GALOIS THEORY
Solutions to Worksheet 10

A 1. (a) $X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1)$ and

$$\zeta = \frac{1 + \mathtt{i}\sqrt{3}}{2} \quad \text{is a root of} \quad \Phi_6(X) = X^2 - X + 1 \in \mathbb{Q}[X]$$

Since $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ is the splitting field of $\Phi_6(X)$, we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.

(b) The goal is to compute the Galois group over $\mathbb{Q}$ of the splitting field K of the polynomial

$$f(X) = X^6 + 3 \in \mathbb{Q}[X]$$

Now $f(X)$ is irreducible (Eisenstein at $p = 3$) so if α is a root then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. In fact let us take $\alpha = \mathtt{i}\sqrt[6]{3} \in \mathbb{C}$; we see that $\alpha^3 = \mathtt{i}\sqrt{3}$ so

$$F = \mathbb{Q}(\alpha^3) = \mathbb{Q}(\mathtt{i}\sqrt{3}) \subset K$$

and in fact all of the following statements are true and I will use them freely below:

(1) F is the splitting field of $X^6 - 1$ over $\mathbb{Q}$; in other words, F is the field $\mathbb{Q}(\mu_6)$ of 6^{th} roots of unity;

(2) F is the splitting field of $X^3 - 1$ over $\mathbb{Q}$; in other words, F is the field $\mathbb{Q}(\mu_3)$ of 3^{rd} roots of unity (and I write $\omega = \frac{1+\mathtt{i}\sqrt{3}}{2} \in F$);

(3) $[F : \mathbb{Q}] = 2$ and the Galois group is generated by the complex conjugation.

From (1) we conclude that $K = \mathbb{Q}(\alpha)$ and then $|G| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

Corresponding to the tower $\mathbb{Q} \subset F \subset K$ we have an exact sequence of groups

$$1 \to H \to G \to G/H \to 1$$

where:

(i) G is the Galois group we want to study;

(ii) $H = F^\dagger \leq G$ is the Galois group of the normal extension $F \subset K$. By the tower law $|H| = [K : F] = 3$, hence $H \cong C_3$ is a cyclic group of order 3;

(iii) In fact H is a *normal* subgroup of G (because all index two subgroups of a finite group are normal; because we know that $\mathbb{Q} \subset F$ is a normal extension; etc.) and the quotient $G/H = C_2$ is the Galois group of $\mathbb{Q} \subset F$;

(iv) Complex conjugation is an element of G that *lifts* the generator of G/H: this shows that G is a semidirect product $G = H \rtimes C_2$. (The existence of *some* lift, and hence the semidirect product structure, also follows from simple pure-algebra facts about groups of order 6. However, complex conjugation provides a *natural* lift.)

The final point is to determine the structure of G and the action of G on the roots. By what we said above G is generated by H and complex conjugation τ. We know how τ operates so we only really need to study the operation of H.

Now H is the Galois group of the degree 3 extension $F \subset K$. We have that

$$X^6 + 3 = (X^3 + \mathtt{i}\sqrt{3})(X^3 - \mathtt{i}\sqrt{3}) \in F[X]$$

is the prime decomposition of $f(X) \in F[X]$ (how do I know this?) and $F \subset K$ is the splitting field of either of the two factors. Writing $\alpha = \mathtt{i}\sqrt[6]{3}$, $\beta = -\mathtt{i}\sqrt[6]{3}$, the six roots of $X^6 + 3$ are:

$$\alpha, \omega\alpha, \omega^2\alpha, \beta, \omega\beta, \omega^2\beta$$

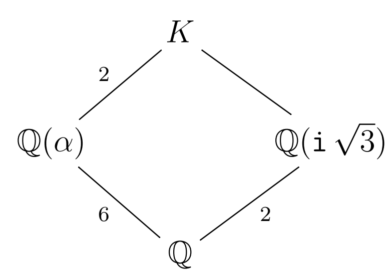
where the first three roots are roots of the first factor in the decomposition, and the other roots are roots of the second factor. Draw a picture! It follows that we can identify H with μ_3 operating on the set of roots by multiplication (how do I know this? There is an element $\sigma \in H$ that maps $\alpha_1 = \alpha$ to $\alpha_2 = \omega\alpha$ — transitivity of action of H — so now: prove that σ acts on the set of six roots as multiplication by ω!).

At this point we can show that $G = \mathfrak{S}_3$ and to draw the action on the set of roots. Indeed for example

$$\tau\omega\tau(\alpha) = \tau(\omega\beta) = \omega^2\alpha$$

so $\tau\omega\tau = \omega^2$.

(c) As before $X^6 - 3 \in \mathbb{Q}[X]$ is irreducible. Let $\alpha \in \mathbb{R}$, $\alpha^6 = 3$. As before $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ but now, because $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\zeta \notin \mathbb{Q}(\alpha)$ and $\Phi_6(X)$ remains irreducible in $\mathbb{Q}(\alpha)$. We have a diagram of fields



The diagram shows that $[K : \mathbb{Q}] = 12$. The situation at this point is similar to $X^4 - 2 \in \mathbb{Q}[X]$ — which was discussed at length in class — and you can treat it in a similar fashion: an element $\sigma \in G$ is completely determined once you know: $\sigma(\alpha)$ (6 possibilities) and $\sigma(\zeta)$ (two possibilities) for a total of 12 possibilities. Because $|G| = 12$ all these possibilities are realised, and it is not hard to see that one gets the dihedral group D_{12}.

A 2. I am sorry, I can't write this down for you. You do it.

A 3. I only sketch this.

(a) This is obvious: the polynomial splits and L is generated by the roots.

(b) $\mathfrak{S}_n$ acts on L fixing K'...

(c) ...but actually $\mathfrak{S}_n$ fixes the larger field K hence $K' = K$. The polynomial is irreducible because the Galois group acts transitively on the roots.

(d) This follows from taking fields of fractions of the rings in the statement from Question 6 of Worksheet 7.