Math 55a, Fall 2004

Ninth Assignment, Solutions
Adapted from Andrew Cotton and George Lee

Problem 1.

(a) Since L is a field it is an additive group; since $L \cdot L \subset L$ we have $K \cdot L \subset L$; and associativity and distributivity $[(k_1 k_2)\ell = k_1(k_2\ell)$, $(k_1 + k_2)\ell = k_1\ell + k_2\ell$, $k(\ell_1 + \ell_2) = k\ell_1 + k\ell_2]$ follow from associativity and distributivity in the field L. Also, $1 \in K$ is also the identity in L, so we have $1 \cdot \ell = \ell$ for any $\ell \in L$. Therefore, L is a vector space over K.

(b) Clearly k is a subfield of L, so L is a vector space over k. Now we need to prove L is a *finite* extension of k.

Suppose that $\{u_1, u_2, \ldots, u_m\} \subset L$ is an m-element basis of L over K, and that $\{v_1, v_2, \ldots, v_n\} \subset K$ is an n-element basis of K over k. We claim that

$$B = \{v_j u_i \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

is an mn-element basis of L over k.

Any element $\ell \in L$ can be written as a linear combination $\sum_{i=1}^{m} a_i u_i$ for $a_1, a_2, \ldots, a_m \in K$. And each a_i can be written as a linear combination $\sum_{j=1}^{n} b_j^{(i)} v_j$ for $b_1^{(i)}, b_2^{(i)}, \ldots, b_n^{(i)} \in k$. Therefore we can write ℓ as a linear combination of elements $v_j u_i \in B$ with coefficients in k:

$$\ell = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} b_j^{(i)} v_j \right) u_i = \sum_{i=1}^{m} \sum_{j=1}^{n} b_j^{(i)} \cdot v_j u_i.$$

Next, suppose that

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{i,j} \cdot v_j u_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} b_{i,j} v_j \right) \cdot u_i$$

for $b_{i,j} \in k$. Since the u_i are linearly independent over K, for each i the coefficient

$$\sum_{j=1}^{n} b_{i,j} v_j$$

in K must be 0. But then because the v_j are linearly independent over k, each coefficient $b_{i,j} \in k$ must be zero as well. So, the elements of B are linearly independent.

Hence, we've shown that B contains mn linearly independent elements; and that every element in L can be written as a linear combination over k of elements of B. Thus, B is a basis of L over k; L is a finite extension of k with degree mn; and $[L : k] = [L : K][K : k]$.

(c) Suppose L is a finite extension of K with degree n. For any element $\ell \in L$, consider the elements $1, \ell, \ell^2, \ldots, \ell^n$. If they are linearly independent over K, then they are distinct and $\{1, \ell, \ell^2, \ldots, \ell^n\}$ can be extended to a basis of L over K with at least $n+1$ elements—a contradiction. So, there exist $k_0, k_1, \ldots, k_n \in K$ such that

$$\sum_{i=0}^{n} k_i \ell^i = 0,$$

as desired.

Problem 2.

Given a subset $S \subset \mathbb{R}^2$ call a line "S-piffy" if it every point (x, y) satisfies some single linear equation in x and y with coefficients in $\mathbb{Q}(S)$. Call a circle S-piffy if it is centered at a point in $\mathbb{Q}(S) \times \mathbb{Q}(S)$ and passes through some point in $\mathbb{Q}(S) \times \mathbb{Q}(S)$.

(a) Given distinct points (x_1, y_1) and (x_2, y_2), the line passing through them satisfies the equation

$$(y - y_1)(x_2 - x_1) = (x - x_1)(y_2 - y_1)$$

or

$$(x_2 - x_1)y + (y_1 - y_2)x + x_1y_2 - x_2y_1 = 0.$$

A point (x, y) lies on the line if and only if it satisfies this equation. Note that the coefficients of x and y are not both zero. And if $x_1, y_1, x_2, y_2 \in \mathbb{Q}(S)$, so are the coefficients of this equation (since the field is closed under addition, subtraction, and multiplication).

(b) Since p lies on ℓ_1, from (a) the coordinates (x_p, y_p) of p satisfy some nontrivial linear equation with coefficients in $\mathbb{Q}(S)$; similarly, any because p lies on ℓ_2 it satisfies some other linear equation with coefficients in $\mathbb{Q}(S)$. So (x_p, y_p) satisfies some equations

$$\begin{aligned} s_1x_p + s_2y_p &= s_3 \\ t_1x_p + t_2y_p &= t_3 \end{aligned}$$

for $(s_i, t_i) \in \mathbb{Q}(S) \times \mathbb{Q}(S) - \{(0,0)\}$. Since ℓ_1 and ℓ_2 are not parallel, $s_1 t_2 \neq s_2 t_1$. So solving these equations gives

$$x_p = \frac{s_3 t_2 - s_2 t_3}{s_1 t_2 - s_2 t_1} \quad \text{and} \quad y_p = \frac{s_1 t_3 - s_3 t_1}{s_1 t_2 - s_2 t_1}.$$

But again, since $\mathbb{Q}(S)$ is closed under subtraction, multiplication, and division (by nonzero numbers), both x_p and y_p are in $\mathbb{Q}(S)$.

(c) Let $p = (x_p, y_p)$ be a point of intersection. Suppose the first circle is centered at (x_1, y_1) and passes through (s_1, t_1), where $x_1, y_1, s_1, t_1 \in \mathbb{Q}(S)$. If its radius is r_1, then $r_1^2 = (x_1 - s_1)^2 + (y_1 - t_1)^2$ is also in $\mathbb{Q}(S)$. Writing $R_1 = r_1^2 \in \mathbb{Q}(S)$, we know that (x_p, y_p) satisfies the equation

$$(x_p - x_1)^2 + (y_p - y_1)^2 = R_1.$$

Similarly, it satisfies an analagous equation

$$(x_p - x_2)^2 + (y_p - y_2)^2 = R_2$$

for $x_2, y_2, R_2 \in \mathbb{Q}(S)$. Subtracting these equations yields

$$2(x_2 - x_1)x_p + 2(y_2 - y_1)y_p + x_1^2 + y_1^2 + R_1 - x_2^2 - y_2^2 - R_2 = 0,$$

which is indeed a linear equation with coefficients in $\mathbb{Q}(S)$ (since, as before, $\mathbb{Q}(S)$ is closed under subtraction, multiplication, and addition — notice, for example, that $2(x_2 - x_1) = (x_2 - x_1) + (x_2 - x_1)$ is in $\mathbb{Q}(S)$). And since $(x_1, y_1) \neq (x_2, y_2)$, the coefficients of x_p and y_p are not both zero so this equation indeed describes a line.

(d) We prove that if p is an intersection point of a S-piffy line ℓ and a S-piffy circle c, then $[\mathbb{Q}(S \cup \{p\}) : \mathbb{Q}(S)] = 1$ or 2.

Suppose the equation of ℓ is

$$s_1 x + s_2 y = s_3$$

and that the equation of C is

$$(x - x_1)^2 + (y - y_1)^2 = R,$$

where $s_1, s_2, s_3, x_1, y_1, R \in \mathbb{Q}(S)$ as before. Given a point $p = (x_p, y_p)$ on both ℓ and C, we know it satisfies both these equations. Suppose without loss of generality that $s_1 \neq 0$ (both s_1 and s_2 cannot equal 0 since then we would not have an equation for a line). Plugging in $x_p = \frac{s_3 - s_2 y_p}{s_1}$ into the equation for C, we have

$$\left(\frac{s_3 - s_2 y_p}{s_1} - x_1 \right)^2 + (y_p - y_1)^2 = R,$$

which expands to a quadratic in y_p with coefficients in $\mathbb{Q}(S)$ and nonzero leading coefficient. Dividing by the leading coefficient gives an equation $y_p^2 + ay_p + b = 0$ with coefficients $a, b \in \mathbb{Q}(S)$. Either $X^2 + aX + b$ or one of its linear factors is irreducible in $\mathbb{Q}(S)[X]$ and has root y_p. Then as argued in the next problem assignment, $\mathbb{Q}(S)(y_p)$ has degree 1 or 2 over $\mathbb{Q}(S)$.

(This can also be proved directly by looking at the set $F = \{m+ny_p \mid m, n \in \mathbb{Q}(S)\}$. It is easy to verify that F is closed under addition, multiplication, and the additive inverse. To check that $m + ny_p$ has multiplicative inverse in F, we consider two cases. If $n = 0$ or $y_p = 0$, the result follows easily. Otherwise, we can set $f = -a - \frac{m}{n}$ to find that $(m + ny_p)(y_p + f)$ equals a nonzero constant $bn + mf$. Therefore $\frac{1}{bn+mf}(y_p + f) \in F$ is a multiplicative inverse of y_p. It follows that $F$is a field containing $\mathbb{Q}(S)$ and y_p. Thus $\mathbb{Q}(S)(y_p) \subset F$, and because $[F : \mathbb{Q}(S)]$ equals 1 or 2, $\mathbb{Q}(S)(y_p)$ equals 1 or 2 as well.)

Now,

$$x_p = \frac{s_3 - s_2 y_p}{s_1}.$$

is in $\mathbb{Q}(S)(y_p)$. Hence, $\mathbb{Q}(S \cup \{p\}) = \mathbb{Q}(S)(y_p)$ has degree 1 or 2 over $\mathbb{Q}(S)$, as desired.

(e) This proof ignores constructions that involve drawing "arbitrary" lines and circles, although if "arbitrary" is defined properly the result still holds for such constructions.

Given a set of points S, let an *S-constructible line* be a line passing through two points in S. Let an *S-constructible circle* be a circle centered at a point in S, and whose radius equals AB for distinct points $A, B \in S$.

We call a point p *constructible from* $(0, 0)$ *and* $(0, 1)$ if it lies in a sequence $p_1, p_2, \ldots, p_n$ of points with the following properties: $p_1 = (0, 0)$, $p_2 = (0, 1)$, and $p_n = p$; and writing $A_k = \{p_1, p_2, \ldots, p_k\}$ for $1 \le k \le n$, each point p_k is of one of the following types:

- the intersection of two distinct A_{k-1}-constructible lines;
- the intersection of two distinct A_{k-1}-constructible circles;
- the intersection of an A_{k-1}-constructible line and an A_{k-1}-constructible circle.

Now suppose we have any such sequence $p_1, p_2, \ldots, p_n$. We prove by induction on k that for $2 \le k \le n$, the degree of $\mathbb{Q}(A_k)$ over $\mathbb{Q}$ is a power of 2. For $k = 2$, $\mathbb{Q}(\{(0, 0), (0, 1)\}) = \mathbb{Q}$ is a degree-one extension.

Now assume that $[\mathbb{Q}(A_{k-1}) : \mathbb{Q}] = 2^m$, and write $S = A_{k-1}$ and $Q = \mathbb{Q}(A_k) = \mathbb{Q}(A_{k-1} \cup \{p_k\})$. Any S-constructible circle is centered at some point $(x_1, y_1) \in \mathbb{Q}(S) \times \mathbb{Q}(S)$ and has radius BC for some (x_2, y_2), $(x_3, y_3) \in \mathbb{Q}(S) \times \mathbb{Q}(S)$. Then this circle ω passes through $(x_1 + x_2 - x_3, y_1 + y_2 - y_3 \in \mathbb{Q}(S) \times \mathbb{Q}(S)$, so it is an S-piffy circle.

Suppose p_k is the intersection of two S-constructible lines; then they each pass through two points in S, so from (b) we know that $p \in \mathbb{Q}(S) \times \mathbb{Q}(S)$ so that $Q = \mathbb{Q}(S)$.

If p_k is the intersection of two S-constructible circles, then these circles are S-piffy; so from (c) and our observation at the beginning of (d), $[Q : \mathbb{Q}(S)] = 1$ or 2.

And if p_k is the intersection of an S-constructible line and an S-constructible circle, then from (d) we know $[Q : \mathbb{Q}(S)] = 1$ or 2 as well.

Thus $[Q : \mathbb{Q}] = [Q : \mathbb{Q}(S)][\mathbb{Q}(S) : \mathbb{Q}] = [Q : \mathbb{Q}(S)]2^m$ equals 2^m or 2^{m+1}, still a power of two — as claimed.

Now back to the original problem. Given a point p, suppose it equals p_n in a sequence $p_1, p_2, \ldots, p_n$ as described above. Writing $S = \{p_1, p_2, \ldots, p_n\}$, we know that $[\mathbb{Q}(S) : \mathbb{Q}] = 2^m$ for some integer $m \geq 0$. Because $\mathbb{Q}(S)$ is a (finite) field extension of $\mathbb{Q}(\{p\})$, which in turn is a (finite) field extension of $\mathbb{Q}$, $[\mathbb{Q}(\{p\}) : \mathbb{Q}] = [\mathbb{Q}(S) : \mathbb{Q}]/[\mathbb{Q}(S) : \mathbb{Q}(\{p\})]$ divides $[\mathbb{Q}(S) : \mathbb{Q}] = 2^m$. Thus $[\mathbb{Q}(\{p\}) : \mathbb{Q}]$ is itself a power of two, as desired.