D-MATH Algebra I HS 2022
Prof. Richard Pink

Musterlösung Serie 11

Algebraische Körpererweiterungen, Konstruktionen mit Zirkel und Lineal

1. Sei $n \in \mathbb{Z}_{\geqslant 1}$ und p eine Primzahl. Zeige:

   (a) Für alle $m \in \mathbb{Z}_{\geqslant 1}$ mit $m < n$ ist $(\sqrt[n]{p})^m \notin \mathbb{Q}$.

   (b) Das Polynom $X^n - p$ ist irreduzibel über $\mathbb{Q}$.

   (c) Die Körpererweiterung $\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}$ hat Grad n.

   (d) Für jedes $m \in \mathbb{Z}_{\geqslant 1}$ bestimme das Minimalpolynom von $\sqrt[mn]{p}$ über $\mathbb{Q}(\sqrt[n]{p})$.

   (e) Es existiert ein unendlicher Körperturm der Form $\ldots/K_i/\ldots/K_1/K_0 = \mathbb{Q}$ mit $[K_i/K_{i-1}] = 2$ für alle $i \geqslant 1$.

   (f) Es existiert eine algebraische Körpererweiterung $K/\mathbb{Q}$, die nicht endlich ist.

   Lösung:

   (a) Wenn $(\sqrt[n]{p})^m$ rational wäre, so würden teilerfremde $a, b \in \mathbb{Z}$ existieren, sodass $(\sqrt[n]{p})^m = \frac{a}{b}$. Dies implizierte $p^m = \frac{a^m}{b^m}$. Aufgrund der Teilerfremdheit von a und b folgte damit $b = 1$. Also wäre $p^m = a^n$, was im Widerspruch dazu steht, dass p eine Primzahl und $0 < m < n$ ist.

   (b) Aus der Multiplikativität der komplexen Betragsfunktion folgt, dass alle Nullstellen von $X^n - p$ den Betrag $\sqrt[n]{p}$ haben. Der konstante Koeffizient eines normierten Faktors von $X^n - p$ vom Grad $0 < m < n$ hat dann einen konstanten Koeffizienten mit Betrag $(\sqrt[n]{p})^m$, welcher nach (a) nicht rational ist. Deswegen ist $X^n - p$ irreduzibel.

   (c) Die Zahl $\sqrt[n]{p}$ ist Nullstelle des normierten Polynoms $X^n - p$. Da dieses irreduzibel über $\mathbb{Q}$ ist, ist es das Minimalpolynom von $\sqrt[n]{p}$ über $\mathbb{Q}$. Somit ist $[\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}] = \deg(X^n - p) = n$.

   (d) Setze $F := \mathbb{Q}(\sqrt[n]{p})$ und $E := \mathbb{Q}(\sqrt[mn]{p})$. Wegen $\sqrt[n]{p} = (\sqrt[mn]{p})^m \in E$ gilt dann $F \subset E$. Aus (c) und der Multiplikativität der Körpergrade folgt nun

   $$mn \;=\; [E/\mathbb{Q}] \;=\; [E/F] \cdot [K/\mathbb{Q}] \;=\; [E/F] \cdot n$$

   und damit $[E/F] = m$. Wegen $F \subset E = \mathbb{Q}(\sqrt[mn]{p})$ ist aber auch $E = F(\sqrt[mn]{p})$. Daher hat das Minimalpolynom von $\sqrt[mn]{p}$ über F den Grad m. Schliesslich ist $\sqrt[mn]{p}$ eine Nullstelle des normierten Polynoms $X^m - \sqrt[n]{p} \in F[X]$. Folglich ist dieses das Minimalpolynom von $\sqrt[mn]{p}$ über $F = \mathbb{Q}(\sqrt[n]{p})$.

(e) Für jedes $i \geqslant 0$ setzen wir $K_i := \mathbb{Q}(\sqrt[2^i]{p})$. Nach (c) ist dann $[K_i/\mathbb{Q}] = 2^i$. Weiter ist $(\sqrt[2^i]{p})^2 = \sqrt[2^{i-1}]{p}$, weswegen K_{i-1} in K_i enthalten ist. Die Gleichung

$$2^i = [K_i/\mathbb{Q}] = [K_i/K_{i-1}] \cdot [K_{i-1}/\mathbb{Q}] = [K_i/K_{i-1}] \cdot 2^{i-1}$$

impliziert dann $[K_i/K_{i-1}] = 2$. Damit haben wir den gesuchten Körperturm.

(f) Setze $K := \bigcup_{i \geqslant 0} K_i$ mit den K_i aus (e). Für je zwei $x, y \in K$ wähle $i, j \geqslant 0$ mit $x \in K_i$ und $y \in K_j$. Für $k := \max\{i, j\}$ ist dann $x, y \in K_k$, also liegen $x \pm y$ und xy sowie x/y, falls definiert, schon in $K_k \subset K$. Da ausserdem $0, 1$ in K sind, ist K also ein Unterkörper von $\mathbb{R}$.

Weiter ist die Erweiterung $K_i/\mathbb{Q}$ endlich und daher algebraisch für jedes i. Somit ist jedes Element von $K = \bigcup_{i \geqslant 0} K_i$ algebraisch über $\mathbb{Q}$. Daher ist $K/\mathbb{Q}$ eine algebraische Körpererweiterung. Schliesslich ist $[K/\mathbb{Q}] \geqslant [K_i/\mathbb{Q}] = 2^i$ für alle i. Somit muss $[K/\mathbb{Q}] = \infty$ sein.

2. 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 $\alpha := \frac{2\pi}{5}$ is constructible. From the lecture course we know that this is so if and only if $\cos\alpha$ is a constructible length. Set $z := e^{i\alpha}$, so that $z^5 = e^{2\pi i} = 1$ and $z \neq 0, 1$. Then

$$z^2 + z + 1 + z^{-1} + z^{-2} \;=\; \frac{z^4 + z^3 + z^2 + z + 1}{z^2} \;=\; \frac{z^5 - 1}{z^2(z-1)} \;=\; 0.$$

But the fact that $2\cos\alpha = e^{i\alpha} + e^{-i\alpha} = z + z^{-1}$ implies that $4\cos^2\alpha = (z + z^{-1})^2 = z^2 + 2 + z^{-2}$. Plugging this into the preceding equation yields that

$$4\cos^2\alpha + 2\cos\alpha - 1 \;=\; z^2 + z + 1 + z^{-1} + z^{-2} \;=\; 0.$$

Solving this quadratic equation and using the fact that $\cos\alpha > 0$ implies that

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

Thus $\cos\alpha$ 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.

3. 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 Aufgabe 1 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.

4. Sei p eine ungerade Primzahl. Zeige:

   (a) Für $\zeta := e^{2\pi i/p}$ gilt $[\mathbb{Q}(\zeta)/\mathbb{Q}] = p - 1$.

   (b) Ist ein regelmässiges p-Eck mit Zirkel und Lineal konstruierbar, so ist p eine *Fermat-Primzahl*, das heisst, $p = 2^{2^k} + 1$ für ein $k \geqslant 0$.

   (c) Die p-Teilung eines allgemeinen Winkels mit Zirkel und Lineal ist nicht möglich.

   Es darf ohne Beweis verwendet werden, dass das *zyklotomische Polynom* $\Phi_p(X) := X^{p-1} + \ldots + X + 1$ sowie das Polynom $\Phi_p(X^p)$ über $\mathbb{Q}$ irreduzibel ist.

   Lösung: (a) Wegen $\zeta^p = 1$ ist ζ eine Nullstelle des Polynoms $X^p - 1$. Mit $\zeta \neq 1$ folgt aus der Zerlegung $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \ldots + X + 1)$, dass ζ sogar eine Nullstelle von Φ_p ist. Da Φ_p irreduzibel und normiert ist, ist es also das Minimalpolynom von ζ über $\mathbb{Q}$. Somit ist $[\mathbb{Q}(\zeta)/\mathbb{Q}] = \deg \Phi_p = p - 1$.

(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 $m \geqslant 0$.

Ausserdem soll p ja eine Primzahl sein. Ist aber $m = ab$ mit $a > 1$ ungerade und beliebigem $b \geqslant 1$, so ist $(Y^a+1) = (Y+1)(Y^{a-1} - Y^{a-2} + -... - Y + 1)$ und daher

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

zusammengesetzt. Somit kann $p = 2^m+1$ nur prim sein, wenn m eine Zweierpotenz ist, das heisst, wenn $p = 2^{2^k} + 1$ ist für eine natürliche Zahl $k \geqslant 0$.

Bemerkung: Die ersten fünf Zahlen dieser Form sind allesamt Primzahlen:

$$2^1 + 1 = 3, \quad 2^2 + 1 = 5, \quad 2^4 + 1 = 17, \quad 2^8 + 1 = 257, \quad 2^{16} + 1 = 65537.$$

Danach ist keine weitere Fermat-Primzahl bekannt.

Bemerkung: In einer Doktorarbeit in Göttingen um 1900 herum hat jemand eine explizite Konstruktion des regelmässigen 65537-Ecks ausgeführt.

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.

(c) Wäre die p-Teilung eines 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 $\xi := e^{2\pi i/p^2}$ konstruierbar. Nach (a) ist $\xi^p = e^{2\pi i/p}$ eine Nullstelle von Φ_p, also ξ eine Nullstelle des Polynoms $\Phi_p(X^p)$. Da dieses normiert und irreduzibel über $\mathbb{Q}$ ist, ist es das Minimalpolynom von ξ über $\mathbb{Q}$. Somit gilt $[\mathbb{Q}(\xi)/\mathbb{Q}] = \deg(\Phi_p(X^p)) = p^2 - p$. Da dies keine Zweierpotenz ist, ist ξ und damit der Winkel $2\pi/p^2$ nicht konstruierbar.