Solutions to Homework 3

Section 2, Exercises 2, 3, 4, and 6.

Exercise 2. Determine the Galois groups of the following polynomials.
(a) $x^3 - 2$ **(b)** $x^3 + 27x - 4$ **(c)** $x^3 + x + 1$ **(d)** $x^3 + 3x + 14$
(e) $x^3 - 3x^2 + 1$ **(f)** $x^3 - 21x + 7$ **(g)** $x^3 + x^2 - 2x - 1$
(h) $x^3 + x^2 - 2x + 1$

Solution. We know that the Galois group of a polynomial permutes the roots of that polynomial, so the Galois group of a cubic must be a subgroup of S_3. Up to isomorphism, there are only 4 subgroups of S_3: the trivial group, C_2, C_3, and S_3. Since these all have different orders, we only need to find the degree of the Galois group and we will know that Galois group.

There are four cases:

1. If f splits into linear factors over $\mathbb{Q}$, then the splitting field has degree 1, so the Galois group is trivial.

2. If f is reducible over $\mathbb{Q}$, but factors into a linear term and a quadratic term, then the splitting field has degree 2, so the Galois group is C_2.

3. If f is irreducible over $\mathbb{Q}$ and the discriminant is a square in $\mathbb{Q}$, then the splitting field has degree 3, so the Galois group is C_3.

4. If f is irreducible over $\mathbb{Q}$ and the discriminant is not a square in $\mathbb{Q}$, then the splitting field has degree 6, so the Galois group is S_3.

To check irreducibility, we note that a cubic is reducible over some field if and only if it has a root in that field. Then we can use the rational roots theorem, which says that any rational root of a monic polynomial with constant term r/s must be of the form $\pm a/b$, where a divides r and b divides s. We compute the discriminant of $x^3 + px + q$ by $-4p^3 - 27q^2$. For a general polynomial $x^3 + ax^2 + bx + c$, we use the substitution $x = y - a/3$ to get a polynomial in the special form above. We note that since the discriminant depends only on the differences between the roots, this substitution does not affect the discriminant.

(d): factors as $(x-2)(x^2 - 2x + 7)$, and this second factor is irreducible, so the Galois group is C_2.

(e), (f), (g): irreducible with discriminants 81, 35721, and 49, respectively, which are all squares in $\mathbb{Q}$. So the Galois group is C_3.

(a), (b), (c), (h): irreducible with discriminants $-108, -79164, -31, -31$, respectively, none of which is a square in $\mathbb{Q}$. So the Galois group is S_3. □

Exercise 3. Let f be an irreducible cubic polynomial over F, and let δ be the square root of the discriminant of f. Porve that f remains irreducible over the field $F(\delta)$.

Proof. Suppose that f is reducible over $F(\delta)$. Then since f is a cubic, it must have a root α in the field $F(\delta)$. Then we can form a tower of fields

$$F \subseteq F(\alpha) \subseteq F(\delta).$$

But since f is irreducible, $[F(\alpha) : F] = 3$, but $[F(\delta) : F]$ is clearly 1 or 2. This is a contradiction. □

Exercise 4. Let α be a complex root of $f(x) = x^3 + x + 1$ over $\mathbb{Q}$, and let K be a splitting field of this polynomial over $\mathbb{Q}$.

(a) Is $\sqrt{-3}$ in $\mathbb{Q}(\alpha)$? Is it in K?

(b) Prove that $\mathbb{Q}(\alpha)$ has no automorphism except the identity.

Solution. The answer to (a) is no to both questions. Suppose that $\sqrt{-3}$ were in K. Then since the square root of the discriminant (which we calcluated above as $\sqrt{-31}$) can be written in terms of the roots of f, it is also in K. This means that we have two intermediate fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-31})$ that are both degree 2 extensions of $\mathbb{Q}$. By the main Galois theorem, the intermediate fields of degree 2 are in correspondence with the index 2 (order 3) subgroups of the Galois group of f, which we calculated to be S_3. But S_3 only has two elements of order 3, and hence one subgroup of order 3, so this is a contradiction. Of course, this implies also that $\mathbb{Q}(\sqrt{-3})$ is not in $\mathbb{Q}(\alpha)$.

For (b) I will show that α is the only root of f in $\mathbb{Q}(\alpha)$, which implies that there are no non-identity automorphisms of $\mathbb{Q}(\alpha)$. Suppose that another root β of f is in $\mathbb{Q}(\alpha)$. Then since the product of the three roots of f is 1, the third root is equal to $1/(\alpha\beta)$, which must also be in $\mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\alpha)$ must be the splitting field of f. Since f is irreducible, $\mathbb{Q}(\alpha)$ must be a degree 3 extension, which contradicts the fact that the Galois group of f is S_3. □

Exercise 6. Let $f \in \mathbb{Q}[x]$ be an irreducible cubic polynomial which has exactly one real root, and let K be its splitting field over $\mathbb{Q}$. Prove that $[K : \mathbb{Q}] = 6$.

Proof. Let α be the real root of f. Since f is irreducible, $\mathbb{Q}(\alpha)$ is a degree 3 extension of $\mathbb{Q}$. Since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, it does not contain all the roots of f and thus is not equal to K. Hence $[K : \mathbb{Q}] > [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, but we also know that $[K : \mathbb{Q}]$ divides 6, so $[K : \mathbb{Q}] = 6$, as desired. □