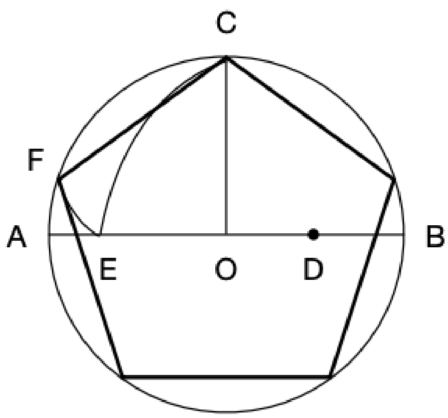
Homework 10 Solution
Kaiying Hou

1. Given a square, it is possible to construct a pentagon of the same area. Without lost



of generality, the square has side length 1. Recall that the pentagon in the above image can be constructed in the following steps:

1. We are given the segment AO. Then we construct B, C, and D.
2. Using CD, we construct point E.
3. Using CE and the circle ABC, we obtain point F. Once F is constructed, all other edges of the pentagon can be constructed by going around the circle.

If we call the length of OC the "radius" of the pentagon, AO has length equal to the radius. By the above procedure, since AO is all that is needed, to construct a pentagon of radius r, we simply need to prove that r is a constructible number.

For a pentagon of radius r, the area is

$$\frac{5}{2}r^2 \sin(\frac{2\pi}{5}).$$

Since the constructible numbers form a field and is closed under taking square roots, we only need to prove that $\sin(2\pi/5)$ is constructible. In homework 5 problem 3, we proved that $\cos(\pi/5), \sin(\pi/5)$ are both constructible. Applying the double angle formula gives us that $\sin(2\pi/5)$ is constructible.

2. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{5}), t = \sqrt{2} + \sqrt{5}$.

1. Suppose for contradiction that $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$. Then $\sqrt{5} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. Then $a^2 + 2b^2 + 2ab\sqrt{2} = 5$. Because $\sqrt{2} \notin \mathbb{Q}$, $a = 0$ or $b = 0$. Thus, $a^2 = 5$ or $b^2 = 5/2$ where $a, b \in \mathbb{Q}$, which is clearly impossible. Thus, $[K : \mathbb{Q}(\sqrt{2})] = 2$ because $x^2 = 5$ is a degree 2 polynomial with $\sqrt{5}$ as root. This implies K/L is degree 4.

2. To show $K = \mathbb{Q}(t)$, we simply need to show $\sqrt{2} \in \mathbb{Q}(t)$ since $t = \sqrt{2} + \sqrt{5}$. Calculating t^2 shows that $\sqrt{10} \in \mathbb{Q}(t)$. Thus, $\sqrt{10}t = 2\sqrt{5} + 5\sqrt{2} \in \mathbb{Q}(t)$. Taking suitable $\mathbb{Q}-$linear combination of t with $\sqrt{10}t$ isolates $\sqrt{2}$ and shows that $\sqrt{2} \in \mathbb{Q}(t)$.

3. We know that the minimal polynomial p has degree 4 due to $[K : \mathbb{Q}] = 4$. We see that t^2 and t^4 involve only $\sqrt{10}$ and no other irrational number. Thus, we can cancel out the $\sqrt{10}$ in t^2 and t^4 by choosing suitable coefficients and use the t^0 term to cancel out the remaining rational number. Calculation shows that the polynomial we obtain is $9 - 14x^2 + x^4$.

3. Let $K = \mathbb{Q}(i)$ and $p(x) = x^4 - 5$.

1. $x^4 - 5 = (x - a_1)(x - a_2)(x - a_3)(x - a_0)$ where $a_j = 5^{1/4} i^j$. We easily check that $(x - a_j), (x - a_j)(x - a_k) \notin \mathbb{Q}(i)[x]$ for all j, k by direct computation. Thus, $x^4 - 5$ cannot be factored anymore in $\mathbb{Q}(i)[x]$ and is irreducible.

2. Let $L = K(5^{1/4})$. $p(x) = (x - a_1)(x - a_2)(x - a_3)(x - a_0)$ satisfies $a_j \in L$ for all j. Furthermore, we see that L is generated by K and $\{a_j\}_j$ since $a_0 = 5^{1/4}$. Thus, L is the splittting field.

3. We have field isomorphisms $\phi_k : \mathbb{Q}[x]/p(x) \to L$ defined by $\phi_j(x) = a_j$ since $p(x)$ is irreducible and the minimal polynomial for all a_j. $\alpha = \phi_1 \circ \phi_0^{-1}$ satisfies the problem.

4. $\beta \in \mathrm{Gal}(L/K)$ must send a_0 to a_j for some j since $p(x)$ has coeffiicent in K. Moreover, β is completely determined by $\beta(a_0)$ because a_0 generates L. Thus, we see that the allowed automorphisms are exactly $\{\phi_j \circ \phi_0^{-1}\}_{j=0,1,2,3}$, no more, no less. The isomorphism with $\mathbb{Z}/4$ is given by $j \mapsto \phi_j \circ \phi_0^{-1}$.

4. Claim: Let $t = 2\cos(\pi/9)$. Then t is a root of $p(x) = x^3 - 3x - 1$.
Proof: We see that $t = e^{i\pi/9} + e^{-i\pi/9}$. Then

$$\begin{aligned} t^3 =& e^{i\pi/3} + e^{-i\pi/9} + 2e^{i\pi/9} + e^{i\pi/9} + e^{-i\pi/3} + 2e^{-i\pi/9} \\ =& 3t + e^{-i\pi/3} + e^{i\pi/3} \\ =& 3t + 2\cos(\pi/3) \\ =& 3t + 1 \end{aligned}$$

5. Claim: Let p be an odd prime. The minimal polynomial for $\cos(2\pi/p)$ in $\mathbb{Q}[x]$ has degree $(p-1)/2$.

Proof: Because $2\cos(x) = e^{ix} + e^{-ix}$, $\mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{Q}(\zeta_p)$. The following statements are manifestly equivalent.

- The minimal polynomial for $\cos(2\pi/p)$ in $\mathbb{Q}[x]$ has degree $(p-1)/2$.
- $[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = (p-1)/2$.
- $[\mathbb{Q}(\zeta_p), \mathbb{Q}(\cos(2\pi/p))] = 2$.

Note that we are using the fact that $[\mathbb{Q}(\zeta_p), \mathbb{Q}] = p - 1$ for the equivalence of the second and the third bullet point. It remains to prove $[\mathbb{Q}(\zeta_p), \mathbb{Q}(\cos(2\pi/p))] = 2$. Because $\mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{R}$, $[Q(\zeta_p), \mathbb{Q}(\cos(2\pi/p))] \geq 2$. Notice that $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\cos(2\pi/p), i\sin(2\pi/p))$ and $i\sin(2\pi/p)$ has degree 2 minimal polynomial $-x^2 + \cos^2(2\pi/p) = 1$. Thus, the extension is degree 2 as desired.

6. Claim: Given $\mathbb{Z} \cup i\mathbb{Z}$ and a straightedge, $p \in \mathbb{C}$ can be constructed iff $p \in \mathbb{Q}[i]$

Proof: Given a set $S \subset \mathbb{C}$, we use $c(S) \subset \mathbb{C}$ denote the set of points constructible using a straightedge and points in S. Note that $B := c(\mathbb{Z} \cup i\mathbb{Z})$ is closed under reflections across x, y axis because $\mathbb{Z} \cup i\mathbb{Z}$ is. We will prove that $B = \mathbb{Q}[i]$

Let L_1 be the line passing $(a, 0), (0, c)$ and L_2 be the line passing $(b, 0), (0, d)$. Then L_1, L_2 intersect at

$$p = (\frac{ab(-c + d)}{-bc + ad}, \frac{(a - b)cd}{-bc + ad}) \in c(\mathbb{Z} \cup i\mathbb{Z})$$

given that a, b, c, d are integers. Let p' be the resulting of reflecting p across the $x-$axis. Then the line passing through p', p will intersect the $x-$axis at $\frac{ab(-c+d)}{-bc+ad}$. Thus, $(\frac{ab(-c+d)}{-bc+ad}, 0)$ is constructible for arbitrary integers a, b, c, d. Plugging in $c = d - 1$, $a = 2b$ into the above expression we get that

$$(\frac{ab(-c + d)}{-bc + ad}, 0) = (\frac{2b}{d + 1}, 0)$$

is constructible for arbitrary integer b, d. Thus, $\mathbb{Q} \times \{0\}$ is constructible. By symmetry, $\{0\} \times \mathbb{Q}$ is constructible. We arrive at that $B = c(\mathbb{Q} \cup i\mathbb{Q})$. Thus, B is closed under multiplication by rational numbers (closure under rational scaling).

Using closure under rational scaling and the intersection of L_1, L_2 constructed before, we see that $(ab(-c + d), (a - b)cd) \in B$ for arbitrary rational numbers a, b, c, d as long as $-bc + ad \neq 0$. Thus, $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ can be constructed (just find any rational a, b, c, d such that $\frac{ab(-c+d)}{(a-b)cd} = \frac{p}{q}$ and apply closure under rational scaling). Thus, $\mathbb{Z} \times \mathbb{Z} \in B$. Apply closure under rational scaling once more gives us $\mathbb{Q} \times \mathbb{Q} \subset B$.

It is clear that no irrational number coordinates can be constructed using this process since $\mathbb{Q}$ is closed under field operations. Thus, $B = \mathbb{Q} \times \mathbb{Q} = \mathbb{Q}[i]$.