Algebra I

Musterlösung 21

Konstruktionen mit Zirkel und Lineal, symmetrische Gruppen

---

126. 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.

127. (a) Zeige, dass sich ein Winkel α genau dann mit Zirkel und Lineal dreiteilen lässt, wenn das Polynom $4X^3 - 3X - \cos(\alpha)$ reduzibel über $\mathbb{Q}(\cos(\alpha))$ ist.

(b) Zeige, dass für jede nicht durch 3 teilbare natürliche Zahl n die Dreiteilung des Winkels $\frac{2\pi}{n}$ möglich ist.

Lösung: (a) Im Gegensatz zur Vorlesung startet man hier nicht nur mit den Punkten 0 und 1, sondern mit $0, 1$ und $\cos(\alpha)$. Die Resultate aus der Vorlesung lassen sich aber offensichtlich folgendermasse übertragen. Der Winkel α lässt sich genau dann mit Zirkel und Lineal dreiteilen, wenn $\cos(\frac{\alpha}{3})$ über $\mathbb{Q}(\alpha)$ konstruierbar ist. Das ist genau dann der Fall, wenn es einen Körperturm $K_n : \cdots : K_0 = \mathbb{Q}(\alpha)$ gibt, sodass die Erweiterung $[K_i : K_{i-1}] = 2$ ist und $\cos(\frac{\alpha}{3})$ in K_n liegt.

Mit Hilfe bekannter Identitäten, z.B. $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$, berechnen wir, dass $\cos(\frac{\alpha}{3})$ eine Nullstelle des Polynoms $4X^3 - 3X - \cos(\alpha)$ ist. Falls das Polynom also irreduzibel ist, so hat $\cos(\frac{\alpha}{3})$ den Grad 3 über $\mathbb{Q}(\alpha)$, ist also nicht konstruierbar. Falls das Polynom jedoch reduzibel ist, so hat $\cos(\frac{\alpha}{3})$ den Grad 1 oder 2 über $\mathbb{Q}(\alpha)$, ist also konstruierbar.

(b) Sei $\alpha = \frac{2\pi}{n}$. Wir wissen, dass der Winkel $\frac{2\pi}{3}$ konstruierbar ist, denn er ist die Verdopplung eines Winkels in einem gleichseitigen Dreieck. Da n nicht durch 3 teilbar ist, existiert ein $k \in \mathbb{N}$ mit $k\alpha < \frac{2\pi}{3} < (k+1)\alpha$. Somit gilt $\frac{2\pi}{3} - k\alpha = \frac{\alpha}{3}(n-3k)$, und nach Wahl von k ist $n-3k$ gleich 1 oder 2. Da wir Winkel halbieren können, ist $\frac{\alpha}{3}$ also konstruierbar.

128. 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 $k \geq 0$.

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 beweisen wir ähnlich wie in Aufgabe 87. 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 $0 \leq k \leq p-2$ 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 Real- und Imaginärteil $\cos(\zeta)$ und $\sin(\zeta)$ der primitiven p-ten Einheitswurzel ζ konstruierbar sind. Aus der Vorlesung ist bekannt, dass für jede konstruierbare Zahl α der Grad $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ eine Zweierpotenz ist. Also muss auch $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ eine Zweierpotenz sein, denn $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\cos(\zeta), \sin(\zeta), i)$. Damit ζ also konstruierbar sein kann, muss $p-1$ nach (a) eine Zweierpotenz sein, also $p = 2^m + 1$ für ein $m \geq 0$. Nach der Voraussetzung, dass p eine Primzahl ist, muss m ausserdem selbst eine Zweierpotenz sein; wäre nämlich $m = ab$, mit $a > 1$ ungerade und $b \geq 1$ 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 $k \geq 0$ ist und $p_1, \ldots, p_\ell$ paarweise verschiedene Fermat-Primzahlen sind. Dieses Resultat geht zurück auf Gauss.

129. Sei $L \subset \mathbb{C}$ der Körper der über $\mathbb{Q}$ mit Zirkel und Lineal konstruierbaren Zahlen.

Zeige, dass $L : \mathbb{Q}$ eine normale Erweiterung ist.

Lösung: Wir benutzen zwei Lemmata.

Lemma 1: Sei $M : K$ eine endliche Körpererweiterung, sei $\tilde{M}$ ein weiterer Körper und sei $\psi\colon M \to \tilde{M}$ ein Körperhomomorphismus. Dann ist $[M : K] = [\psi(M) : \psi(K)]$.

Beweisskizze: Es lässt sich schnell nachprüfen, dass eine K-Basis $m_1, \ldots, m_{[M:K]}$ von M von ψ auf eine $\psi(K)$-Basis von $\psi(M)$ abgebildet wird.

Lemma 2: Eine komplexe Zahl α ist genau dann konstruierbar, wenn es einen quadratischen Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{C}$ gibt mit $\alpha \in K_n$.

Beweis: Wir wissen aus der Vorlesung, dass $\alpha = a + ib \in \mathbb{C}$ genau dann konstruierbar ist, falls es einen quadratischen Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_{n-1} \subset \mathbb{R}$ mit $a, b \in K_{n-1}$ gibt. Mit $K_n := K_{n-1}(i)$ liegt $\alpha \in K_n$ und wir haben die eine Richtung bewiesen. Sei umgekehrt $\alpha \in \mathbb{C}$, sodass es einen quadratischen Körperturm $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{C}$ gibt mit $\alpha \in K_n$. Sei $\beta_i \in K_i \setminus K_{i-1}$ und $X^2 + aX + b$ sein Minimalpolynom über K_{i-1}. Es ist $X^2 + aX + b = (X + \frac{a}{2})^2 - \frac{a^2}{4} + b$. Somit gibt es jeweils ein $\alpha_i \in K_i \setminus K_{i-1}$ mit $\alpha_i^2 \in K_{i-1}$, nämlich $\alpha_i = \beta_i + \frac{a}{2}$. Mit Aufgabe 125 ist α_i konstruierbar und wegen $K_i = K_{i-1}(\alpha_i)$ sind somit alle Zahlen aus K_i konstruierbar, insbesondere auch α.

Sei $\alpha \in L$ und $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{C}$ ein quadratischer Körperturm mit $\alpha \in K_n$. Für jeden Homomorphismus $\varphi \in \mathrm{Hom}(L, \overline{\mathbb{Q}})$ in einen algebraischen Abschluss $\overline{\mathbb{Q}} \subset \mathbb{C}$ ist $\varphi(\mathbb{Q}) = \mathbb{Q} \subset \varphi(K_1) \subset \ldots \subset \varphi(K_n)$ wiederum ein quadratischer Erweiterungsturm über $\mathbb{Q}$ wegen Lemma 1. Dann ist $\varphi(\alpha) \in \varphi(K_n)$, also ist $\varphi(\alpha)$ auch in so einem quadratischen Körperturm enthalten. Nach Lemma 2 ist $\varphi(\alpha)$ konstruierbar, das heisst in L enthalten. Soimt gilt $\varphi(L) \subset L$ für jeden solchen Homomorphismus φ; und nach Aufgabe 103 ist $L : \mathbb{Q}$ eine normale Erweiterung.

130. Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom und sei L dessen Zerfällungskörper über $\mathbb{Q}$.

Zeige: Falls $[L : \mathbb{Q}]$ einen ungeraden Primteiler hat, so ist keine Nullstelle von f mit Zirkel und Lineal konstruierbar.

Lösung: Sei $K \subset \mathbb{C}$ der Körper der über $\mathbb{Q}$ mit Zirkel und Lineal konstruierbaren Zahlen. Nach Aufgabe 120 ist die Erweiterung $K : \mathbb{Q}$ normal. Sei nun $a \in \mathbb{C}$ eine Nullstelle von f. Wir leiten aus der Annahme, dass a konstruierbar ist über $\mathbb{Q}$, einen Widerspruch her.

Wegen der Normalität sind auch alle anderen Nullstellen von f in K. Da K ein Körper ist, sind somit alle Elemente des Zerfällungskörpers von f in K. Sei dieser $L \subseteq K$.

Variante 1: Es gilt $[L : \mathbb{Q}] = \mathrm{Gal}(L : \mathbb{Q})$. Sei $G \leq \mathrm{Gal}(L : \mathbb{Q})$ eine Sylow 2-Untergruppe. Da $[L : \mathbb{Q}]$ einen ungeraden Primteiler besitzt, ist G eine echte Untergruppe. Sei L^G der Fixkörper von G. Nach einem Korollar des Hauptsatzes der Galoistheorie gilt $[L : L^G] = |G|$ und weiter

$$[L^G : \mathbb{Q}] = [\mathrm{Gal}(L : \mathbb{Q}) : G] = \frac{|\mathrm{Gal}(L : \mathbb{Q})|}{|G|}.$$

Dieser Erweiterungsgrad ist also grösser als 1 und ungerade. Sei $b \in L^G \setminus \mathbb{Q}$. Für dieses b ist $[\mathbb{Q}(b) : \mathbb{Q}]$ ungerade und grösser als 1. Also hat das Minimalpolynom von b über $\mathbb{Q}$ ungeraden Grad, folglich eine reelle Nullstelle. Diese ist laut Vorlesung nicht mit Zirkel und Lineal konstruierbar, denn ihr Grad über $\mathbb{Q}$ ist ungerade. Dies ist ein Widerspruch.

Variante 2: Sei $\tilde{L} \subseteq \mathbb{R}$ der kleinste Körper welcher die Menge $\{a, b \in \mathbb{R} : a + bi \in L\}$ enthält. Dann ist $\mathbb{Q} \subseteq \tilde{L} \subseteq \mathbb{R}$ und $\tilde{L}$ ist ein konstruierbarer Körper.

- Ist $L = \tilde{L}$, so ist $[L : \mathbb{Q}] = [\tilde{L} : \mathbb{Q}]$ und $[\tilde{L} : \mathbb{Q}]$ hat einen ungeraden Primteiler.
- Andernfalls ist $L \subseteq \tilde{L}(i)$ und $[\tilde{L}(i) : \mathbb{Q}] = [\tilde{L}(i) : L] \cdot [L : \mathbb{Q}]$. Wir prüfen zuerst nach, dass $[\tilde{L}(i) : \mathbb{Q}]$ endlich ist, indem wir $\tilde{L}(i) \subseteq L(i)$ beweisen. Sei $a + ib \in L$ mit $a, b \in \mathbb{R}$. Wir wollen zeigen, dass a und b in $L(i)$ sind. Da L normal über $\mathbb{Q}$ ist, ist auch $a - ib \in L$. Folglich ist $2a \in L$ und somit gilt $a \in L(i)$. Also ist auch $bi \in L$ und damit $b \in L(i)$. Somit ist $\tilde{L}(i) \subseteq L(i)$. Weil $[L : \mathbb{Q}]$ einen ungeraden Primteiler hat, hat auch $[\tilde{L}(i) : \mathbb{Q}]$ einen ungeraden Primteiler, und weil $[\tilde{L}(i) : \mathbb{Q}] = [\tilde{L}(i) : \tilde{L}] \cdot [\tilde{L} : \mathbb{Q}]$ und $[\tilde{L}(i) : \tilde{L}] = 2$, hat auch $[\tilde{L} : \mathbb{Q}]$ einen ungeraden Primteiler.

Da nun $\tilde{L}$ ein konstruierbarer Körper ist, haben wir $[\tilde{L} : \mathbb{Q}] = 2^k$, und somit kann $[\tilde{L} : \mathbb{Q}]$ keinen ungeraden Primteiler besitzen.

131. Sei $n \geq 5$ eine natürliche Zahl.

(a) Zeige, dass die Gruppe A_n einfach ist.
Hinweis: Sei $N \trianglelefteq A_n$ ein nichttrivialer Normalteiler. Zeige, dass N einen 3-Zykel der Form $ngn^{-1}g^{-1}$ mit $n \in N$ und $g \in A_n$ enthält.

(b) Folgere daraus, dass A_n die einzige normale Untergruppe von S_n ist.

Lösung: (a) Wir wissen aus der Algebra I, dass A_n von allen 3-Zykeln erzeugt ist, und auch, dass alle 3-Zykeln zueinander konjugiert sind. Wenn wir also beweisen können, dass N einen 3-Zykel enthält, dann enthält N alle 3-Zykeln und wir sind fertig.

Sei $n \in N$ ein nichttriviales Element. Schreibe $n = \sigma_1 \dots \sigma_m$ als Produkt elementfremder Zyklen. Nun unterscheiden wir drei Fälle.

Fall 1: Einer der Zykeln hat Länge > 3.

Sei dieser Zykel $(a_1\, a_2\, \dots\, a_l)$ mit $l > 3$. Sei $g = (a_1\, a_2\, a_3)$. Dann ist $ngn^{-1}g^{-1} = (a_1\, a_3\, a_2)$. Ausserdem ist dieses Element sicher in N, da wegen der Normalität $gn^{-1}g^{-1} \in N$ ist.

Fall 2: Einer der Zykel ist ein 3-Zykel und ein anderer Zykel ist ein 2- oder 3-Zykel.

Seien diese Zykeln $(a_1\, a_2\, a_3)$ und entweder $(b_1\, b_2)$ oder $(b_1\, b_2\, b_3)$. Sei $h = (a_1\, a_2\, b_1)$. Dann ist $nhn^{-1}h^{-1} = (a_1\, b_1\, a_3\, b_2\, a_2) \in N$ und wir sind im 1. Fall.

Fall 3: Alle Zyklen sind Transpositionen.

Da $n \in A_n$ ist, ist $k \geq 2$. Seien diese Zyklen $(a_1\, a_2)$ und $(b_1\, b_2)$. Sei $h = (a_1\, b_1\, c)$ für ein $c \notin \{i, j, k, l\}$. Dann ist

$$nhn^{-1}h^{-1} = \begin{cases} (a_1\, a_2\, b_2\, c\, b_1) & \text{falls } n(c) = c \\ (a_2\, b_2\, n(c))(a_1\, c\, b_1) & \text{falls } n(c) \neq c \end{cases}$$

und wir haben uns auf die vorigen Fälle reduziert.

(b) Sei $\{e\} \neq N \neq S_n$ eine normale Untergruppe. Dann ist $N \cap A_n \trianglelefteq A_n$. Da A_n einfach ist, gilt $N \cap A_n = \{e\}$ oder $N \supseteq A_n$.

Nehmen wir zuerst an, dass $N \supseteq A_n$ gilt. Wegen $2 = [S_n : A_n] = [S_n : N][N : A_n]$ muss daher $N = A_n$ gelten.

Sei nun $N \cap A_n = \{e\}$. Seien $g, h \in N \setminus A_n$ nicht notwendigerweise verschieden. Falls keine solchen g, h existieren, ist $N = \{e\}$ und wir sind fertig. Dann hat das Produkt von g und h Signum 1, liegt also in A_n, daher gilt $gh = e$. Insbesondere sind auch g^2 und h^2 in A_n, also gleich e. Es folgt $g = g^{-1} = h = h^{-1}$. Somit kann N nur ein einziges nichttriviales Element α haben, und dieses muss Ordnung 2 haben. Ausserdem muss $\sigma\alpha\sigma^{-1} = \alpha$ für jedes $\sigma \in S_n$ gelten. Das kann aber nicht sein.