D-MATH Algebra II FS18
Prof. Marc Burger

Solution 23

Galois extensions. Constructions with ruler and compass.

1. Let E/k be a finite field extension, write $G := \mathrm{Gal}(E/k)$ and consider an element $\alpha \in E$. Consider the polynomial

$$q := \prod_{\sigma \in G/\mathrm{Stab}_G(\alpha)} (X - \sigma(\alpha)) \in E[X].$$

Prove that $q \in E^G[X]$.

Solution: By the orbit stabilizer theorem, the action of $\sigma \in G/\mathrm{Stab}_G(\alpha)$ on α is well-defined and the $\sigma(\alpha)$'s are all distinct. Each $\tau \in G$ extends to a unique automorphism $\tilde{\tau}$ of $E[X]$ sending $X \mapsto X$. Then,

$$\tilde{\tau}(q) = \tilde{\tau}\left(\prod_{\sigma \in G/\mathrm{Stab}_G(\alpha)} (X - \sigma(\alpha))\right) = \prod_{\sigma \in G/\mathrm{Stab}_G(\alpha)} (X - \tau(\sigma(\alpha))) = q,$$

because τ permutes the $\sigma(\alpha)$'s, that is, the elements of the orbit of α. Hence τ fixes the coefficients of q. By arbitrarity of τ, we conclude that $q \in E^G[X]$.

2. Let E/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/k)$ of degree $n = [E : k]$. Define the *trace* $T : E \longrightarrow E$ by

$$T(x) = \sum_{\sigma \in G} \sigma(x).$$

One can prove that this map coincides with the trace defined in Assignment 12, Exercise 7.

(a) Prove that $\mathrm{im}(T) \subseteq k$ and that T is k-linear.

(b) Show that T is not identically zero and deduce that $\dim(\ker(T)) = n - 1$. [*Hint:* Independence of characters].

(c) Now suppose that $\mathrm{Gal}(E/k)$ is cyclic and generated by an automorphism σ. Consider the linear map $\tau = \sigma - \mathrm{id}_E$. Prove that

$$\ker(T) = \mathrm{im}(\tau) = \{\sigma(u) - u : u \in E\}.$$

Solution:

(a) Let $\tau \in G$. For each $x \in E$,

$$\tau(T(x)) = \tau\left(\sum_{\sigma \in G} \sigma(x)\right) = \sum_{\sigma \in G} \tau\sigma(x) = T(x),$$

because $\sigma \mapsto \tau\sigma$ is a bijection $G \longrightarrow G$. By arbitrarity of τ and $x \in E$, the image of T is in E^G, which coincides with k because E/k is Galois.

In order to prove that T is k-linear, let $x, y \in E$ and $a \in k$. Then

$$T(x + ay) = \sum_{\sigma \in G} \sigma(x + ay) = \sum_{\sigma \in G} (\sigma(x) + a\sigma(y)) = T(x) + aT(y).$$

(b) The map $T \in \mathrm{Hom}(E^\times, E)$ is a non-trivial linear combination (with coefficients all equal to 1) of the finitely many characters $\sigma \in \mathrm{Gal}(E/k) \subset \mathrm{Hom}(E^\times, E^\times)$. Hence $T \neq 0$. Then the image of T is a non-zero k-linear subspace of k, which means that $\mathrm{im}(T) = k$ so that $\dim(\mathrm{im}(T)) = 1$. Then by the rank-nullity theorem we conclude that

$$\dim(\ker(T)) = n - \dim(\mathrm{im}(T)) = n - 1.$$

(c) We notice that $\ker(\tau) = \{u \in E : \sigma(u) = u\} = E^G = k$, because σ generates G so that the elements of E fixed by σ are fixed by the whole G. Again by the rank-nullity theorem, we obtain

$$\dim(\mathrm{im}(\tau)) = n - \dim(\ker(\tau)) = n - 1.$$

As $\ker(T)$ and $\mathrm{im}(\tau)$ have the same dimension, it suffices to show that one is contained in the other. We show that $\mathrm{im}(\tau) \subset \ker(T)$: for all $x \in E$,

$$T(\sigma(x) - x) = \sum_{\sigma' \in G} \sigma'(\sigma(x) - x) = \sum_{\sigma' \in G} \sigma'\sigma(x) - \sum_{\sigma' \in G} \sigma'(x) = T(x) - T(x) = 0.$$

3. Define the set $S \subset \mathbb{R}^2$ of *constructible points* as the smallest subset S of the Euclidean plane containing O, $(1, 0)$ and such that:

- if $A, B, C, D \in S$ and the line through A and B is not parallel to the one through C and D, then the intersection point is in S;
- if $A, B, C, D, E \in S$, then all points of intersection between the line through A and B and the circle centered at C with radius equal to $d(D, E)$ are in S.
- if $A, B, C, D, E, F \in S$, then all points of intersection between the circle centered at C with radius equal to $d(D, E)$ and the circle centered at F with radius equal to $d(A, B)$ are in S.

(a) Suppose that the points A, B, C, D, E, F have coordinates in a common field $K \subset \mathbb{R}$. Explain why if a point X can be constructed by performing one of the two steps above, then its coordinates belong to a field extension K'/K such that $[K' : K] \leqslant 2$.

We say that a real number $r \in \mathbb{R}$ is *constructible* if the point $(r, 0) \in \mathbb{R}^2$ is constructible.

(b) Prove that the point $(a, b) \in \mathbb{R}^2$ is constructible if and only if a and b are constructible.

(c) Prove that a real number $r \in \mathbb{R}$ is constructible if and only if there are field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

such that $[K_i : K_{i-1}] \leqslant 2$ and $r \in K_n$.

(d) Prove that the real numbers π, $\sqrt[3]{2}$ and $\cos(20°)$ are not constructible. Explain what this means in terms of classical ruler-and-compass construction problems. [*Hint:* What is the degree of $\mathbb{Q}(z)/\mathbb{Q}$ if z is a constructible number? You may need the trigonometric identity $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$].

Solution:

(a) We use some basic high-school geometry. If the point $X = (x_1, x_2)$ lies on a line through points with coordinates in K, then the coordinates satisfy a linear equation

$$(I) : ax_1 + bx_2 + c = 0$$

for some $a, b, c \in K$. More precisely, if X lies on the line passing through (p_1, p_2) and (q_1, q_2), then the equation $(p_2 - q_2)(x_1 - p_1) = (p_1 - q_1)(x_2 - p_2)$ holds.

If the point X lies on a circle with center $C = (c_1, c_2)$ and radius r such that $r^2 \in k$ (which is the case if r is the distance between two points with coordinates in K), such that C has coordinates in k, then the coordinates of X satisfy a quadratic equation of the form

$$(II) : x_1^2 + x_2^2 + ux_1 + vx_2 + w = 0$$

for some $u, v, w \in K$. In the given situation, the precise equation is $(x_1 - c_1)^2 + (x_2 - x_2)^2 = r^2$.

The points obtained in one of the three manners described in the exercise are solutions of a system of two equations, each of type (I) or (II). The case of two equations of type (II) falls into the one of one equation of type (I) and one of type (II), because subtracting two equations of the type (II) one gets an equation of type (I). Hence we can ignore the intersection of two circles.

In the case in which we intersect two lines, the coordinates of X satisfy a system of two linear equations, which by basic linear algebra has a unique solution in $\mathbb{R}^2$ if and only if the relevant matrix in $\mathbb{R}^{2,2}$ has non-zero determinant. Since all the coefficients lie in K, then the solution exists in K as well. Hence $K' = K$ does the job in this case.

In the case in which we intersect one line with a circle we get equations

$$\begin{cases} ax_1 + bx_2 = c \\ x_1^2 + x_2^2 + ux_1 + vx_2 + w = 0 \end{cases}$$

If $a = 0$, then $b \neq 0$ (as the first equation represents a line) so that $x_2 = c/b \in K$; then, substituting x_2 in the second equation, we see that x_1 must be a root of a degree-2 polynomial with coefficients in K, so that this polynomial is divisible by $\operatorname{irr}(x_1, K)$, so that $K' = K(x_1)$ has degree 2 over K and does the job. Else, if $a \neq 0$, we write $x_1 = (c - bx_2)/a \in K(x_2)$, substituting this in the second equation we see that x_2 satisfies a degree-2 equation with coefficients in K, so that $K' = K(x_2)$ does the job.

(b) The reader is encouraged to make a drawing of the constructions.

We can draw the horizontal axis as the line through O and $(1, 0)$. Intersecting it with the circle centered in O of radius 1, we realise that $(-1, 0) \in S$. Intersecting the two circles centered at $(-1, 0)$ and $(1, 0)$ of radius 2, we see that $(0, \pm\sqrt{2}/2) \in S$, so that connecting those two points we can draw the vertical axis. Hence, $(a, 0) \in S$ if and only if $(0, a) \in S$, because we can move points from an axis to the other by intersecting those axes with a circle centered at the origin of radius a.

Hence, if a and b are constructible numbers, then $(a, 0)$ and $(0, b)$ are constractible, and drawing a circle centered at $(0, b)$ with radius a and a circle centered at $(a, 0)$ of radius b, we see that $(a, b) \in S$.

Conversely, assume that $(a, b) \in S$. As we have drawn the two cartesian axes, we are left to check that the projection of a point $P \in S$ to the line passing through two points $A, B \in S$ can be constructed with rule and compass. This can be done by intersecting the line through A and B with the circle centered at P and passing through A, in order to obtain another point A', such that P belongs to the axis of the segment $\overline{AA'}$. This axis can be drawn by taking circles centered in A and A' of radius $d(A, A')$. Intersecting this axis with $\overline{AA'}$, we obtain the projection of P.

(c) First, we recall that there are methods to replicate and divide equally a segment by using ruler and compass (in order to divide a segment AB into n equal parts, consider a point C outside their line—which can be constructed by intersecting two circles centered in A and B of radius $d(A, B)$—and replicate n times the segment $\overline{AC}$ by adding points $C_1 = C, \ldots, C_n$ on its line, one after the other; connect C_n with B and draw parallel lines to BC_n passing through each C_j[1] and intersecting $\overline{AB}$ into points $B_1, \ldots, B_n = B$ with $d(B_i, B_{i+1}) = \frac{d(A,B)}{n}$) the last point with B and draw parallel, so that all rational numbers are constructible starting with O and $(1, 0)$. By part (b), this implies that all points with rational coordinates are constructible. By part (a), we know that the coordinates of a constructible point lie in an extension which is obtained by iterating quadratic extensions. Again by part (b), this implies that all constructible numbers belong to such an extension.

Conversely, recall that a quadratic extension in characteristic zero is obtained by adding a square root. In particular, a real quadratic extension is obtained by adding a square root of a positive number. This means that in order to conclude that each real number belonging to an iteration of a quadratic extension is constructible, it is enough to check that the square root of a positive constructible number is constructible. This can be done as follow: given the positive constructible number r, take the points $B = (-1, 0)$ and $A = (r, 0)$. By intersecting circles of radius $r + 1$ centered at A and B, we obtain two points laying on the axis of $\overline{AB}$. Drawing this axis and intersecting it with $\overline{AB}$, we find the middle point M of $\overline{AB}$. Then we can draw the circle centered at M with radius $d(M, A) = (r + 1)/2$ and intersect it with the vertical axis (drawn in part (b)) in order to get a unique point $C = (0, c)$ such that $c > 0$. The triangles BMC and CMA are similar. Hence, the equation $1/c = c/r$ holds, implying that $c = \sqrt{r}$.

(d) By part (c), all constructible real numbers are algebraic over $\mathbb{Q}$ and they must have order given by a power of 2. In particular, π is transcendental, so that it is not constructible. This means that it is not possible to draw a segment which is as long as a constructible circle.

The number $\sqrt[3]{2}$ is a root of the irreducible polynomial $X^3 - 2$, so that any extension containing it has order divisible by 3, which implies that $\sqrt[3]{2}$ is not constructible. This means that, given the side of a cube, it is not possible to construct the side of a cube having double volume. This problem was already considered in ancient Greece: Theon of Smyrna narrates that the inhabitants of Delos asked their oracle for a way to stop a plague epidemic and the response they obtained was that they should have replaced the altar to Apollo, which was a cube, with a new one with the same shape and double the volume.

Finally, we know that $1/2 = \cos(3 \cdot 20°) = 4\cos^3(20°) - 3\cos(20°)$, so that $20°$ is a root of the polynomial $8X^3 - 6X - 1 \in \mathbb{Q}[X]$, which is easily seen to be irreducible (e.g., by noticing that it has no rational root), so that we can conclude in the same way as for $\sqrt[3]{2}$ that it is not a constructible number. This means that the angle 60°, which is constructible, cannot be divided into three equal parts by using ruler and compass.

[1] this can be done by drawing a perpendicular line through the external point as in part (b), and then its perpendicular through the same point, in a similar way.