Problems

1. Draw a diagram of all the subfields of $\mathbf{Q}(\zeta_{17})$, with a line between any pair of fields $E \subset F$ indicating the degree of the corresponding extension.

2. Let $F = \mathbf{C}(x_1, x_2, \ldots, x_n)$ be the field of fractions of the polynomial ring $\mathbf{C}[x_1, \ldots, x_n]$. Let s_i denote the elementary symmetric polynomials in the x_i, that is,

$$\begin{aligned} s_1 &= x_1 + x_2 + \ldots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n \\ &\ddots \\ s_n &= x_1x_2 \ldots x_n. \end{aligned}$$

   Let $E = \mathbf{C}(s_1, \ldots, s_n)$. Prove that, with respect to the natural inclusion $E \subset F$, that:

   (a) F/E is a finite Galois extension.
   (b) $\mathrm{Gal}(F/E) = S_n$.

3. **Imprimitive subgroups.** Let G act on a set A of n points. Recall that G is imprimitive (equivalently, not primitive) if and only if there does exists a decomposition

$$A = \coprod A_i$$

   of A into distinct sets A_i such that:

   - There is at least one i such that $|A_i| \geq 2$.
   - If $g \in G$ and a, $a' \in A_i$, then $g.a$ and $g.a'$ both lie in A_j for some j.

   Let G be a finite group which acts on a set A.

   (a) If G is not transitive, prove that G is not imprimitive by taking A_i to be the orbits of G.
   (b) Say that G is 2-transtive if, for any two pairs (a_1, a_2) and (a_1', a_2') of distinct elements of A, there exists a $g \in G$ such that $g(a_1) = a_1'$ and $g(a_2) = a_2'$. If G is 2-transitive, prove that G is primitive.
   (c) If G is transitive, but not primitive, prove that $|A_i| = |A_j|$ for all i and j.
   (d) Deduce that if G is transitive, and $|A|$ is prime, then G is primitive.
   (e) Suppose that G is transitive, imprimitive, and acts faithfully on A.
      i. Let B denote the set of sets $\{A_i\}$. Prove that G acts transitively on B.
      ii. Show there exists integers a, b, and n such that $|A| = n$, $|B| = b$, $|A_i| = a$ for all i, and $ab = n$.
      iii. Let H denote the kernel of G acting on B. Prove that H is isomorphic to a subgroup of $(S_a)^b = S_a \times S_a \times \ldots S_a$.
      iv. Prove that G/H is isomorphic to a subgroup of S_b.
      v. Deduce that G has order dividing $b! \cdot (a)!^b$.
      vi. Let N be any group which acts faithfully and transitively on a points, and let Γ be any group which acts faithfully and transitively on b points. Prove that there is a group $N \wr \Gamma$ which acts faithfully, transitively, and imprimitively on a set A of order $n = ab$ points, where G preserves a decomposition of A into sets A_i of order $|A_i| = a$, where the action of G onto the set B of sets $\{A_i\}$ factors through Γ, and where the kernel of this action is $H = N^b$.

vii. Prove that G is subgroup of $S_a \wr S_b$.

(f) Prove that the 2-Sylow of S_4 is $S_2 \wr S_2$.

(g) Prove that the 3-Sylow of S_9 is $\mathbf{Z}/3\mathbf{Z} \wr \mathbf{Z}/3\mathbf{Z}$.

(h) If N is the p-Sylow of S_{p^n}, prove that $N \wr \mathbf{Z}/p\mathbf{Z}$ is the p-Sylow of $S_{p^{n+1}}$.

(i) Deduce that any p-group is a subgroup of $\mathbf{Z}/p\mathbf{Z} \wr \mathbf{Z}/p\mathbf{Z} \wr \mathbf{Z}/p\mathbf{Z} \dots \mathbf{Z}/p\mathbf{Z}$.

(j) Deduce that any p-group is solvable.

(k) Find out what a Rubix cube is.

(l) Let G be the group defined by the possible combinations of moves.

(m) Prove that the action of G on the $9 \cdot 6 = 54$ has orbits of size 24, 24, and 6 orbits of size 1.

(n) Prove that G admits a quotient N which is a subgroup of S_{24} by showing that some quotient acts faithfully on the corner squares.

(o) Prove that the action of N on the corner squares is imprimitive, by taking A_i to be the triples of squares along each corner.

(p) Deduce that N is a subgroup of $S_3 \wr S_8$, and hence $|N|$ divides $3!^8 \cdot 8! = 67722117120$.

(q) Prove that the stabilizer H in N of the cubes always preserves the orientation of the triple of colours around the corners, and hence that H is actually a subgroup of $(\mathbf{Z}/3\mathbf{Z})^8$.

(r) Deduce that N is a subgroup of $(\mathbf{Z}/3\mathbf{Z}) \wr S_8$, and hence $|N|$ divides $3^8 \cdot 8! = 264539520$. (Actually, N has index 2 in $(\mathbf{Z}/3\mathbf{Z}) \wr S_8$.)

(s) Let M be the quotient on which G acts on the edge squares of the cube. Prove that M is a subgroup of S_{24}.

(t) Prove that M acts imprimively on the set of edges, since it preserves the squares on each pair.

(u) Deduce that M is a subgroup of $\mathbf{Z}/2\mathbf{Z} \wr S_{12}$.

(v) Prove that G is a subgroup of $M \oplus N$.

(w) Deduce that G is a subgroup of

$$(\mathbf{Z}/3\mathbf{Z}) \wr S_8 \oplus (\mathbf{Z}/2\mathbf{Z}) \wr S_{12},$$

and hence that G has order dividing

$$|G| = 3^8 \cdot 8! \cdot 2^{12} \cdot 12! = 519024039293878272000.$$

(In fact, it turns out that G has index 12 in this group.)

4. Let L/K be Galois with Galois group Γ. Let M/L be Galois with Galois group N. Show that the Galois closure N/K of M/K is Galois with Galois group a subgroup of $N \wr \Gamma$.

5. Prove that $\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}$.

6. (14.5 (10) Prove that $\mathbf{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbf{Q}$.

7. (See 14.6 (2),(4),(5),(6),(7),(8),(9),(10)) Determine the Galois group of the following polynomials:

   (a) $x^3 - x^2 - 4$.
   (b) $x^3 - 2x + 4$.
   (c) $x^3 - x + 1$.
   (d) $x^3 + x^2 - 2x - 1$.
   (e) $x^4 - 25$.
   (f) $x^4 + 4$.
   (g) $x^4 + 3x^3 - 3x - 2$.
   (h) $x^4 + 8x + 12$.
   (i) $x^4 + 4x - 1$.
   (j) $x^5 + x - 1$.

8. Let $K/\mathbf{Q}$ be a Galois extension.

   (a) If $[K : \mathbf{Q}] = 2009$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.
   (b) If $[K : \mathbf{Q}] = 2010$, prove that K contains an extension E with $[E : \mathbf{Q}] = 2$.
   (c) If $[K : \mathbf{Q}] = 2011$, prove that $\mathrm{Gal}(K/\mathbf{Q})$ is abelian.
   (d) If $[K : \mathbf{Q}] = 2012$, prove that K contains an extension E with $[E : \mathbf{Q}] = 503$.
   (e) If $[K : \mathbf{Q}] = 2013$, prove that K contains an extension E with $[E : \mathbf{Q}] = 3$.