GALOIS THEORY
Worksheet 10

Q 1. In this question $\zeta = e^{\frac{2\pi\,\mathrm{i}}{6}}$.

(a) Factorise the polynomial $X^6 - 1 \in \mathbb{Q}[X]$. Hence or otherwise determine the degree $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

(b) Show that the polynomial $f(X) = X^6 + 3 \in \mathbb{Q}[X]$ is irreducible. Let $\mathbb{Q} \subset K$ be the splitting field of $f(X)$. What is the degree $[K : \mathbb{Q}]$?. Determine the Galois group G of the extension $\mathbb{Q} \subset K$ and describe, perhaps by drawing some picture(s), the action of G on the set of roots of $f(X)$.

[*Hint*: Consider first the field $\mathbb{Q}(\alpha)$ where $f(\alpha) = 0$ and study the intersection $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\zeta)$.]

(c) Let $\mathbb{Q} \subset L$ be the splitting field of the polynomial $g(X) = X^6 - 3 \in \mathbb{Q}[X]$. Compute the degree $[L : \mathbb{Q}]$, determine the Galois group G of the extension $\mathbb{Q} \subset L$ and describe, perhaps by drawing some picture(s), the action of G on the set of roots of $g(X)$.

Q 2. (†) For all integers $3 \leq n \leq 16$, draw pictures illustrating the lattice of subgroups of the Galois group of the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$. Draw the corresponding picture of subfields $\mathbb{Q} \subset F \subset \mathbb{Q}(\mu_n)$. For each of these subfields, find "natural" generators.

If you feel brave, then do the case $n = 17$. (The Galois group $(\mathbb{Z}/17\mathbb{Z})^\times = C_{16}$ is not in and of itself very complicated. The field $\mathbb{Q}(\mu_{17})$ is a tower of quadratic extensions but it takes some elbow grease to determine at each stage what you are taking the square root of; in particular this leads to a formula for $\cos\frac{2\pi}{17}$ involving just iterated square roots of rational numbers. Gauss did this calculation in his teens and it led him to a construction of the regular 17-gon with ruler and compass. You don't yourself need to get to the bitter end of the calculation: do the first couple of steps and then look up the last steps on Google.)

Q 3. Fix a positive integer n and a field k — for simplicity assumed to be of characteristic 0 — that contains all n^{th} roots of unity. In this question you will construct a splitting field $K \subset L$ of a degree n irreducible polynomial $f(X) \in K[X]$ of Galois group the full symmetric group $G = \mathfrak{S}_n$ of the roots of $f(X)$.

Consider the field L and polynomial $f(X) \in L[X]$:

$$L = k(X_1, \dots X_n), \quad f(X) = \prod_{i=1}^{n}(X - X_i) \in L[X]$$

Now let the symmetric group $\mathfrak{S}_n$ act on L by permuting the variables in the obvious way. By definition the fixed field

$$K = L^{\mathfrak{S}_n} = \mathfrak{S}_n^\star$$

is the field of *symmetric rational functions*. The polynomial $f(X)$ is actually in $K[X]$:

$$f(X) = X^n + \sum_{i=1}^{n} (-1)^i \sigma_i X^{n-i} \in K[X]$$

where $\sigma_i = \sigma_i(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]^{\mathfrak{S}_n} \subset K$ is the i^{th} elementary symmetric *polynomial*. Denote by

$$K' = \mathrm{Frac}\Big(k[\sigma_1, \ldots, \sigma_n]\Big) \subset K$$

the subfield of K generated by the elementary symmetric polynomials.[1]

(a) Prove that $K' \subset L$ is the splitting field of $f(X)$;

(b) Prove that the Galois group of the extension $K' \subset L$ is the full permutation group $\mathfrak{S}_n$ on the roots of $f(X)$;

(c) Hence prove that $K' = K$ and that the polynomial $f(X) \in K[X]$ is irreducible;

(d) Show that the statement $K' = K$ also follows from Question 6 of Worksheet 7.

[1] That is, the fraction field of the ring generated by the elementary symmetric polynomials. The ring generated by the elementary symmetric polynomials is a subring of $k[X_1, \ldots, X_n]$ hence it is an integral domain hence forming the fraction field is a standard and uncontroversial operation.

You can be more concrete: by Question 6 of Worksheet 7, the ring generated by the elementary symmetric polynomials is itself a polynomial ring, that is, there are no algebraic relations between the elementary symmetric polynomials, and hence its fraction field is just a ring of rational functions. We are not invoking this here, however: at least part of the point of this question is to bypass Question 6 of Worksheet 7.