Musterlösung 17

Konstruktionen mit Zirkel und Lineal

1. Zeige, dass ein reguläres Pentagon mit Zirkel und Lineal konstruierbar ist,

   (a) abstrakt mit Hilfe von Körpertheorie.

   (b) durch Angabe einer expliziten Konstruktion.

   Lösung: a) The regular pentagon is constructible if and only if the angle $\frac{2\pi}{5}$ is constructible. Set $\alpha := \frac{2\pi}{5}$ and $z := e^{i\alpha} = \cos(\alpha) + i\sin(\alpha) =: x + iy$. Then developing

   $$z^5 = (x+iy)^5 = 1$$

   into

   $$x^5 + 5xy^4 - 10x^3y^2 = 1$$

   and using $y^2 = 1 - x^2$, one gets that $\cos\alpha$ is a root of the polynomial

   $$16x^5 - 20x^3 + 5x - 1.$$

   Clearly 1 is another root and we can further factorize

   $$\begin{aligned} 16x^5 - 20x^3 + 5x - 1 &= (x-1)(16x^4 + 16x^3 - 4x^2 - 4x + 1) \\ &= (x-1)(4x^2 + 2x - 1)^2 \end{aligned}$$

   so that, by the quadratic formula and the fact that $\alpha = \cos(2\pi/5) > 0$, we get

   $$\alpha = \frac{-1+\sqrt{5}}{4}.$$

   So α has degree 2 over $\mathbb{Q}$ and is therefore constructible over $\mathbb{Q}$.

   b) Start from the points 0 and 1 in the complex plane.

   - Construct the length $\cos(2\pi/5)$.
     i) Draw the line through 1 perpendicular to the real line and construct $1+2i$. The distance between 0 and $1+2i$ is $\sqrt{5}$.
     ii) Draw the circle of radius 1 around 0, let P be its intersection point with the line segment between 0 and $1+2i$. The distance between P and $1+2i$ is $\sqrt{5}-1$.

iii) Construct the midpoint of the line segment between P and $1+2i$, and the midpoint between the just constructed point and $1+2i$. Call it Q. Then, the distance between Q and $1+2i$ is $\frac{\sqrt{5}-1}{4} = \cos(2\pi/5)$.

- Construct the pentagon.
  i) Construct the point $\cos(2\pi/5)$ on the positive real line.
  ii) Draw the line perpendicular to real line through $\cos(2\pi/5)$. Call its intersection points with the unit circle A and D. The angle between the real line and the line through 0 and A (or 0 and D) is $2\pi/5$.
  iii) Draw the circle of radius $|1-A| = |1-D|$ around A and D. The intersection points with the unit circle (amongst which is 1) together with A and D are the five vertices of the pentagon.

2. Ausserirdische, die im $\mathbb{R}^n$ leben, haben dich gebeten, den n-Würfel mit Zirkel und Lineal zu verdoppeln. Für welche Werte von n kannst du das erreichen?

   Lösung: Der n-Würfel kann genau dann mit Zirkel und Lineal verdoppelt werden, wenn seine Kantenlänge $\sqrt[n]{2}$ konstruierbar ist.

   Diese Zahl ist eine Nullstelle des normierten Polynoms $X^n - 2 \in \mathbb{Q}[X]$. Nach Eisenstein mit $p = 2$ ist dieses irreduzibel; folglich ist es das Minimalpolynom von $\sqrt[n]{2}$ über $\mathbb{Q}$. Daher gilt $[\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}] = n$.

   Nach der Vorlesung ist der Grad über $\mathbb{Q}$ jedes Elementes von $\mathrm{Kons}(\{0,1\})$ eine Zweierpotenz. Also kann $\sqrt[n]{2}$ höchstens dann konstruierbar sein, wenn n eine Zweierpotenz ist. Umgekehrt ist $\sqrt[2^m]{2}$ konstruierbar für jede natürliche Zahl m, denn für $m = 0$ ist $\sqrt[2^0]{2} = 2 \in \mathbb{Q}$ und für $m > 0$ ist $\sqrt[2^m]{2}$ eine Quadratwurzel aus $\sqrt[2^{m-1}]{2}$ und die Aussage folgt durch Induktion.

   Somit kannst du den Wunsch der Ausserirdischen genau dann erfüllen, wenn n eine Zweierpotenz ist.

3. Sei $\zeta := e^{2\pi i/p}$ für eine ungerade Primzahl p. Zeige:

   (a) $[\mathbb{Q}(\zeta)/\mathbb{Q}] = p - 1$. (*Hinweis:* Eisenstein-Kriterium.)
   (b) Ist ein regelmässiges p-Eck konstruierbar, so ist p eine *Fermat-Primzahl*, das heisst, $p = 2^{2^k} + 1$ für ein $k \geqslant 0$.

   Lösung: a) Es gilt $\zeta^p = 1$, also ist ζ eine Nullstelle des Polynoms $X^p - 1$. Aus der Zerlegung $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X + 1)$ folgt, dass ζ sogar eine Nullstelle des Polynoms $\Phi_p := X^{p-1} + \ldots + X + 1 \in \mathbb{Z}[X]$ ist. Wir wollen nun zeigen, dass Φ_p irreduzibel ist. Daraus wird folgen, dass Φ_p das Minimalpolynom von ζ über $\mathbb{Q}$ ist, und somit, dass $[\mathbb{Q}(\zeta)/\mathbb{Q}] = \deg \Phi_p = p - 1$ ist.

   Die Irreduzibilität von Φ_p wurde schon in Algebra I Abschnitt 2.7 gezeigt. Zur Erinnerung: Mit der Substitution $X \leftrightarrow Y + 1$ ist

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}.$$

Also ist $\Phi_p(Y)$ ein normiertes Polynom vom Grad $p-1$, und der k-te Koeffizient ist $\binom{p}{k+1}$. Somit erfüllt $\Phi_p(Y)$ die Voraussetzungen des Eisenstein-Kriteriums für die Primzahl p, nämlich:

- Der höchste Koeffizient ist 1, also nicht durch p teilbar,
- für $0 \leqslant k \leqslant p-2$ ist $\binom{p}{k+1}$ durch p teilbar, also sind alle tieferen Koeffizienten durch p teilbar,
- der konstante Term ist $\binom{p}{1} = p$, also nicht durch p^2 teilbar.

b) Ein regelmässiges p-Eck ist genau dann konstruierbar, wenn die primitive p-te Einheitswurzel ζ konstruierbar ist. Aus der Vorlesung ist bekannt, dass für jede konstruierbare Zahl α der Grad $[\mathbb{Q}(\alpha)/\mathbb{Q}]$ eine Zweierpotenz ist. Damit ζ also konstruierbar sein kann, muss $p-1$ nach (a) eine Zweierpotenz sein, also $p = 2^m + 1$ für ein $m \geqslant 0$. Nach der Voraussetzung, dass p eine Primzahl ist, muss m ausserdem selbst eine Zweierpotenz sein; wäre nämlich $m = ab$, mit $a > 1$ ungerade und $b \geqslant 1$ beliebig, so wäre

$$p = 2^{ab} + 1 = \underbrace{(2^b + 1)}_{>1}\underbrace{(2^{b(a-1)} - 2^{b(a-2)} + 2^{b(a-3)} - + \ldots - 2^b + 1)}_{>1},$$

Widerspruch.

Bemerkung: Die Umkehrung von (b) gilt ebenfalls. Im Allgemeinen ist das regelmässige n-Eck genau dann konstruierbar, wenn

$$n = 2^k \cdot p_1 \cdots p_\ell$$

ist, wobei $k \geqslant 0$ ist und $p_1, \ldots, p_\ell$ paarweise verschiedene Fermat-Primzahlen sind. Dieses Resultat geht zurück auf Gauss.

*4. Sei $n \geqslant 1$. Zeige, dass die n-Teilung eines allgemeinen Winkels mit Zirkel und Lineal genau dann möglich ist, wenn n eine Zweierpotenz ist.

Lösung: Da die Zweiteilung des allgemeinen Winkels möglich ist, gilt dasselbe auch für die n-Teilung des allgemeinen Winkels für jede Zweierpotenz n. Es bleibt also umgekehrt zu zeigen, dass die n-Teilung des allgemeine Winkels nicht möglich ist, wenn n keine Zweierpotenz ist. Dazu reicht es den Fall zu betrachten, in welchem $n > 2$ prim ist, denn wenn die n-Teilung eines Winkels möglich ist, dann ist auch die p-Teilung möglich für jeden Primfaktor p von n.

1. Variante: Sei also $p > 2$ prim. Wäre die p-Teilung des allgemeinen Winkels möglich, so wäre insbesondere der Winkel $2\pi/p$ und folglich auch der Winkel $2\pi/p^2$ konstruierbar. Da ein Winkel α genau dann konstruierbar ist, wenn $e^{i\alpha} \in \mathbb{C}$ konstruierbar ist, wäre dann also $\zeta := e^{2\pi i/p^2}$ konstruierbar.

Es gilt $\zeta^{p^2} = 1$, also ist ζ eine Nullstelle des Polynoms $X^{p^2} - 1$. Aus der Zerlegung $X^{p^2} - 1 = (X^p - 1)(X^{p^2-p} + X^{p^2-2p} + \ldots + X^p + 1)$ folgt wegen $\zeta^p - 1 \neq 0$, dass

ζ sogar eine Nullstelle des Polynoms $\Phi_{p^2} := X^{p^2-p} + \ldots + X^p + 1$ ist. Durch die Substitution $X \leftrightarrow Y + 1$ und mithilfe der Feststellung

$$(Y+1)^p \equiv Y^p + 1 \pmod{p}$$

erhalten wir

$$\begin{aligned}
\Phi_{p^2}(X) &= (X^p)^{p-1} + \ldots + X^p + 1 \\
&= ((Y+1)^p)^{p-1} + \ldots + (Y+1)^p + 1 \\
&\equiv (Y^p+1)^{p-1} + \ldots + (Y^p+1) + 1 \pmod{p} \\
&= \frac{(Y^p+1)^p - 1}{(Y^p+1) - 1} \\
&= \sum_{k=1}^{p} \binom{p}{k} (Y^p)^{k-1} \\
&\equiv Y^{p^2-p} \pmod{p}.
\end{aligned}$$

Also ist der höchste Koeffizient von $\Phi_{p^2}(Y)$ nicht durch p teilbar, alle tieferen Koeffizienten aber schon. Zudem liest man aus

$$\Phi_{p^2}(Y) = ((Y+1)^p)^{p-1} + \ldots + (Y+1)^p + 1$$

ab, dass der konstante Term von $\Phi_{p^2}(Y)$ gerade p ist, also insbesondere nicht durch p^2 teilbar.

Somit erfüllt $\Phi_{p^2}(Y)$ die Voraussetzungen des Eisenstein-Kriteriums; also ist Φ_{p^2} irreduzibel und somit das Minimalpolynom von ζ. Daraus folgt, dass der Grad $[\mathbb{Q}(\zeta)/\mathbb{Q}] = p^2 - p$ ist, also insbesondere keine Zweierpotenz. Somit haben wir gezeigt, dass ζ und damit der Winkel $2\pi/p^2$ nicht konstruierbar sind.

2. Variante: Der Satz von de Moivre lautet für jede ganze Zahl $p \geqslant 1$

$$\begin{aligned}
\cos x + i \sin x &= \left(\cos \tfrac{x}{p} + i \sin \tfrac{x}{p}\right)^p \\
&= \textstyle\sum_{k=0}^{p} \binom{p}{k} i^k (\cos \tfrac{x}{p})^{p-k} (\sin \tfrac{x}{p})^k \ .
\end{aligned}$$

Durch Vergleichen der Realteile beider Seiten der Gleichung erhalten wir für p ungerade

$$\begin{aligned}
\cos x &= \textstyle\sum_{k=0}^{(p-1)/2} \binom{p}{2k} (-1)^k (\cos \tfrac{x}{p})^{p-2k} (\sin \tfrac{x}{p})^{2k} \\
&= \textstyle\sum_{k=0}^{(p-1)/2} \binom{p}{2k} (-1)^k (\cos \tfrac{x}{p})^{p-2k} (1 - \cos^2 \tfrac{x}{p})^k \ .
\end{aligned}$$

Wir setzen $a := \cos \frac{x}{p}$ und $b := \cos x$. Dann ist nach der letzten Gleichung a eine Nullstelle des Polynoms

$$F_p(X) := \sum_{k=0}^{(p-1)/2} \binom{p}{2k} (-1)^k X^{p-2k} (1-X^2)^k - b.$$

Sei nun $p \geqslant 3$ prim. In diesem Fall gilt $p \,|\, \binom{p}{2k} = \frac{p\cdot(p-1)\cdots(p-2k+1)}{1\cdot 2\cdots 2k}$ für $1 \leqslant k \leqslant (p-1)/2$, also kann man schreiben

$$\begin{aligned} F_p(X) &= X^p + p\sum_{k=1}^{(p-1)/2} c_k X^{p-2k}(1-X^2)^k - b \\ &= X^p + pG_p(X) - b \end{aligned}$$

mit $c_k = \frac{(-1)^k}{p}\binom{p}{2k}$ und $G_p(X) = \sum_{k=1}^{(p-1)/2} c_k X^{p-2k}(1-X^2)^k \in \mathbb{Z}[X]$. Das Polynom F_p hat also Grad p und besteht abgesehen vom konstanten Term $-b = -\cos x$ nur aus Termen von ungeradem Grad. Sei q die nächstgrösste Primzahl nach p. Dann gilt $p/q < 1$ und $x_p = \arccos(p/q)$ ist wohldefiniert. Für dieses $x = x_p$ ist $b \in \mathbb{Q}$ und das Polynom F_p irreduzibel über $\mathbb{Q}$, da das primitive Polynom

$$qF_p(X) = qX^p + pqG_p(X) - p \in \mathbb{Z}[X]$$

wegen des Eisensteinkriteriums mit der Primzahl p irreduzibel ist. In der Tat gilt:

- Der höchste Koeffizient ist kongruent zu $q \not\equiv 0$ modulo p.
- Alle anderen Koeffizienten sind durch p teilbar.
- Der konstante Koeffizient ist gleich $-p$, also nicht durch p^2 teilbar.

Somit ist $a = \cos\frac{x_p}{p}$ als Nullstelle von F_p vom Grad p über $\mathbb{Q}$, was keine Zweierpotenz ist. Daher ist $\cos\frac{x_p}{p}$ nicht konstruierbar und der Winkel x_p nicht p-teilbar.