Math 55a, Fall 2004

---

9 th Assignment, due November 23

The point of the two problems of this assignment is to get started with Galois theory. Along the way, you will also prove the impossibility of "doubling the cube" and "squaring the circle" by ruler and compass.

1. Let L be a field, and $K \subset L$ a subfield. One refers to this situation by calling L an *extension field* of K.

a) Show that the additive structure of L and multiplication of elements of L by elements of K turn L into a vector space over K.

More terminology: one says that L is a *finite extension* of K if L, considered as a vector space over K as in part a), is finite dimensional. The *degree* of L over K, denoted by $[L : K]$, is the dimension of this vector space. An element $a \in L$ is said to be *algebraic* over K if it is the root of a non-constant polynomial with coefficients in K. Prove the following statements:

b) Suppose L is a finite extension of the the field K, and K a finite extension of the field k. Then L is a finite extension of k, and $[L : k] = [L : K][K : k]$.

c) Every element of a finite extension L of a field K is algebraic over K.

2. For any subset $S \subset \mathbb{R}^2$, $\mathbb{Q}(S)$ shall denote the smallest subfield of $\mathbb{R}$ containing both the x- and y-coordinate of every point in S. Prove the following statements:

a) Let ℓ be a straight line passing through two distinct points in some subset $S \subset \mathbb{R}^2$. The coordinates of every point $(x, y) \in \ell$ satisfy a linear equation with coefficients in $\mathbb{Q}(S)$.

a) Let p be the point of intersection of two non-parallel lines ℓ_1, $\ell_2 \subset \mathbb{R}^2$, such that both ℓ_1 and ℓ_2 pass through pairs of unequal points in S. Then the coordinates of p lie in $\mathbb{Q}(S)$.

c) Let C_1, $C_2 \subset \mathbb{R}^2$ be two distinct circles, each centered at points of S and each passing through a point in S. Then $C_1 \cap C_2$ lies on a straight line ℓ, whose equation has coefficients in $\mathbb{Q}(S)$.

d) Suppose ℓ is a straight line passing through two distinct points in S, and C a circle centered at a point in S and passing through a point in S. If p is a point of intersection of ℓ and C, the field $\mathbb{Q}(S \cup \{p\})$ either coincides with $\mathbb{Q}(S)$, or has degree two over $\mathbb{Q}(S)$.

e) If $p \in \mathbb{R}^2$ can be constructed by ruler and compass from the two points $(0, 0)$, $(1, 0)$, the degree of the field $\mathbb{Q}(\{p\})$ over $\mathbb{Q}$ is a power of 2.