HOMEWORK #10
SOLUTIONS TO SELECTED PROBLEMS

Problem 10.6. The idea is to use the theorems that show the existence of elements with special cycle structure (when viewed as permutation on the roots). Here are a few examples.

The polynomial $f(t) = t^5 - 4t + 2$. $f(t)$ is irreducible over $\mathbb{Q}$ by Eisenstein criterion with the prime 2. Evaluating, we see that $f(-1) = 5$ and $f(1) = -1$ so f has a root in $[-1, 1]$. Moreover, $f'(t) = 5t^4 - 4$ and $f''(t) = 20t^3$ so f has a local maximum at $t_0 = -\sqrt[4]{4/5} > -1$ (so $f(t_0) > 0$) and a local minimum at $t_1 = \sqrt[4]{4/5} < 1$ (so $f(t_1) < 0$). But $\lim_{x\to-\infty} f(x) = -\infty$ and $\lim_{x\to\infty} f(x) = \infty$, so there are two more roots, one smaller than -1 and the other larger than 1. The above considerations show that f has exactly three real roots. By using the appropriate theorem on irreducible polynomials of degree p having exactly $p-2$ real roots, we see that the Galois group of the splitting field of f over $\mathbb{Q}$ is S_5.

The polynomial $f(t) = t^4 + 2t^2 + t + 3$. Here we will examine the reduction of f modulo various primes p.

Reducing modulo 2, we get $t^4 + t + 1$ over $\mathbb{F}_2$. We check that there are no roots in $\mathbb{F}_2$, so the only possible factorization is of the form

$$t^4+t+1 = (t^2+at+b)(t^2+ct+d) = t^4+(a+c)t^3+(b+d+ac)t^2+(ad+bc)t+bd$$

but then $a + c = 0$ (coefficient of t^3) and $b = d = 1$ (coefficient of t^0), but then $ad + bc = a + c = 0$ contradicting $ad + bc = 1$ (coefficient of t^1).

We proved that the reduction of f modulo 2 is irreducible. This shows that f is irreducible in $\mathbb{Z}[t]$, since any factorization in $\mathbb{Z}[t]$ can be reduced to a factorization in $\mathbb{F}_2[t]$. By Gauss lemma, f is irreducible in $\mathbb{Q}[t]$. Moreover, by the Theorem 10.1, we get an element in the Galois group of f which is a cycle of length 4.

Now we reduce modulo 3. We get $t^4 + 2t^2 + t \in \mathbb{F}_3[t]$. Obviously, we have a factorization $t^4+2t^2+t = t(t^3+2t+1)$. The factor t^3+2t+1 is irreducible since it is of degree 3 and has no roots in $\mathbb{F}_3$. Again, by Theorem 10.1, we get an element in the Galois group of f which is a cycle of length 3.

We can label the roots so that the cycle of length 4 is $\sigma_4 = (1234)$. The cycle of length 3, σ_3, involves three labels, so by conjugation with an appropriate power of σ_4 we can assume that $\sigma_3 = (123)$. But now $\sigma_4^{-1}\sigma_3 = (4321)(123) = (34)$ is a simple transposition of adjacent labels, so the group generated by σ_3 and σ_4 contains a cycle of length 4 and a simple transposition of adjacent elements, hence it is equal to S_4.

We conclude that the Galois group of (the splitting field of) f over $\mathbb{Q}$ is S_4.