In this optional assignment, we exhibit some examples of the inverse Galois problem: which groups occur as Galois groups of finite extensions of \( \mathbb{Q} \)? This assignment will not be collected; you will not be responsible for its contents on the final exam.

At certain points, you may find it useful to make some numerical computations of the roots of polynomials. I’m sure this can be done using Wolfram Alpha, but I couldn’t tell you how. The computer algebra system I generally use is Sage, which is based on Python (and taught in Math 157); it can be used for free via CoCalc (https://cocalc.com).

No office hours Wednesday, May 30. However, if you want to meet by videoconference, let me know and I will set that up. (And no lecture Monday, May 28 because of the Memorial Day holiday.)

Some of the following examples are taken from the “global number fields” section of the L-Functions and Modular Forms Database: http://www.lmfdb.org/.

(1) Artin, chapter 16, exercise M.11. This exercise addresses the question: given an irreducible quartic polynomial \( f(x) \in \mathbb{Q}[x] \), how does one tell whether its Galois group is \( C_4 \) or \( D_4 \)?

(2) (a) Let \( m \) be a positive integer and let \( \Phi_m(x) \in \mathbb{Q}[x] \) be the \( m \)-th cyclotomic polynomial. Prove that for any integer \( n \), every prime divisor of \( \Phi_m(n) \) is either a divisor of \( m \) or is congruent to 1 modulo \( m \). (Hint: if \( p \) is a prime divisor of \( \Phi_m(n) \) not dividing \( m \), then \( \mathbb{F}_p^\times \) is a cyclic group of order \( p - 1 \) containing a cyclic subgroup of order \( m \).)

(b) Using (a), prove that there are infinitely many primes \( m \) congruent to 1 modulo \( n \). (Hint: imitate Euclid’s proof that there are infinitely many primes.) This also follows from Dirichlet’s theorem on primes in arithmetic progressions, but the proof of that requires analytic number theory.

(c) Prove that every abelian group occurs as the Galois group of some Galois extension of \( \mathbb{Q} \).

(3) In this exercise, we realize \( A_4 \) as a Galois group. Let \( f(x) \) be the polynomial \( x^4 - 2x^3 + 2x^2 + 2 \).

(a) Show that \( f \) is irreducible and its discriminant is \( 3136 = 2^6 \times 7^2 \).

(b) Compute the resolvent cubic and check that it is irreducible.

(c) Deduce that the splitting field of \( f \) has Galois group \( A_4 \).

(4) In addition to \( A_4 \) and \( S_3 \times C_2 \), there is a third nonabelian group of order 12. In this exercise, we realize this group as a Galois group. (See Artin, section 7.8 for the classification of groups of order 12.)

(a) Show that \( f(x) = x^3 - 12x - 14 \) is irreducible and its discriminant is \( 1620 = 2^2 \times 3^4 \times 5 \).

(b) Let \( F_1 \) be the splitting field of \( f(x) \) in \( \mathbb{C} \). Show that \( G(F_1/\mathbb{Q}) \cong S_3 \) and \( \mathbb{Q}(\sqrt{5}) \subseteq F_1 \).

(c) Put \( F_2 := \mathbb{Q}(\zeta_6) \) as a subfield of \( \mathbb{C} \). Check that \( F_1 \cap F_2 = \mathbb{Q}(\sqrt{5}) \). (Hint: compare \([F_1 : \mathbb{Q}(\sqrt{5})]\) and \([F_2 : \mathbb{Q}(\sqrt{5})]\).)

(d) Let \( K \) be the compositum of \( F_1 \) and \( F_2 \) in \( \mathbb{C} \) (that is, the subfield of \( \mathbb{C} \) generated by \( F_1 \) and \( F_2 \) together). Prove that \( K \) is a Galois extension of \( \mathbb{Q} \) and \([K : \mathbb{Q}] = 12\).
(e) Show that \( G(K/\mathbb{Q}) \not\cong A_4, S_3 \times C_2 \). (Hint: neither of those groups has a normal subgroup of index 3.)

(5) In this exercise, we realize the quaternion group \( H \) (see Artin, section 2.4) as a Galois group. Let \( K \) be the field \( \mathbb{Q}((\sqrt{2}), \sqrt{3}) \). Let \( G = \{1, g, h, gh\} \) be the Galois group of \( K/\mathbb{Q} \), where the labeling of elements is such that

\[
g(\sqrt{2}) = -\sqrt{2}, \quad g(\sqrt{3}) = \sqrt{3}, \quad h(\sqrt{2}) = \sqrt{2}, \quad h(\sqrt{3}) = -\sqrt{3}.
\]

(a) Check that \( \alpha := (2 + \sqrt{2})(3 + \sqrt{3}) \) is not a square in \( K \). (Hint: if it were, then \( \alpha \cdot g(\alpha) \) would be a square in \( \mathbb{Q}(\sqrt{3}) \), but this product is \( 2(3 + \sqrt{3})^2 \).)

(b) Prove that \( g(\alpha)/\alpha \) and \( h(\alpha)/\alpha \) are squares in \( K \). Note that this implies that \( (gh)(\alpha)\alpha = g \left( \frac{h(\alpha)}{\alpha} \right) g(\alpha) \alpha \) is a square in \( K \).

(c) Let \( L \) be the field \( K(\sqrt{\alpha}) \); by (a), \( [L : \mathbb{Q}] = 8 \). Find automorphisms \( \tilde{g}, \tilde{h} \in G(L/\mathbb{Q}) \) restricting to \( g, h \in G(K/\mathbb{Q}) \).

(d) Show that \( L/\mathbb{Q} \) is Galois and that \( G(L/\mathbb{Q}) \cong H \).

(6) In this exercise, we realize \( D_5 \) as a Galois group. Define the polynomial \( f(x) = x^5 - 2x^4 + 2x^3 - x^2 + 1 \). Let \( K \) be the splitting field of \( f \) over \( \mathbb{Q} \) in \( \mathbb{C} \) and put \( G := G(K/\mathbb{Q}) \).

(a) Prove that \( f \) is irreducible over \( \mathbb{F}_2 \), then use Gauss’s lemma to deduce that \( f \) is also irreducible over \( \mathbb{Q} \).

(b) Make a numerical computation of the five roots \( \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \) and check that the discriminant of \( f \) equals \( 47^2 \). Deduce that \( G \subseteq A_5 \).

(c) Observe that only one of the five roots of \( f \) is real. Deduce that \( G \) contains a double transposition; in particular, \( G \not\cong C_5 \).

(d) Show that the roots can be labeled in such a way that

\[
\alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \alpha_3 \alpha_4 + \alpha_4 \alpha_5 + \alpha_5 \alpha_1 = 3.
\]

Then show (by averaging over \( G \)) that if \( G = A_5 \), this would imply that

\[
\sum_{1 \leq i < j \leq 5} \alpha_i \alpha_j = 6
\]

whereas this sum is actually 2. Deduce that \( G \not\cong A_5 \) and hence \( G = D_5 \).

(7) In this exercise, we realize \( A_5 \) as a Galois group. Define the polynomial \( f(x) = x^5 - x^4 + 2x^2 - 2x + 2 \) and let \( K \) be the splitting field of \( f \) over \( \mathbb{Q} \) in \( \mathbb{C} \).

(a) Check that \( f \) is irreducible using Eisenstein’s criterion.

(b) Compute that the discriminant of \( f \) is \( 2^6 \cdot 17^2 \), a perfect square.

(c) Check that \( f \) has exactly two roots in \( \mathbb{F}_{11} \).

(d) There is a theorem (not proved in class) that states: for any prime \( p \) such that \( f \) has no repeated factors in \( \mathbb{F}_p \), the factor structure of \( f \) in \( \mathbb{F}_p \) is the cycle structure of some element of \( G(K/\mathbb{Q}) \). Using this fact, show that \( G(K/\mathbb{Q}) \cong A_5 \).