18.782 Introduction to Arithmetic Geometry **Fall 2013**

Problem Set #6 **Due: 10/29/2013**

These problems are related to the material covered in Lectures 12-13. I have made every effort to proof-read them, but some errors may remain. The first person to spot each error will receive 1-5 points of extra credit.

The problem set is due by the start of class on 10/29/2013 and should be submitted electronically as a pdf-file e-mailed to drew@math.mit.edu. You can use the latex source for this problem set as a template for writing up your solutions; be sure to include your name in your solutions and to identify collaborators and any sources not listed in the syllabus.

Problem 1. The absolute Galois group of $\mathbb{F}_q$ (50 points)

Let $\mathbb{F}_q$ be the finite field $\mathbb{Z}/q\mathbb{Z}$ for some fixed prime[1] q, let $\overline{\mathbb{F}}_q$ be a fixed algebraic closure of $\mathbb{F}_q$, and for every positive integer n let

$$\mathbb{F}_{q^n} = \{x \in \overline{\mathbb{F}}_q : x^{q^n} = x\}.$$

Recall from Lecture 3 that $\mathbb{F}_{q^n}$ is a finite field with q^n elements, and the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of order n, generated by the Frobenius automorphism $x \mapsto x^q$.

In several of the questions below you will be asked to compute various cardinal numbers. Recall that a cardinal number is an equivalence class of sets that can be put in bijection, and we write $\#A \le \#B$ whenever there is an injective map from A to B. Your answer should be either (1) a nonnegative integer, (2) $\#\mathbb{Z}$, (3) $\#\mathbb{R}$, or (4) $> \#\mathbb{R}$. You are welcome to assume the continuum hypothesis, which says that $\#S > \#\mathbb{Z} \implies \#S \ge \#\mathbb{R}$.[2]

(a) Prove that $\overline{\mathbb{F}}_q = \bigcup_{n\ge 1} \mathbb{F}_{q^n}$.

(b) Compute the cardinals $\#\overline{\mathbb{F}}_q$ and $[\overline{\mathbb{F}}_q : \mathbb{F}_q]$.

In order to compute the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, we need to generalize our notion of an inverse limit.

Definition. A *directed poset* is a nonempty set I with an *order relation* $\leqslant$ that satisfies

1. $i \leqslant i$ (reflexive)
2. $i \leqslant j$ and $j \leqslant i \implies i = j$ (anti-symmetric)
3. $i \leqslant j$ and $j \leqslant k \implies i \leqslant k$ (transitive)
4. For all $i, j \in I$ there exists k such that $i \leqslant k$ and $j \leqslant k$ (upper bound)

Definition. An *inverse system of groups* is a collection of groups $(G_i)_{i\in I}$ indexed by a directed poset I and homomorphisms $G_j \to G_i$ for each $i \leqslant j$, such that $G_i \to G_i$ is the identity map, and for all $i \leqslant j \leqslant k$ the composition $G_k \to G_j \to G_i$ is $G_k \to G_i$. The *inverse limit* $G = \varprojlim_{i\in I} G_i$ is the group whose elements are all collections $(g_i)_{i\in I}$ with $g_i \in G_i$, subject to the constraint that for all $i \le j$ the component g_i is the image of g_j under the homomorphism $G_j \to G_i$. The group operation on G is defined component-wise (so G is a subgroup of the direct product $\prod_{i\in I} G_i$).

[1] Nothing in this problem depends on q being prime, we make this assumption only for the sake of making things more concrete. The key point is that we are singling out a particular choice of $\mathbb{F}_q$ and every $\mathbb{F}_{q^n}$.

[2] You are also welcome to use the cardinal notations $\aleph_n$ and $\beth_n$ if these are familiar to you.

If we take our directed poset to be the positive integers with the usual ordering, the definition above agrees with our earlier definition of an inverse system (of groups). But now we want our directed poset to be the positive integers with the divisibility ordering, that is, $m \leqslant n$ if and only if $m|n$. This is motivated by the fact that $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m|n$.

So let $\mathbb{N}_{\text{div}}$ denote the set of positive integers ordered by divisibility, and consider the inverse system of groups

$$\big(\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\big)_{n\in\mathbb{N}_{\text{div}}},$$

where for $m|n$ the map $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the restriction map; that is, the image of an automorphism $\sigma \in \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ in $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is obtained by simply restricting the domain of σ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$.

(c) Prove that

$$\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}_{\text{div}}} \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim_{n\in\mathbb{N}_{\text{div}}} \mathbb{Z}/n\mathbb{Z}. \tag{1}$$

Conclude that $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is abelian (so all of its subgroups are normal).

(d) The group on the RHS of (1) is denoted $\hat{\mathbb{Z}}$ (it also has a ring structure, but here we view it as an additive group). Prove that

$$\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p,$$

as additive abelian groups.

(e) Compute $\#\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Conclude that $\#\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \neq [\overline{\mathbb{F}}_q : \mathbb{F}_q]$.

(f) Compare the number of subgroups of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ to the number of intermediate fields F with $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}}_q$ (as cardinals). Conclude that the Galois correspondence does not hold for $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, and that, in particular, two distinct subgroups of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ may have the same fixed field.

(g) For any subgroup $G \subseteq \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, let $\overline{G}$ denote the group generated by the union of all subgroups of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ that have the same fixed field as G, and call G *closed* if $G = \overline{G}$.[3] Show that there is a one-to-one inclusion-reversing correspondence between closed subgroups $G \subseteq \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and intermediate fields $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}}_q$ such that

(i) $G = \text{Gal}(\overline{\mathbb{F}}_q/F)$;

(ii) $F = \overline{\mathbb{F}}_q^{\,G}$.

Problem 2. Homogeneous ideals and projective algebraic sets (50 points)

Let k be a perfect field and fix an algebraic closure $\overline{k}$. Fix a positive integer n, let R be the polynomial ring $\overline{k}[x_0, \ldots, x_n]$, and let R^h be the set of all homogeneous polynomials in R. Recall from lecture that (1) a homogenous ideal in R is an ideal generated by elements of R^h, (2) for any subset $S \subset R$ the algebraic set Z_S is the zero locus in $\mathbb{P}^n$ of $S \cap R^h$, and (3) for any subset $Z \subset \mathbb{P}^n$ the ideal $I(Z)$ is the homogeneous ideal generated by the polynomials in R^h that vanish at every point in Z.

[3] One can define a topology on $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ for which $\overline{G}$ is precisely the closure of G; this is known as the Krull topology.

(a) Prove the "homogeneous *Nullstellensatz*," which says that if $I \subseteq R$ is a homogeneous ideal and $f \in R^h$ is a nonconstant polynomial that vanishes at every point in Z_I, then $f^r \in I$ for some $r > 0$ (hint: re-interpret the problem in $\mathbb{A}^{n+1}$ and use the usual *Nullstellensatz*).

(b) Let R_+ denote the set of all polynomials in R with no constant term. Prove that for any homogeneous ideal $I \subseteq R$ the following are equivalent:

(i) Z_I is the empty set;

(ii) Either $\sqrt{I} = R$ or $\sqrt{I} = R_+$.

(iii) I contains every polynomial in R^h of degree d, for some $d > 0$.

(c) Prove the following:

(i) If $S \subseteq T$ are subsets of R^h then $Z_T \subseteq Z_S$.

(ii) If $Y \subseteq Z$ are subsets of $\mathbb{P}^n$ then $I(Z) \subseteq I(Y)$.

(iii) For any two subsets Y, Z in $\mathbb{P}^n$ we have $I(Y \cup Z) = I(Y) \cap I(Z)$.

(iv) For any algebraic set $Z \subseteq \mathbb{P}^n$ we have $Z_{I(Z)} = Z$.

(v) For any homogeneous radical ideal I for which $Z_I \neq \emptyset$ we have $I(Z_I) = I$.

(d) Conclude from (a), (b), and (c) that there is a one-to-one inclusion-reversing correspondence between algebraic sets in $\mathbb{P}^n$ and homogeneous radical ideals in R that are not equal to R_+, given by the maps $Z \to I(Z)$ and $I \to Z_I$.[4]

(e) Prove that an algebraic set $Z \in \mathbb{P}^n$ is irreducible if and only if $I(Z)$ is a prime ideal.

Problem 3. Survey

Complete the following survey by rating each problem on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast"), and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
10/17	Field extensions, algebraic sets				
10/22	Affine and projective varieties				

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they might be improved.

[4] The ideal R_+ that does not appear in this correspondence is called the *irrelevant* ideal.