## D-MATH

Algebra II
FS19
Prof. Rahul Pandharipande

## Solution 21

## Constructions with straightedge and compass.

1. (a) Express cos $\frac{\pi}{12}$ in terms of real square roots.
(b) Prove that an angle $\alpha$ can be trisected if and only if $4 X^{3}-3 X-\cos \alpha$ is reducible over $\mathbb{Q}(\cos \alpha)$.

## Solution:

(a) Set $\beta:=\frac{\pi}{12}$. We have $\cos \frac{\pi}{6}=\frac{\sqrt{3}}{2}$ and thus

$$
\frac{\sqrt{3}}{2}=\cos (2 \beta)=2 \cos ^{2}(\beta)-1,
$$

so

$$
\cos (\beta)=\sqrt{\frac{\sqrt{3}+2}{4}}=\frac{\sqrt{2+\sqrt{3}}}{2} .
$$

(b) This follows immediately from the identity $\cos (\alpha)=4 \cos ^{3}(\alpha / 3)-3 \cos (\alpha / 3)$.
2. (Constructible polygons)
(a) Is the regular 9-gon constructible?
(b) Deduce that the regular 15 -gon is constructible from the fact that the regular 3 -gon and the regular 5 -gon are.
(c) More generally, prove that if $m$ and $n$ are coprime and both the $m$-gon and the $n$-gon are constructible, then so is the $m n$-gon.

Solution: We repeatedly use the fact that a regular $n$-gon is constructible if and only if its associated angle $2 \pi / n$ is constructible.
(a) We know from the lecture that $\cos (\pi / 9)$ is not constructible. Using the trigonometric identity $\cos ^{2}(\alpha)=\frac{1+\cos (2 \alpha)}{2}$, we write

$$
\cos (2 \pi / 9)=2(\cos (\pi / 9))^{2}-1
$$

Since $\cos (\pi / 9)$ is not constructible, neither is its square and it follows that $\cos (2 \pi / 9)$ is not constructible.
(b) If the regular 3 - and 5 -gons are constructible, then their angles $2 \pi / 3$ and $2 \pi / 5$ are. Thus so is the angle $2 \cdot 2 \pi / 5-2 \pi / 3=2 \pi / 15$ of the regular 15 -gon.
(c) With coprime $m$ and $n$, set $\alpha:=2 \pi / m n$, and assume we can construct $\beta=2 \pi / n=m \alpha$ and $\gamma=2 \pi / m=n \alpha$. Since $m$ and $n$ are coprime, by Euclidean division there exist integers $u$ and $v$ such that $1=u m+v n$. Thus, $\alpha=u \beta+v \gamma$ can also be constructed.
3. Is it possible to construct a square whose area is that of a given triangle?

Solution: Let $\Delta$ denote the given triangle. As area $(\Delta)=\frac{1}{2} b h$, where $b$ refers to the base of $\Delta$ and $h$ to its height, we construct a length $s$ such that $s^{2}=\frac{1}{2} b h$. We know how to mark off lengths, here $b / 2$ and $h$, onto a constructed line so that the two segments are adjacent. Then take the circle passing through the endpoints of diameter $b / 2+h$, and then the triangle inscribed in this circle with vertices the endpoints.
We can now check that the height $s$ of this triangle is exactly the length we are looking for by checking

$$
\frac{s}{h}=\frac{b / 2}{s} .
$$

Denote the angles $\alpha, \beta$, $\gamma$, where $\beta=\pi / 2$ breaks down in $\beta=\beta_{1}+\beta_{2}$ for the triangle on the left and the triangle on the right. We then observe

$$
\frac{s}{h}=\tan \gamma=\tan \left(\pi / 2-\beta_{2}\right)=\tan \left(\beta_{1}\right)=\frac{b / 2}{s} .
$$

4. Show that a root $\alpha$ of $f(X):=X^{4}-4 X+2 \in \mathbb{Q}[X]$ generates a degree 4 extension of $\mathbb{Q}$ but is not constructible.

Hint: The splitting field of $f$ over $\mathbb{Q}$ has Galois group $S_{4}$.
Solution: The polynomial $f$ is irreducible by the Eisenstein criterion at $p=2$, thus any root of $f$ generates a degree 4 extension of $\mathbb{Q}$.
Let $E$ be the splitting field of $f$ over $\mathbb{Q}$.
Version 1. If the roots of $f$ were constructible, then all the elements of $E$ would be constructible. Let $H$ be a 2-Sylow $\operatorname{subgroup}$ of $\operatorname{Gal}(E / \mathbb{Q})$. Then the fixed field $E^{H}$ has odd degree over $\mathbb{Q}$, and so the elements of $E^{H} / \mathbb{Q}$ cannot be constructible.
Version 2. By Corollary 7 of the lecture, a number $\alpha \in \mathbb{C}$ is constructible if and only if it lies in a tower of degree 2 extensions. Suppose there exists a tower of quadratic extensions $\mathbb{Q}[\alpha] \supset F \supset \mathbb{Q}$. By Galois theory, the groups $\operatorname{Gal}(E / F) \supset$ $\operatorname{Gal}(E / \mathbb{Q}[\alpha])$ have orders 12 and 6 respectively. $\operatorname{As} \operatorname{Gal}(E / \mathbb{Q})=S_{4}$, we must have $\operatorname{Gal}(E / F)=A_{4}$. But $A_{4}$ has no subgroup of order 6 - contradiction.

