MA 3419: Galois theory
Selected answers/solutions to the assignment due November 28, 2017

1. (**a**) Note that this polynomial is irreducible (Eisenstein for $p = 2$). Also, we note that $f(100) > 0$, $f(1) = -1 < 0$, $f(-1) = 5 > 0$, $f(-100) < 0$, so this polynomial has at least three real roots, and $f'(x) = 5x^4 - 4$, so this polynomial has two extrema, which means that it cannot have more than three roots. Thus, two of the roots are complex conjugate, and hence the Galois group contains a transposition (induced by the complex conjugation). We know from class that a transitive subgroup of S_5 (transitivity follows from irreducibility) containing a transposition must coincide with S_5.

(**b**) This polynomial is irreducible (Eisenstein for $p = 2$ again), and $f(100) > 0$, $f(1) = -1 < 0$, $f(-100) > 0$, so there are at least two real roots. Also, $f'(x) = 4x^3 - 4$, so the only extremal point is at $x = 1$. This means that this polynomial cannot have more than two roots. Thus, two of the root are complex conjugate, and the Galois group contains a transposition. Two only transitive subgroups of S_4 containing a transposition are D_4 and S_4.

Let a_1, a_2, a_3, a_4 be the roots of this polynomial; consider, as we discussed in class in the beginning of this semester, the quantities x_1, x_2, x_3 determined by

$$\begin{aligned} 2a_1 &= x_1 + x_2 + x_3, \\ 2a_2 &= x_1 - x_2 - x_3, \\ 2a_3 &= -x_1 + x_2 - x_3, \\ 2a_4 &= -x_1 - x_2 + x_3. \end{aligned}$$

We have

$$\begin{gathered} x_1^2 + x_2^2 + x_3^2 = 0, \\ x_1x_2x_3 = -4, \\ x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = -8. \end{gathered}$$

Thus, x_1^2, x_2^2, x_3^2 are roots of the polynomial

$$t^3 - 8t - 16 = 0.$$

This polynomial is irreducible over rational numbers because it has no rational roots. This means that the splitting field contains a subfield of degree 3, and hence the cardinality of the Galois group is divisible by 3, which rules out the case of D_4. Therefore the Galois group is S_4.

2. Without loss of generality, the cycle is (123). By transitivity, each element 1,2,3,4,5 is involved in at least one 3-cycle, so there is another 3-cycle involving at least one other element. Without loss of generality, that cycle is (124) or (145). In the latter case, $(145)(123)(145)^{-1} = (234)$. Thus, our subgroup contains either the subgroup generated by (123) and (124) or the subgroup generated by (123) and (234). These subgroups are clearly transitive on $\{1, 2, 3, 4\}$. Note that a group that acts transitively on a set of n elements has cardinality divisible by n, since the cardinality of an orbit of x is the index of the stabiliser of x. Therefore, the cardinality of our subgroup is divisible by 3 (as it contains a 3-cycle), by 4 (as its subgroup acts transitively on a 4-element set), and by 5 (since it acts transitively on a 5-element set), which means that it is divisible by $3 \cdot 4 \cdot 5 = 60$, which is already the cardinality of A_5.

3. (**a**) Without loss of generality the n-cycle is $\sigma = (1, 2, \dots, n)$, and the transposition is (i, j) for some $1 \leqslant i < j \leqslant n$. There exists $k < n$ for which $\tau = \sigma^k$ satisfies $\tau(i) = j$; note that since n is prime, the element τ is also an n-cycle. Consider the permutation $\mu = \tau \cdot (ij)$. We have $\mu(j) = j$, and all other elements are permuted cyclically, so μ is an $(n-1)$-cycle, and a result from class applies. (The subgroup is transitive because it contains σ.)

(**b**) In case of S_4, the subgroup D_4 satisfies this property.

4. The polynomial $x(x-1)\cdots(x-(p-4))$ has $p-3$ simple roots, each of which is close to one simple root of

$$x^p - N^3p^3x(x-1)\cdots(x-(p-4)) - p = N^3p^3\left(\frac{1}{N^3p^3}(x^p - p) - x(x-1)\cdots(x-(p-4))\right).$$

Also, there is one simple root close to Np, since

$$x^p - N^3p^3x(x-1)\cdots(x-(p-4)) - p = (Np)^p\left(\left(\frac{x}{Np}\right)^p - \frac{x}{Np}\left(\frac{x}{Np} - \frac{1}{Np}\right)\cdots\left(\frac{x}{Np} - \frac{p-4}{Np}\right) - \frac{p}{(Np)^p}\right).$$

This already gives $p-2$ roots. If there were more roots, there would be p of them, and there will be at least one root different from the roots we found (possibly with multiplicity 2). Then by Rolle theorem, the derivative of this polynomial would have at least $p-2$ different roots, ..., the $p-3$-rd derivative would have at least 2 different roots. But that derivative is of the form $Ax^3 - B$, which has just one real root. This implies that the Galois group of the splitting field of this polynomial contains a transposition (corresponding to the complex conjugation). Also, by Eisenstein this polynomial is irreducible, so the Galois group is a transitive subgroup of S_p. The number of elements in the orbit, that is p, divides the order of the subgroup, which divides the order of S_p, that is $p!$, so the maximal power of p dividing the order of the subgroup is p, and by Sylow's theorem it contains a subgroup of order p. The only elements of order p in S_p are p-cycles, and the previous problem applies.

5. (**a**) Note that $[L \colon K] = p^2$, since we adjoin two p-th roots. (The polynomial $t^p - x$ is irreducible over K, and the polynomial $t^p - y$ is irreducible over $K(\sqrt[p]{x})$, by Eisenstein). However, it is clear by direct inspection that for each element of $a \in L$, we have $a^p \in K$, so $K(a)$ generates an extension of degree at most p.

(**b**) Each element $\sqrt[p]{x} + a\sqrt[p]{y}$, where $a \in k$, generates a nontrivial subfield which is a degree p extension of K, and these fields are clearly distinct, as if a subfield contains $\sqrt[p]{x} + a\sqrt[p]{y}$ and $\sqrt[p]{x} + b\sqrt[p]{y}$ for $a \neq b$, then it contains both $\sqrt[p]{x}$ and $\sqrt[p]{y}$.

6. (**a**) First of all, an extension of a field K has the same characteristic as K, so $p = p'$. Also, an extension of a field K is a vector space over K, so an extension of $\mathbb{F}_q$ has q^m elements, where m is the dimension of the extension as a vector space over $\mathbb{F}_q$. Thus, $p^n = (p^{n'})^m$, and $n = n'm$.

(**b**) We know that $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, so it is normal. It is manifestly an extension of a finite degree n. Finally, an extension of finite fields is always separable.

(**c**) We have $(xy)^p = x^py^p$, and $(x+y)^p = x^p + y^p$ (the latter because we are in characteristic p), so $x \mapsto x^p$ is an automorphism. The k-th power of it is $x \mapsto x^{p^k}$, which is different from $x \mapsto x$ for $k < n$, since the multiplicative group of $\mathbb{F}_{p^n}$ is cyclic, and therefore contains an element of order $p^n - 1$; for such an element η, we have $\eta^{p^k} \neq \eta$ for $k < n$. A Galois extension has a Galois group of order equal to the degree, so we found all automorphisms.

(**d**) If n is divisible by n', then every root of $x^{p^{n'}} - x$ is a root of $x^{p^n} - x$, since $p^n - 1$ is divisible by $p^{n'} - 1$, therefore there is inclusion between splitting fields.

(**e**) As before, it is normal and separable and finite. The Galois group is the group of all elements fixing $\mathbb{F}_{p^{n'}}$, that is the subgroup generated by $x \mapsto x^{p^{n'}}$. This subgroup is isomorphic to $\mathbb{Z}/(n/n')\mathbb{Z}$. A Galois extension has a Galois group of order equal to the degree, so we found all automorphisms.