MATH 81/111: RINGS AND FIELDS
HOMEWORK #6

Problem 6.1. Recall that $V = \{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq S_4$ is a normal subgroup.

(a) Show that any transitive subgroup $G \leq S_4$ is equal to one of S_4, A_4, V or is isomorphic to either D_8 (three conjugate subgroups) or $\mathbb{Z}/4\mathbb{Z}$ (three conjugate subgroups). *[Hint: see Figure 8 on page 110 of Dummit and Foote.]*

(b) Suppose that $G \leq S_4$ is a transitive subgroup. Prove that the indices in the following table are correct.

$G \cong$	$\#(G \cap V)$	$[G : V \cap G]$
S_4	4	6
A_4	4	3
V	4	1
D_8	4	2
$\mathbb{Z}/4\mathbb{Z}$	2	2

(c) Compute the Galois groups of the following polynomials:

$$f_1(X) = X^4 - X + 1, \quad f_2(X) = X^4 - X^3 + X^2 - X + 1$$
$$f_3(X) = X^4 - X^3 + 2X^2 + X + 1, \quad f_4(X) = X^4 - 2X^3 + 2X^2 + 2.$$

(d) For each of the polynomials in part (c), and for each partition λ of 4, count the proportion of primes $p \leq 10^5$ with $p \nmid D(f)$ such that the factorization of f_i modulo p is given by λ. Assuming that these proportions are rational numbers with denominator dividing $\#\operatorname{Gal}(f_i)$, give a conjecture for what they are (and how they relate to G).

Problem 6.2 (M4-1).

(a) What is the splitting field of $X^m - 1$ over $\mathbb{F}_p$?

(b) Show that there is a field homomorphism $\mathbb{F}_{p^r} \hookrightarrow \mathbb{F}_{p^s}$ if and only if $r \mid s$.

Problem 6.3. Let p be prime and define

$$a_n(p) = \#\{f \in \mathbb{F}_p[X] : \deg f = n,\ f \text{ monic irreducible}\}.$$

(a) Show that $a_2(p) = (p^2 - p)/2$ and $a_3(p) = (p^3 - p)/3$.

(b) Use the equality

$$(*) \qquad \sum_{d \mid n} d a_d(p) = p^n$$

(which you may assume) to compute $a_n(2)$ for $n = 1, \ldots, 5$.

(c) Use $(*)$ to prove that

$$\frac{p^n - 2p^{n/2}}{n} < a_n(p) \leq \frac{p^n}{n}.$$

Date: 11 February 2015; due Wednesday, 18 February 2015.

Conclude that the probability that a random monic polynomial of degree n over $\mathbb{F}_p$ is irreducible is roughly $1/n$. (This is like the "prime number theorem" for $\mathbb{F}_p[X]$.)

Problem 6.4 (M4-9). Let $f(X)$ be an irreducible polynomial in $\mathbb{Q}[X]$ with both real and nonreal roots. Show that its Galois group is nonabelian. Can the condition that f is irreducible be dropped?

Problem 6.5. Let $\alpha = \sqrt[3]{2}$ and $\omega = (-1+\sqrt{-3})/2$. Show that $\omega + c\alpha$ is a primitive element for $K = \mathbb{Q}(\alpha, \omega)$ for all $c \in \mathbb{Q}^\times$.