Galois theory practice exercises

Feel free to consult the book (up to section 16.7) or your notes when working on these problems.

Unless stated otherwise, whenever I ask for the Galois group, I mean the Galois group over \( \mathbb{Q} \).

1. Let \( f(x) = x^3 + 3x + 1 \). Show that \( f \) has only one real root. What is the Galois group of \( f \) isomorphic to? (Note: you do not need to do any explicit computations to determine the Galois group.)

**Solution:** First notice that \( f \) is irreducible over \( \mathbb{Q} \) (for example by checking mod 2). Since \( f(x) \) is cubic, it has a real root. Moreover, since \( f'(x) = 3x^2 + 3 \) is positive for all \( x \), \( f \) is always increasing, so it has only one real root. Let \( \alpha \) be the unique real root of \( f(x) \). Then \( \mathbb{Q}(\alpha)/\mathbb{Q} \) has degree 3. Moreover, \( \mathbb{Q}(\alpha) \) is not a splitting field for \( f \) because its other roots are not real. So its splitting field is an extension \( K/\mathbb{Q}(\alpha) \). Since \( [K: \mathbb{Q}] \) is at most 6, and it’s not 3, it must be exactly 6. Therefore \( K/\mathbb{Q} \) has Galois group isomorphic to \( S_3 \) since it’s a subgroup of \( S_3 \) of order \( |S_3| \).

2. Let \( f(x) = x^3 - 3x + 1 \). Show that if \( \alpha \) is a root of \( f \) then so is \( \alpha^2 - 2 \). Explicitly write out the Galois group of \( f \).

**Solution:** Let \( \alpha \) be a root of \( f \), so \( \alpha^3 = 3\alpha - 1 \). Then

\[
(\alpha^2 - 2)^3 - 3(\alpha - 2) + 1 = \alpha^6 - 6\alpha^4 + 12\alpha^2 - 8 - 3\alpha^2 + 2 + 1 \\
= \alpha^6 - 6\alpha^4 + 9\alpha^2 - 1 = (3\alpha - 1)^2 - 6\alpha(3\alpha - 1) + 9\alpha^2 - 1 \\
= 9\alpha^2 - 6\alpha + 1 - 6(3\alpha^2 - \alpha) + 9\alpha^2 - 1 = 0,
\]

so \( \alpha^2 - 2 \) is also a root of \( f \). Since \( f \) has three roots, and \( (\alpha^2 - 2)^2 - 2 \) is another root, which is distinct from \( \alpha \) and \( \alpha^2 - 2 \), \( f \) splits completely in \( \mathbb{Q}(\alpha) \). Therefore \( f \) has Galois group isomorphic to \( \mathbb{Z}/3\mathbb{Z} \). In particular, it is generated by the automorphism

\[ \sigma: \alpha \mapsto \alpha^2 - 2, \]

cycling through the 3 roots.

3. Let \( \zeta_5 = e^{2\pi i/5} \). Prove that \( K = \mathbb{Q}(\zeta_5) \) is a splitting field for \( x^5 - 1 \) and determine \( [K: \mathbb{Q}] \).

**Solution:** The polynomial \( x^5 - 1 \) factors over \( \mathbb{Q} \) as

\[ x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1), \]

with the second factor being irreducible over \( \mathbb{Q} \) (we proved this in class) and since \( \zeta_5^5 = 1 \), it is a root of \( x^5 - 1 \). Moreover, the remaining 3 roots are \( \zeta_5^2, \zeta_5^3, \zeta_5^4 \). Therefore \( f \) splits in \( \mathbb{Q}(\zeta_5) \), and this is the splitting field since the splitting field must contain \( \mathbb{Q}(\zeta_5) \). Since \( \zeta_5 \) has degree 4, \( K/\mathbb{Q} \) has degree 4, so the Galois group has order 4 since \( K \) is a splitting field. In particular, the Galois group will be isomorphic to \( (\mathbb{F}_5)^\times \). To see this, we need to show that the Galois group is cyclic. Define

\[ \sigma: \zeta_5 \mapsto \zeta_5^2. \]

This is an automorphism of order 4, since \( \sigma^4: \zeta_5 \mapsto \zeta_5^{2^4} \), hence \( \sigma^2 \) is not the identity, but \( \sigma^4 \) is since \( \zeta_5^{16} = \zeta_5 (\zeta_5^2)^3 = \zeta_5 \). So the Galois group of \( x^5 - 1 \) is cyclic of order 4, generated by \( \sigma \).
It remains to figure out the subgroups of \( \text{Gal}(K/Q) \). Other than the identity and the entire group, there is only one subgroup, which is the group \( H = \{1, \sigma^2\} \). To figure out the fixed field of \( H \) we need to figure out what elements of \( K \) are fixed by \( \sigma^2 \). One can do this in general by writing out a generic element of \( K \) in terms of its basis \( \{1, \zeta_5, \zeta_5^2, \zeta_5^3\} \), applying \( \sigma^2 \) to it, and solving the corresponding relations on the coordinates. This is good practice, but somewhat tedious. We can take a shortcut here by noticing that if take \( \zeta_5 \) and consider its orbit under \( H \). This orbit will be necessarily fixed by \( H \). Hence, if we look at the sum of all the elements in the orbit, that will also be fixed by \( H \). That element isn’t necessarily a generator for the fixed field, but it’s a good candidate, and we’ll show that in this case it is.

The orbit of \( \zeta_5 \) under \( H \) is just \( \{\zeta_5, \zeta_5^4\} \), hence \( \zeta_5 + \zeta_5^4 \) is fixed by \( H \). We know that \( [K^H : Q] = [G : H] = 2 \), hence any element not in \( Q \) will generate the extension. Therefore we have the following diagrams.

4. Let \( K/F \) be a Galois extension such that \( \text{Gal}(K/F) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \). How many intermediate fields \( L \) are there with (a) \( [L : F] = 4 \), (b) \( [L : F] = 9 \), (c) \( \text{Gal}(K/L) \simeq \mathbb{Z}/4\mathbb{Z} \).

**Solution:** Let \( G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \) and consider \( G \) additively (generated by \( (0, 1) \) and \( (1, 0) \)). Unfortunately, the set of subgroups of a direct product is not the set of direct products of the subgroups, so we need to be careful. For this problem, we will need to enumerate the subgroups of \( G \) of order 6, and the subgroups isomorphic to \( \mathbb{Z}/4\mathbb{Z} \). Since every subgroup of \( G \) of order 6 is cyclic (\( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \)), we start by enumerating elements of order 6 and elements of order 4. These are listed below:

- **Order 6:** \((0, 2), (1, 2), (1, 4), (1, 8), (0, 10), (1, 10)\)
- **Order 4:** \((0, 3), (1, 3), (0, 9), (1, 9)\).

From here we see that \((0, 2)\) and \((0, 10)\) generate the same groups, as do \((1, 2)\) and \((1, 10)\), and \((1, 4)\) and \((1, 8)\). So we get three subgroups of order 6. We also have that \((0, 3)\) and \((0, 9)\) generate the same subgroups, as do \((1, 3)\) and \((1, 9)\) so we have two subgroups isomorphic to \( \mathbb{Z}/4\mathbb{Z} \). Now we’re ready to solve the problems.

(a) \([L : F] = 4 \) implies \([G : H] = 4 \), where \( L = K^H \), so \(|H| = 6 \). There are 3 possibilities for \( H \), so there are 3 possibilities for \( L \).

(b) \([L : F] = 9 \) implies \([G : H] = 9 \), where \( L = K^H \), but \( G \) has no subgroup of index 9 since \( 9 \nmid 24 \), so there are no possibilities for \( L \).

(c) \( \text{Gal}(K/L) \simeq \mathbb{Z}/4\mathbb{Z} \) implies that \( L \) is the fixed field of a subgroup of \( H \subseteq G \) isomorphic to \( \mathbb{Z}/4\mathbb{Z} \). There are two possibilities for \( H \) hence there are two possibilities for \( L \).