MATH 603: HOMEWORK #5

DUE IN SEBASTIAN MOORE'S MAILBOX BY FRIDAY, APRIL 7, 2017

1. The primitive element theorem

1. Suppose R is a U.F.D. with fraction field F. Let π be an irreducible in R. Let $v_\pi : F^* \to \mathbb{Z}$ be the unique discrete valuation such that for all $\alpha \in R - \{0\}$, $v_\pi(\alpha)$ is the power of π appearing in the factorization of α. Show that if $m > 0$ is an integer and $\beta = \sum_{i=0}^{m-1} b_i^m \pi^i$ for some $b_i \in F$, then $v_\pi(\beta) = 0$ if and only if $v_\pi(b_i) \geq 0$ for each i such that $b_i \neq 0$, and $b_0 \neq 0$ satisfies $v_\pi(b_0) = 0$.

2. Suppose F is an arbitrary field of characteristic p and that $F(x, y)$ is the rational function field over F in two commuting indeterminates x and y. Exhibit explicitly an infinite number of distinct fields L such that $F(x^p, y^p) \subset L \subset F(x, y)$. (Problem # 1 is relevant to one approach to this.)

2. Finite fields.

3. Let $\mathbb{F}_q$ be a finite field of order q and suppose $1 \leq n \in \mathbb{Z}$. Show that the polynomial $x^{q^n} - x \in \mathbb{F}_q[x]$ is the product of all of the irreducible monic polynomials $f(x) \in \mathbb{F}_q[x]$ of degree d as d runs over the divisors of n. For each such d let $z(d)$ be the number of such $f(x)$. Deduce that

$$q^n = \sum_{d|n} z(d)d.$$

The Mobius function $\mu(m)$ of a positive integer m if 1 if $m = 1$, and if $m > 1$ has prime factorization $p_1^{a_1} \cdots p_s^{a_s}$ then

$$\mu(m) = \prod_i \mu(p_i^{a_i}) \quad \text{with} \quad \mu(p_i) = -1 \quad \text{and} \quad \mu(p_i^{a_i}) = 0 \quad \text{if} \quad a_i > 1.$$

Show that

$$\sum_{d|m} \mu(d) = 0 \quad \text{if} \quad m > 1.$$

Deduce that

$$z(n)n = \sum_{m|n} \mu(n/m) q^m.$$

(This is a special case of Mobius inversion.)

4. Show that if $\mathbb{F}_q$ is a finite field with q elements, then every element of $\mathbb{F}_q$ is a sum of two squares. For which q is every element of $\mathbb{F}_q$ a square?

5. Let A be a finitely generated commutative algebra over a finite field $\mathbb{F}_q$ of order q. Let $X = \mathrm{Spec}(A)$. Let $S(X)$ be the set of all maximal ideals P of A. In this exercise we will take for granted that $\#A/P$ is finite and a power of q for each $P \in S(X)$. The zeta function of X is defined to be the formal power series in $q^{-s} = t$ given by

$$\zeta(X, s) = \prod_P \frac{1}{1 - (\#A/P)^{-s}}$$

Show that when $A = \mathbb{F}_q[x]$ (so that X is just the affine line over $\mathbb{F}_q$), one has

$$\zeta(X, s) = \prod_{\pi(x)} \frac{1}{1 - t^{\deg(\pi(x))}}$$

where $\pi(x)$ runs over all of the monic irreducible polynomials in $\mathbb{F}_q[x]$. By expanding the terms on the right side, show that this function can be written as a ratio of polynomials in $\mathbb{Z}[q, t]$, where here q is treated as a variable.

Comments: Calculating $\zeta(X, s)$ for more general X as above is one of the main goals of arithmetic geometry. The zeta function $\zeta(X, s)$ can be viewed as the zeta function of X over $\mathbb{F}_q$. An active area of research now has to do with what are called "varieties over the field $\mathbb{F}_1$ with one element." While $\mathbb{F}_1$ itself does not exist in a literal sense, there are a number of precise definitions of what it means for a variety to be defined over $\mathbb{F}_1$. See, for example, the paper "A blueprinted view on $\mathbb{F}_1$-geometry" by Oliver Lorscheid. One consequence is that when X does meet the conditions required to be considered as a variety over $\mathbb{F}_1$, it will have the zeta function

$$\zeta(X_{\mathbb{F}_1}, s) = \lim_{q \to 1} (q-1)^{-N(1)} \zeta(X, s)^{-1}$$

when $N(1)$ is the order of the pole at $q = 1$ of $\zeta(X, s)$ when $\zeta(X, s)$ is written as a rational function in q^{-s}. Here $\zeta(X, s)$ on the right is a ratio of polynomials in q and q^{-s}, and we view q and s as real variables when taking the limit. The constant $N(1)$ is to be interpreted as the number of points of X over $\mathbb{F}_1$. Try showing $\zeta(X_{\mathbb{F}_1}, s) = s - 1$ when $X = \mathbb{A}^1 = \mathrm{Spec}(\mathbb{F}_q[x])$ as above.

3. Galois Theory.

6. Problem 8 of section 14.1 of Dummit and Foote.
7. Problem 3 of section 14.2 of Dummit and Foote.
8. Problem 16 of section 14.2 of Dummit and Foote.
9. Suppose $f(x) \in \mathbf{Q}[x]$ is an irreducible fourth-degree polynomial and that the Galois group of $f(x)$ is the alternating group A_4. Show that the field $\mathbf{Q}(\alpha)$ obtained by adjoining a root α of $f(x)$ to $\mathbf{Q}$ is a quartic extension which has no subfield L which is quadratic over $\mathbf{Q}$. Conclude that one cannot construct the point $(1, \alpha)$ in $\mathbf{R}^2$ by ruler and compass. Use the theory in Dummit and Foote's section 14.6 (or some other method) to construct an $f(x)$ with the above properties.