Algebra II, Spring 2017

Solutions to Problem Set 3

1. Since F is finite, it is of characteristic p for some prime p. So $\mathbf{F}_p \subset F$. We proved in class that any finite extension of $\mathbf{F}_p$ is Galois with a cyclic Galois group. So $\mathbf{F}_p \subset E$ is Galois, therefore, $F \subset E$ is also Galois and since $\mathrm{Gal(E/F)} \leq \mathrm{Gal(E/\mathbf{F}_p)}$, Gal(E/F) is cyclic too.

2. Clearly $\{x^i y^j \mid 0 \leq i, j \leq p-1\}$ form a basis for E over F, so $[E : F] = p^2$. To show E is not generated over F by one element, it is enough to show there are infinitely many intermediate fields. Clearly F has infinitely many elements. For every $\alpha \in F$, let $F_\alpha = F(x + \alpha y) \subset E$. Then if $\alpha \neq \beta \in F$, $F_\alpha \neq F_\beta$: if $x + \alpha y \in F_\beta$, then since $x + \beta y \in F_\beta$, we have $x, y \in F_\beta$, so $F_\beta = E$ which is not possible since $(x + \beta y)^p = x^p + \beta^p y^p \in F$, so $[F_\beta : F] \leq p$.

3. Let E be the splitting field of $f(x)$ and G the Galois group of E/F. Our assumption implies that G is a subgroup of A_5 and therefore, its order divides 60. Also, $5 || G|$ since if a is any root of $f(x)$, $F \subset F(a) \subset E$, and $[F(a) : F] = 5$, so $5 \mid [E : F] = |G|$. We also know that G is a transitive subgroup of A_5. So $|G| = 5, 10, 15, 20, 30$, or 60.

The order of G cannot be 30 because A_5 has no subgroup of order 30 (a subgroup of order 30 is of index 2 in A_5 and so it is a normal subgroup, but A_5 is a simple group.) The order of G cannot be 15 because we have proved before that every group of order 15 is cyclic, but there is no element of order 15 in S_5. We show that the order of G cannot be 20 either: Every group of order 20 has a subgroup H of order 4. The only permutation in S_5 of order 4 is a cycle $(a\ b\ c\ d)$ which is an odd permutation. So H has to be isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$. Every even permutation of order 2 is S_5 is a product of two disjoint 2-cycles. Assume $H = \{e, g, h, gh\}$ and $g = (1\ 2)(3\ 4)$. Then h is also a product of two cycles $(a\ b)(c\ d)$ none of which can contain 5, because if for example, $(a\ b) = (1\ 5)$, then $gh(1) = 5, gh(5) = 2$, so gh will not be of order 2. So $\{a, b, c, d\} = \{1, 2, 3, 4\}$ and without loss of generality, we can assume $h = (1\ 3)(2\ 4)$ and therefore $gh = (1\ 4)(2\ 3)$. Now H also contains a subgroup of order 5 and therefore an element of order 5, σ. Then σ is a cycle of length 5, and without loss of generality, we can assume $\sigma = (1\ 2\ 3\ 4\ 5)$. Then $g\sigma = (2\ 4\ 5)$ is an element of order 3 which is in H, a contradiction.

So the only possibilities for the order of G are 5, 10, or 60. It easy to see that A_5 has transitive subgroups of order 5 (the subgroup generated by any cycle of order 5), order 10 (the subgroup generated by $(1\ 2)(4\ 5)$ and $(1\ 2\ 3\ 4\ 5)$. This subgroup is isomorphic to the Dihedral group. A_5 has no cyclic group of order 10 since there is no permutation of order 10 in S_5), and of order 60 (A_5).

Next we show that if G is any transitive subgroup of S_5, it is the Galois group of an irreducible polynomial. We showed in class there is an irreducible polynomial of degree 5 $f(x)$ over $\mathbf{Q}$ whose Galois group is S_5. Let E be the splitting field of $f(x)$ and F the fixed field of G. We have $\mathbf{Q} \subset F \subset E$ and Gal(E/F) = G. So it is enough to show that E is the splitting field of an irreducible polynomial of degree 5 in $F[x]$. We show that $f(x)$ as a polynomial in $F[x]$ is irreducible. If $f(x) = g(x)h(x) \in F[x]$, then every element of the Galois group of E/F sends roots of g to roots of g and therefore a root of g cannot be sent to a root of h so $G =$ Gal(E/F) cannot be transitive. So our assumption on G implies that $f(x)$ is irreducible considered as a polynomial in $F[x]$, and obviously E is the splitting field of $f(x) \in F[x]$. Therefore all the three groups $\mathbf{Z}_5$, D_{10} and A_5 can be the Galois group of an irreducible polynomial of degree 5.

4. (a) We have shown that for every n, the splitting field E of $x^{p^n} - x \in \mathbf{F}_p[x]$ is an extension of degree n over $\mathbf{F}_p$. If α is a generator of the group $F^\times$, and if $f(x) \in \mathbf{F}_p[x]$ is the minimal polynomial of α, then $f(x)$ is an irreducible polynomial of degree equal to the degree of $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = [E : \mathbf{F}_p] = n$.

(b) Let $g(x) = a_n x^n + \cdots + a_0 \in \mathbf{Z}[x]$ be a (possibly reducible) polynomial of degree n with exactly $n-2$ real roots. Let $\epsilon > 0$ be so that for every polynomial $h(x) = b_n x^n + \cdots + b_0 \in \mathbf{Q}[x]$ such that $|b_i - a_i| < \epsilon$ for all i, then $h(x)$ has also $n-2$ real roots. Let $f(x) = c_n x^n + \cdots + c_0$ $(0 \le c_i \le p-1)$ be the irreducible polynomial constructed in part (a). Then for every i, there is $0 \le m_i < p$ such that $a_i - m_i = c_i$ mod p. So the polynomial $\sum_{i=0}^n (a_i - m_i)x^i$ is irreducible since it is irreducible mod p. Pick N large enough such that $\frac{p}{N} < \epsilon$. Then since $\sum_{i=0}^n \frac{a_i}{N} x^i$ has exactly $n-2$ real roots, by our choice of ϵ,

$$\sum_{i=0}^n \frac{a_i - m_i}{N} x^i \in \mathbf{Q}[x]$$

has exactly $n-2$ real roots. It is also irreducible since $\sum_{i=0}^n (a_i - m_i)x^i$ is irreducible.

(c) The same argument that we used in class to do the case $p = 5$ shows the statement.