \) in \( n \). Then, by Lagrange’s \( n \) divides the order of \( G, \varphi(p^n - 1) \).
Section 14.6

Exercise 2. Determine the Galois groups of the following polynomials:

Note: the field is not stated in the original source of the problem, I presume it is intended to be $\mathbb{Q}$.

i. $x^3 - x^2 - 4$.

**Solution.** Note that $x^3 - x^2 - 4 = (x - 2)(x^2 + x + 2)$. The latter factor has discriminant equal to $-7$. Hence, the Galois group is isomorphic to $S_2$. □

ii. $x^3 - 2x + 4$.

**Solution.** This polynomial is irreducible by the rational root test. Furthermore, its discriminant is equal to $-560$, thus its Galois group is isomorphic to $S_3$. □

iii. $x^3 - x + 1$.

**Solution.** This polynomial is irreducible by the rational root test. Furthermore, its discriminant is equal to $-23$, thus its Galois group is isomorphic to $S_3$. □

iv. $x^3 + x^2 - 2x - 1$.

**Solution.** This polynomial is irreducible by the rational root test. Furthermore, its discriminant is equal to 49, thus its Galois group is isomorphic to $A_3$. □