§ 5. Die Transzendenz von π und e

Erinnerung: aus der Anfängervorlesung kennen wir die Zahlbereiche

$$\mathbb{Z} \subseteq \underbrace{\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}}$$

Ring — Körper

1. Def Eine komplexe (oder reelle) Zahl $z \in \mathbb{C}$ heißt algebraisch (über $\mathbb{Q}$), wenn es ein Polynom $f \in \mathbb{Q}[X]$ gibt mit $\deg(f) \geq 1$, das in z eine Nullstelle hat.

Beispiel (a) $i = \sqrt{-1}$ ist algebraisch, denn i ist Nullstelle des Polynoms $X^2 + 1$

(b) Jede rationale Zahl $q \in \mathbb{Q}$ ist algebraisch, denn q ist Nullstelle von $X - q$.

(c) Ist $p \in \mathbb{P}$ Primzahl, so ist die reelle Zahl $\sqrt{p}$ algebraisch, aber irrational (= nicht rational).

Denn: $\sqrt{p}$ ist Nullstelle von $X^2 - p$, also algebraisch.

Angenommen, $\sqrt{p} \in \mathbb{Q}$, $\sqrt{p} = \frac{a}{b}$ $a, b \in \mathbb{N}$, $b \neq 0$,

Sei $d = ggT(a,b)$, $a = \tilde{a} \cdot d$ $b = \tilde{b} \cdot d$

$\Rightarrow \frac{a}{b} = \frac{\tilde{a}}{\tilde{b}}$ und $ggT(\tilde{a}, \tilde{b}) = 1$. D.h.

$\tilde{b}^2 \cdot p = \tilde{a}^2 \Rightarrow p \mid \tilde{a}^2$. Da $p \in \mathbb{P}$

Folgt aus §1.12, dass $p \mid \tilde{a} \Rightarrow p^2 \mid \tilde{a}^2$

$\Rightarrow p^2 \mid \tilde{b}^2 \cdot p \Rightarrow p \mid \tilde{b}$ ↯ da $ggT(\tilde{a}, \tilde{b}) = 1$

□

2. Def Eine reelle oder komplexe Zahl z heißt transzendent (über $\mathbb{Q}$), wenn z nicht algebraisch ist.

Theorem (Cantor) "Fast alle" reellen oder komplexen Zahlen sind transzendent.

Bem (a) $\mathbb{Q}$ ist abzählbar, da $\mathbb{Z} = \{0, \pm 1, \dots\}$ abzählbar ist

(b) $\mathbb{Q}[x]$ ist abzählbar (es gibt nur abz. viele mögliche Koeffizienten für Polynome $f \in \mathbb{Q}[x]$

(c) Jedes Polynom $f \in \mathbb{Q}[x]$ hat nur endlich viele Nullstellen. Also ist die Menge aller algebraisch Zahlen abzählbar

(d) $\mathbb{R} \subseteq \mathbb{C}$ ist überabzählbar = nicht abzählbar (Cantors Diagonalschluss, oder: betrachte die Menge $F = \{(a_k)_{k\geq 0} \mid a_k \in \{0,2\}\}$

F ist überabzählbar, $h: F \longrightarrow \mathbb{C}$

$$h(a_k)_{k\geq 0} = \sum_{k=0}^{\infty} a_k 3^{-k} \text{ ist injektiv.}$$

Also gibt es mehr komplexe / reelle Zahlen als algebraische Zahlen □

Cantors Satz sagt aber dirs nicht, welche reellen oder komplexen Zahlen transzendent sind. #

3. Erinn: Die Exponentialfunktion. Sei z reell oder komplex. Wir definieren:

$$\exp(z) = \sum_{k=0}^{\infty} \frac{1}{k!} z^k$$

Es gilt $\exp(0) = 1$ (klar) sowie

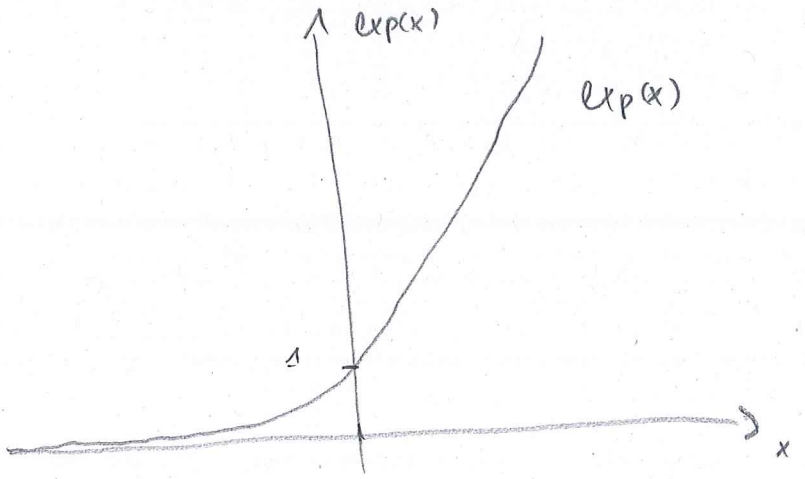
$\exp(u+v) = \exp(u) \cdot \exp(v)$. (Analysis 1)

Insbesondere $\exp(u) \cdot \exp(-u) = 1$ für alle $u \in \mathbb{C}$

$\Rightarrow$ exp hat keine Nullstelle in $\mathbb{C}$ oder $\mathbb{R}$.

Bem $\exp: \mathbb{R} \to \mathbb{R}^*$ ist ein Homomorphismus

$$\exp(u+v) = \exp(u) \cdot \exp(v).$$



$\exp(1) = e \approx 2{,}71\ldots$ ist die Eulersche Zahl,

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}$$

4. Lemma Sei $h : \mathbb{R} \to \mathbb{R}$ eine beliebig oft diff'bare Funktion, sei $\ell \in \mathbb{N}$, $\ell \geq 1$. Sei $a \in \mathbb{R}$ beliebig. Dann gilt für die k-te Ableitung der Funktion $f(x) = (x-a)^{\ell} \cdot h(x)$ an der Stelle a, dass

$$f^{(k)}(a) = \begin{cases} 0 & \text{für } 0 \leq k < \ell \\ \frac{k!}{(k-\ell)!} h^{(k-\ell)}(a) & k \geq \ell \end{cases}$$

$\uparrow$

k-te Ableitung an der Stelle a.

Beweis in zwei Schritten.

1. Schritt Für $f(x) = (x-a)\,h(x)$ gilt

$$f^{(k+1)}(x) = (x-a)\,h^{(k+1)}(x) + (k+1)\,h^{(k)}(x)$$

Beweis mit Induktion nach k.

$\underline{k=0}$ $\quad f'(x) = (x-a)\,h'(x) + h(x)$ ✓

$\underline{k \to k+1}$

$$\frac{d}{dx}\left[(x-a)\,h^{(k+1)}(x) + (k+1)\,h^{(k)}(x)\right]$$

$$= (x-a)\,h^{(k+2)}(x) + h^{(k+1)}(x) + (k+1)\,h^{(k+1)}(x)$$

$$= (x-a)\,h^{(k+2)}(x) + (k+2)\,h^{(k+1)}(x) \quad ✓$$

Es folgt insbesondere: $f^{(k+1)}(a) = (k+1)\,h^{(k)}(a)$,

damit stimmt das Lemma für $l = 1$ (und $l = 0$).

2. Schritt Das Lemma gilt für alle $l \geq 0$.

Induktion nach l

$$F(x) = (x-a)^{l+1}\,h(x) = (x-a)\underbrace{(x-a)^{l}\,h(x)}_{=\tilde{h}(x)}$$

$$f^{(k+1)}(a) = (k+1)\,\tilde{h}^{(k)}(a)$$

$$= \begin{cases} 0 & 0 \leq k < l-1 \\ (k+1)\,\dfrac{k!}{(k-l)!}\,h^{(k-l)}(a) & \end{cases} \quad ✓$$

□

5. Theorem (Hermite 1873) Die Eulersche Zahl $e = \sum_{k=0}^{\infty} \frac{1}{k!} \approx 2{,}7182818\ldots$ ist transzendent.

Beweis Angenommen, e wäre algebraisch.

Dann gibt es $a_n, \ldots, a_0 \in \mathbb{Q}$, $a_n \neq 0$ mit

$$e^n \cdot a_n + e^{n-1} \cdot a_{n-1} + \ldots + a_0 = 0, \quad n \geq 1$$

OE $a_0 \neq 0$ (sonst durch e teilen)

OE $a_n, \ldots, a_0 \in \mathbb{Z}$ (mit Hauptnenner multiplizieren)

Sei $p \in \mathbb{P}$ mit $p > n$, $|a_0|$ $\Rightarrow$ $p \nmid n, a_0$

Setze $f_p = \frac{1}{(p-1)!} X^{p-1} \cdot (X-1)^p (X-2)^p \cdots (X-n)^p$

Für $0 \leq t \leq n$ gilt $|f_p(t)| \leq \frac{1}{(p-1)!} n^{p-1} \cdot n^{n \cdot p}$

$\leq \frac{1}{(p-1)!} n^{(n+1)p}$. Damit konvergiert die Funktionenfolge $(F_p)_{p \in \mathbb{P}}$ auf dem Intervall $[0, n]$ gleichmäßig gegen 0, denn für jedes $x \in \mathbb{R}$ gilt $\lim_k \frac{x^k}{k!} = 0$ ($\to$ ÜA)

Sei $F_p(t) = \sum_{k=0}^{\infty} f_p^{(k)}(t) = f_p(t) + f_p'(t) + f_p''(t) + \ldots + f_p^{(n\cdot p+p-1)}(t)$

↑ endliche Summe

Es gilt $\frac{d}{dt}\left(\exp(-t)\,F_p(t)\right) = -\exp(-t)\,F_p(t) + \exp(-t)\,F_p'(t)$

$= \exp(-t)\left(F_p'(t) - F_p(t)\right) = -\exp(-t)\cdot f_p(t)$,

damit: $\int_0^j \exp(-t) f(t)\,dt = \underbrace{\exp(0)}_{=1} F_p(0) - \exp(-j) F_p(j)$

$\Rightarrow \underbrace{\exp(j)}_{e^j} \cdot \int_0^j \exp(-t) f(t)\,dt = e^j F_p(0) - F_p(j)$

Also

$$\sum_{j=0}^{n} a_j e^j \int_0^j \exp(-t) f(t)\,dt = \underbrace{\sum_{j=0}^{n} a_j e^j F(0)}_{=0} - \sum_{j=0}^{n} a_j F_p(j)$$

Mit Lemma §5.4 folgt nun für $j = 1, 2, \dots, n$

$$f_p^{(k)}(j) = \begin{cases} 0 & 0 \le k < p \\ \text{ganzzahliges Vielfaches von } p & k \ge p \end{cases}$$

$$f_p^{(k)}(0) = \begin{cases} 0 & 0 \le k < p-1 \\ (-1)(-2)\cdots(-n) & k = p-1 \\ \text{ganzzahliges Vielfaches von } p & k > p-1 \end{cases}$$

Es folgt $F_p(j) \in \mathbb{Z}$ für $j = 0, 1, \dots, n$

und $F_p(j) \equiv 0 \pmod p$ für $j = 1, \dots, n$

sowie $F_p(0) \equiv (-1)^n n! \pmod p$.

Folglich $\sum_{j=0}^{n} a_j F(j) \in \mathbb{Z}$ und $\sum_{j=0}^{n} a_j F(j) \equiv a_0 (-1)^n n! \pmod p$

Für $p \in \mathbb{P}$, $p > n$, $|a_0|$ und $a_0 \neq 0$ folgt

$$\sum_{j=0}^{n} a_j F(j) \neq 0 .$$

Andernfalls gilt

$$\lim_{p \in \mathbb{P}} \sum_{j=0}^{n} a_j e^j \int_0^j \exp(-t) f_p(t)\, dt = 0 ,$$

da die Funktion folge $(f_p)_{p \in \mathbb{P}}$ auf dem Intervall $[0,n]$ gleichmäßig gegen 0 konvergiert.

Das ist ein Widerspruch. □ #

Unser nächstes Ziel ist es, die Transzendenz der Kreiszahl $\pi \approx 3.14159\ldots$ zu zeigen. Dafür brauchen wir ein Hilfsmittel aus der Kombinatorik. Wir betrachten dazu Polynome in mehreren Variablen $X_1, X_2, \ldots, X_n$

6. Def Ein Polynom $f(X_1, X_2, \ldots, X_n)$ in n Variablen $X_1, \ldots, X_n$ (mit Koeffizienten in einem kommutativen Ring R) heißt <u>symmetrisch</u>, wenn für <u>jede</u> Permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ gilt: $f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)})$

Beispiele

(a) Für $n=1$ (Polynom in einer Variable $X=X_1$) ist jedes Polynom symmetrisch

(b) $n=2$ $\quad X_1^2 + X_2^2 = X_2^2 + X_1^2$ ist symmetrisch, $X_1^3 + X_1X_2 + X_2^3$ ist symmetrisch, $X_1^2 + X_2 \neq X_2^2 + X_1$ ist nicht symmetrisch.

7. Def Betrachte das Polynom in $n+1$ Variablen $X_1, \dots, X_n, Z$,

$$(Z-X_1)(Z-X_2)(Z-X_3)\cdots(Z-X_n)$$

$$= Z^n - \sigma_1(X_1,\dots,X_n)Z^{n-1} + \sigma_2(X_1,\dots,X_n)Z^{n-2} \cdots + (-1)^n \sigma_n(X_1,\dots,X_n)$$

Die Polynome $\sigma_1, \dots, \sigma_n$ sind symmetrisch (in den Variablen $X_1,\dots,X_n$) und heißen elementarsymmetrische Polynome.

Beispiel $n=1$ $\quad Z-X_1 \rightsquigarrow \sigma_1 = X_1$

$n=2$

$$(z-x_1)(z-x_2) = z^2 - (x_1+x_2)z + x_1x_2$$

$$\sigma_1 = x_1 + x_2$$

$$\sigma_2 = x_1 x_2$$

$n=3$

$$(z-x_1)(z-x_2)(z-x_3) = z^3 - (x_1+x_2+x_3)z^2 + (x_1x_2 + x_2x_3 + x_3x_1)z - x_1x_2x_3$$

$$\sigma_1 = x_1 + x_2 + x_3$$

$$\sigma_2 = x_1x_2 + x_2x_3 + x_3x_1$$

$$\sigma_3 = x_1 x_2 x_3$$

Allgemein gilt immer: $\sigma_1 = x_1 + x_2 \cdots + x_n$

$$\sigma_2 = \sum_{i<j} x_i \cdot x_j$$

$$\sigma_k = \sum_{i_1<\cdots<i_k} x_{i_1} \cdots x_{i_k}$$

$$\sigma_n = x_1 \cdot x_2 \cdots x_n$$

Beobachte: Ist $g(y_1, \ldots, y_n)$ ein Polynom in Variablen $y_1, \ldots, y_n$, so ist

$g(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ein <u>symmetrisches</u> Polynom in Variablen $x_1, \ldots, x_n$.

8. Lemma (Newton) Sei R ein kommutativer Ring (etwa $R=\mathbb{Z}$ oder $R=\mathbb{Q}$). Sei $f(X_1,\dots,X_n)$ ein symmetrisches Polynom in n Variablen $X_1,\dots,X_n$ mit Koeffizienten in R. Dann gibt es ein Polynom $h(X_1,\dots,X_n)$ mit Koeffizienten in R (nicht unbedingt symmetrisch) mit

$$h(\sigma_1,\dots,\sigma_n) = f(X_1,\dots,X_n)$$

Beweis Wir sortieren (ordnen) die Monome $X_1^{l_1}X_2^{l_2}\cdots X_n^{l_n}$ in f so, dass stets $X_1^{l_1}\cdots X_n^{l_n}$ links steht von $X_1^{m_1}X_2^{m_2}\cdots X_n^{m_n}$, wenn gilt $l_1=m_1,\dots,l_{j-1}=m_{j-1}$, $l_j > m_{j+1}$.

Für den Anfangsterm von f gilt dann

$$f = a X_1^{l_1}\cdots X_n^{l_n} + \dots \qquad a\in R,\ a\neq 0$$

$$l_1 \geq l_2 \geq \dots \geq l_n$$

Betrachte nun das Polynom

$$g_1 = a\,\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n}$$

Wir gilt $\sigma_k = X_1 \cdots X_k + \ldots$ (mit Term)

$\Rightarrow \sigma_k^{\wedge} = X_1^{\wedge} \cdots X_k^{\wedge} + \ldots$ (mit Term)

in die Konstante, damit

$$g_1 = a X_1^{l_1} \cdots X_n^{l_n} + (\text{mit Terme})$$

Betrachte $f_1 = f - g_1$. Da f, g_1 symmetrisch sind, ist auch f_1 symmetrisch. Der Aufspalten von f_1 ist nach einem Analysekonstruktion echt kleiner geworden. Fahre mit f_1 fort wie oben usw. nach endlich vielen Schritten $f_1 - g_2 = f_2, \ldots$

$$f_r - g_{r+2} = 0$$

$$f = f_1 + g_1 = f_2 + g_2 + g_1 = f_3 + g_3 + g_2 + g_1$$

$$= \ldots = g_{r+2} + \ldots + g_1$$

□

<u>Beispiel</u> $n = 2$, $f = X_1^2 + X_2^2$

$$\sigma_1 = X_1 + X_2 \qquad \sigma_2 = X_1 \cdot X_2$$

$$g_1 = l_1 = 2 \quad l_2 = 0$$

$$g_1 = \sigma_1^{l_1} \sigma_2^{0} = (X_1 + X_2)^2 = X_1^2 + 2X_1X_2 + X_2^2$$

$$f_1 = f - g_1 = -2X_1X_2 \qquad l_1 = 1 \quad l_2 = 1$$

$$g_2 = -2\sigma_1^{1-1} \cdot \sigma_2^{1} = -2 \cdot X_1 \cdot X_2$$

$$f_2 = f_1 - g_2 = 0$$

$$f = g_1 + g_2 = \sigma_1^2 + 2\sigma_2 = X_1^2 + X_2^2 \qquad (\nu).$$

9. Ansatz: $\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!}$.

Nach Quotientkriterium konvergiert die Exponentialreihe für jede komplexe Zahl $z \in \mathbb{C}$, denn:

$$a_k = \frac{z^k}{k!} \Rightarrow \left|\frac{a_{k+1}}{a_k}\right| = \frac{k!}{(k+1)!}\left|\frac{z^{k+1}}{z^k}\right| = \frac{|z|}{k+1} < 1$$

für $k \geq |z|$

Sei $i = \sqrt{-1}$. Für $t \in \mathbb{R}$ gilt dann

$$\exp(it) = \sum_{k=0}^{\infty} \frac{1}{k!}(it)^k = \sum_{k=0}^{\infty} \frac{1}{(2k)!} t^{2k}(-1)^k$$

$$+ i \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} t^{2k+1} \cdot (-1)^k$$

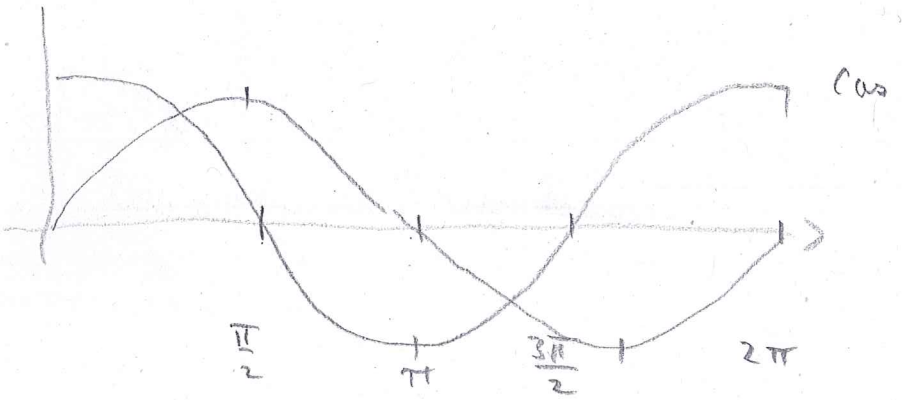
$$= \cos(t) + i \cdot \sin(t) \approx \left(1 - \tfrac{1}{2}x^2 + \ldots\right) + i\left(x - \tfrac{1}{6}x^3 + \ldots\right)$$

Damit erhalt wir Eulers Formel: Fur $t \in \mathbb{R}$ gilt

$$\exp(it) = \cos(t) + i \cdot \sin(t) \qquad i = \sqrt{-1}$$

und insbesondere

$$\exp(i\cdot\pi) = \cos(\pi) + i \cdot \sin(\pi) = -1$$



#

10. Lemma Wenn π algebraisch ist, so ist auch $i\pi$ algebraisch.

Beweis Angenommen, $0 = a_m \pi^m + \dots + a_0$ mit $a_0, \dots, a_m \in \mathbb{Q}$, $a_m \neq 0$, $m \geq 1$. Dann ist $i\pi$ Nullstelle des Polynoms

$$\underbrace{(a_m (iX)^m + a_{m-1}(iX)^{m-1} + \dots + a_0)}_{= h(X)} \underbrace{(a_m (-iX)^m + a_{m-1}\cdot(-iX)^{m-1} + \dots + a_0)}_{= \overline{h(X)}}$$

also $h(X) \cdot \bar{h}(X) \in \mathbb{Q}[X]$ $\rightsquigarrow$ $i\pi$ algebraisch. □

Erinnerung: Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen, d.h. jedes nicht-konstante Polynom in $\mathbb{C}[X]$ hat (mindestens) eine Nullstelle. Mit §4.4 folgt für $f = a_n X^n + \dots + a_0 \in \mathbb{C}[X]$, $n \geq 1$, $a_n \neq 0$, dass $f = a_n (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)$. Dabei ist $\{\lambda_1, \dots, \lambda_n\}$ die Menge der Nullstellen.

11. Theorem (von Lindemann 1882)

Die Kreiszahl $\pi \approx 3{,}14159\dots$ ist transzendent.

Beweis: Angenommen, π ist algebraisch. Dann ist auch $i\pi$ nach §5.10 algebraisch. Folglich gibt es ein Polynom $h_1 \in \mathbb{Q}[X]$ mit $h_1(i\pi) = 0$,

$$h_1 = X^n + a_{n-1} X^{n-1} + \dots + a_0 \qquad n \geq 1$$
$$a_0, \dots, a_{n-1} \in \mathbb{Q}.$$

$$= (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_n)$$

$\uparrow$ $\mathbb{C}$ alg. abg.

$$\lambda_1, \dots, \lambda_n \in \mathbb{C}$$

OE $\lambda_1 = i\pi$

$$\Rightarrow \sigma_k(\lambda_1, \dots, \lambda_n) = (-1)^k a_k \in \mathbb{Q} \qquad (1)$$

Da $\exp(\lambda_i) = -1$ gilt, folgt

$$(\exp(\lambda_1)+1)(\exp(\lambda_2)+1)\cdots(\exp(\lambda_n)+1) = 0$$

$$\exp(\lambda_1+\cdots+\lambda_n) + \cdots + \exp(\lambda_1)+\cdots+\exp(\lambda_n)+1 \quad (2)$$

Betrachte die Hilfsfunktion

$$h_1 = \prod_{j=1}^{n} (X-\lambda_j)$$

$$h_2 = \prod_{j<k} (X-(\lambda_j+\lambda_k))$$

$$h_3 = \prod_{j<k<\ell} (X-(\lambda_j+\lambda_k+\lambda_\ell))$$

$$\vdots$$

$$h_n = X-(\lambda_1+\lambda_2+\cdots+\lambda_n)$$

Die Koeffizienten der h_i Polynome sind symmetrisch in $\lambda_1,\ldots,\lambda_n$. Nach Newtons Lemma §5.4 kann sie sich durch die $\sigma_1(\lambda_1,\ldots,\lambda_n),\ldots$ $\sigma_n(\lambda_1,\ldots,\lambda_n)$ ausdrücken (über $\mathbb{Z}$). Mit (1) folgt: $h_1,\ldots,h_n \in \mathbb{Q}[X]$.

Wir setzen $h = h_1 \cdot h_2 \cdots h_n \in \mathbb{Q}[X]$

Es gibt $c_0, \dots, c_r \in \mathbb{Z}$ mit $c_0, c_r \neq 0$

und $h = \underbrace{\left(X^r + \frac{c_1}{c_0} X^{r-1} + \dots + \frac{c_r}{c_0}\right)}_{=H} \cdot X^{m-r}$

Was ist die Rolle von r? Das Polynom h_k

hat Nullstelle in 0 gdw $\rho_{j_1} + \dots + \rho_{j_k} = 0$

für gewisse $j_1 < j_2 < \dots < j_k$, also

$$X^r + \frac{c_1}{c_0} X^{r-1} + \dots + \underbrace{\frac{c_r}{c_0}}_{\neq 0} = (X - \rho_1) \cdots (X - \rho_r) \qquad \rho_j \neq 0$$

und (2) schließt sich an $\qquad \frac{c_k}{c_0} = \sigma_k(\rho_1, \dots, \rho_r)$

$$0 = \exp(\rho_1) + \exp(\rho_2) + \dots + \exp(\rho_r) + \underbrace{\exp(0)(m-r) + 1}_{= m-r+1 = K \neq 0} \qquad (2')$$

Sei nun $p \in \mathbb{P}$ Primzahl, setze

$$f_p = \frac{c_0^{r \cdot p}}{(p-1)!} X^{p-1} \underbrace{(X - \rho_1)^p \cdots (X - \rho_r)^p}_{= H^p}$$

$$F_p = f_p + f_p' + f_p'' + \dots$$

es folgt $\frac{d}{dt}\left(\exp(-t)\,F_p(t)\right) = -\exp(-t)\,f_p(t)$,

also $\exp(-t)F_p(t) - F_p(0) = -\int_0^t \exp(-y)\,f_p(y)\,dy$

$$\overset{y=tx}{=} -t\int_0^1 \exp(-tx)\,f_p(tx)\,dx \quad , \text{ damit}$$

$$F_p(t) - \exp(t)\,F_p(0) = -t\int_0^1 \exp(t(1-x))\,f_p(x)\,dx$$

Für t fest und $p \gg 1$ ist die rechte Seite beliebig nahe an 0, vgl. §5.5.

Es folgt

$$\sum_{j=1}^{r}\left(F_p(\rho_j) - \exp(\rho_j)\,F_p(0)\right) \overset{(2)'}{=} \sum_{j=1}^{r} F_p(\rho_j) + K\cdot F_p(0)$$

$$= \sum_{j=1}^{r} -\rho_j \int_0^1 \exp(\rho_j(1-x))\,F_p(\rho_j\cdot x)\,dx \qquad (3)$$

beliebig nahe an 0 für $p \gg 1$.

Andererseits gilt:

$$f_p^{(k)}(P_1) = 0 \qquad \text{für } 0 \le k < p.$$

Für $k \ge p$ ist $f_p^{(k)}(P_1)$ ein Produkt aus $p \cdot C_0^{rp}$ und einer ganzzahligen Polynom in $P_2, \dots, P_r$.

Folglich ist $\sum_{j=1}^{r} f_p^{(k)}(P_j)$ ein Produkt von $p \cdot C_0^{r \cdot p}$ und einer ganzen Zahl (mit Newtons Lemma und Vorbilder $\in C_0^{r \cdot p}$)

Es folgt $\sum_{j=1}^{r} F_p(P_j) \in p \cdot \mathbb{Z}$. (4)

Nun ist $f_p^{(k)}(0) = 0 \qquad \text{für } 0 \le k < p-1$

$$f_p^{(p-1)}(0) = C_0^{r \cdot p} \cdot (-P_1)^p \cdots (-P_r)^p$$

$$= C_0^{r \cdot p} (-1)^{rp} (P_1 \cdots P_r)^p$$

$$= C_0^{r \cdot p} (-1)^{r \cdot p} \left(\frac{C_r}{C_0}\right)^p = C_0^{(r-1)p} (-1)^{r \cdot p} C_r^p$$

$$f_p^{(k)}(0) \in p\mathbb{Z} \qquad \text{für } k \ge p$$

Es folgt $F_p(0) \cdot K \equiv K \cdot C_0^{(r-1)p} (-1)^{r \cdot p} C_r^p$

$$\not\equiv 0 \pmod{p}$$

wenn $p > |K|, |C_0|, |C_r|$ ↯ □

#

Wir betrachten zum Abschluss noch die

Unmöglichkeit der Quadratur des Kreises.

Beobachtung: Der Körper der komplexen Zahlen $\mathbb{C}$ ist ein (unendlich-dimensionaler) $\mathbb{Q}$-Vektorraum:

- $(\mathbb{C},+)$ ist eine abelsche Gruppe
- $(\mathbb{Q},+,\cdot)$ ist Körper
- für $a,b\in\mathbb{Q}$, $u,v\in\mathbb{C}$ gilt $(a+b)(u+v)=au+bu+av+bv$, $(ab)u=a(bu)$ und $1\cdot u=u$

12. Lemma Sei $z\in\mathbb{C}$. Dann sind äquivalent:

(i) z ist algebraisch

(iii) es gibt einen endlich-dimensionalen $\mathbb{Q}$-Vektorraum $V\subseteq\mathbb{C}$ mit $1\in V$ und $z\cdot V=\{z\cdot v \mid v\in V\}\subseteq V$.

Beweis (i)$\Rightarrow$(ii) Angenommen, es gibt $a_0,\dots,a_{n-1}\in\mathbb{Q}$ mit $z^n+a_{n-1}z^{n-1}+\dots+a_0=0$, $n\geq 1$. (*)

Sei V die $\mathbb{Q}$-Aufspann von $\{1,z,z^2,z^3,\dots,z^{n-1}\}$.

Es folgt $z^n\in V$ wegen (*) und für $0\leq k<n$ $z\cdot z^k\in V$

$\Rightarrow z\cdot V\subseteq V$ und $1\in V$.

(ii)$\Rightarrow$(i) Sei V wie in (ii), mit Basis $1=u_1,\dots,u_m\in\mathbb{C}$. Angenommen, $z\cdot V\subseteq V$.

Dann gibt es Zahlen $a_{jk} \in \mathbb{Q}$ mit

$$z \cdot u_j = \sum_{k=1}^{n} a_{jk} \cdot u_k \quad , \quad j = 1, \dots, n.$$

Sei $A = (a_{jk})_{j,k=1}^{n}$ die Matrix der (a_{ij}). Es folgt, dass z Eigenwert der Matrix A ist. Folglich ist z Nullstelle des charakteristischen Polynoms $\chi_A = \det(A - \mathbb{1} \cdot X) \in \mathbb{Q}[X]$ und z ist algebraisch. □

13. Satz Sei $K \subseteq \mathbb{C}$ die Menge aller algebraischen Zahlen. Dann ist K ein algebraisch abgeschlossener Körper.

Beweis in mehreren Schritten.

(a) K ist Ring. Sei $z_1, z_2 \in K$. Nach §5.12 gibt es endlich dimensionale $\mathbb{Q}$-Vektorräume $V_1, V_2 \subseteq \mathbb{C}$ mit $1 \in V_1, V_2$ und $z_1 V_1 \subseteq V_1$, $z_2 V_2 \subseteq V_2$. Sei $1 = u_1, \dots, u_n$ Basis von V_1 und $1 = v_1, \dots, v_m$ Basis von V_2, sei $W \subseteq \mathbb{C}$ der $\mathbb{Q}$-Aufspann von $\{ u_j v_k \mid 1 \le j \le n, \ 1 \le k \le m \}$. Es folgt $z_1 W \subseteq W$, $z_2 W \subseteq W$ $\Rightarrow (z_1 \pm z_2) W \subseteq W$ und $(z_1 \cdot z_1) W \subseteq W \Rightarrow z_1 \pm z_2, z_1 \cdot z_2 \in K$. Klar: $1 \in K$ $\Rightarrow (K, +, \cdot)$ ist Teilring von $(\mathbb{C}, +, \cdot)$

(b) $\mathbb{K}$ ist Körper Sei $z \in \mathbb{K}$, $z \neq 0$.

Sei $V \subseteq \mathbb{C}$ $\mathbb{Q}$-Vektorraum mit $1 \in V$, $zV \subseteq V$.
Da $z \neq 0$ ist die Abbildung $V \to V$, $v \mapsto zv$ injektiv,
also bijektiv, weil $\dim(V) < \infty$ (Dimensionsformel),
d.h. $z \cdot V = V$. Es folgt $V = \frac{1}{z} \cdot V \Rightarrow \frac{1}{z} \in \mathbb{K}$.

(c) Ist $b_1, \dots, b_m \in \mathbb{K}$, so gibt es ein $\mathbb{Q}$-Vektorraum
$V \subseteq \mathbb{C}$ endlicher Dimension, mit $1 \in V$ und
$b_j V \subseteq V$ für alle $j = 1, \dots, m$.

Denn: es gibt $V_1, \dots, V_m$ mit $b_j V_j \subseteq V_j$, $1 \in V_j$,
V_j endlich-dim. $\mathbb{Q}$-Vektorraum. Sei V der Aufspann der
m-fachen Produkte der Basisvektoren der V_j.

(d) Der Körper $\mathbb{K}$ ist algebraisch abgeschlossen

Sei $f = X^n + a_{n-1} X^{n-1} + \dots + a_0$, $n \geq 1$
$a_0, \dots, a_{n-1} \in \mathbb{K}$

Zu zeigen: f hat Nullstelle in $\mathbb{K}$. Sei $z \in \mathbb{C}$
eine Nullstelle von f ($\mathbb{C}$ ist algebraisch abg.!)
Sei $V \subseteq \mathbb{C}$ endlich dimensionaler $\mathbb{Q}$-Vektorraum
mit $a_j V \subseteq V$ für $j = 0, \dots, n-1$ und $1 \in V$.
Sei $u_1, \dots, u_m$ Basis von V. Betrachte den
Vektor $(u_j z^h \mid 1 \leq j \leq m, 0 \leq h < n)$

(1) - Vektorraum W. Es gilt $z^n = -a_{n-1} z^{n-1} \dots - a_0 \in W$

$\Rightarrow$ $u_j z^n = -u_j^{n-1} \cdot (a_{n-1} z^{n-1} + \dots + a_0) \in W$

$\Rightarrow$ $zW \subseteq W$ und $1 \in W \Rightarrow z \in K$. $\square$

14. Theorem Die Quadratur des Kreises ist unmöglich, d.h. es ist nicht möglich, mit Zirkel und Lineal, ausgehend von den Punkten $(0,0) \in \mathbb{R}^2$ und $(1,0) \in \mathbb{R}^2$, eine Strecke der Länge π zu konstruieren.

Beweis: Wir identifizieren die Ebene $\mathbb{R}^2$ mit $\mathbb{C}$.

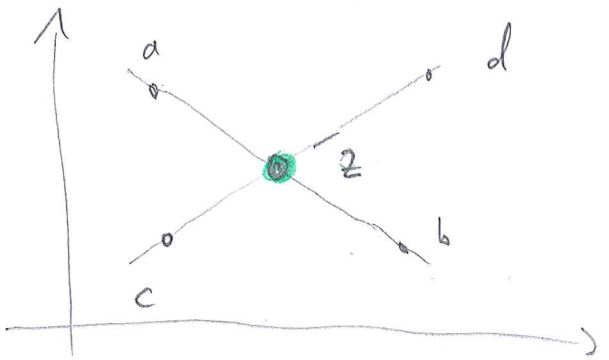
Behauptung: Alle Punkte in der Ebene, die wir mit Zirkel und Lineal konstruieren, sind in der Menge $K \subseteq \mathbb{C} \cong \mathbb{R}^2$ enthalten.

Da nach von Lindemanns Theorem §5.11 gilt $\pi \notin K$, folgt dann die Behauptung des Theorems.

Wann erhalten wir neue Punkte in K? Es gibt drei Sorten von Punkten, die man mit Zirkel und Lineal konstruieren kann.

Schnitt zwei Gerade

(1) Punkte $a, b, c, d \in \mathbb{K}$



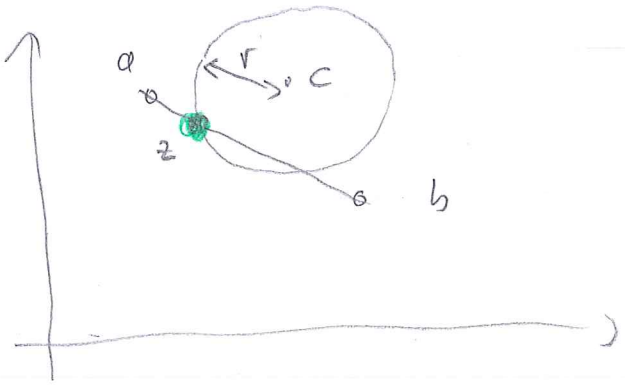
z Schnittpkt der Gerade $\overline{ab}$, $\overline{cd}$

$z = s(a + (1-s)b$
$= t \cdot b + (1-t)d$

LGS. Wenn $a, b, c, d \in \mathbb{K}$, dann $z \in \mathbb{K}$, weil $\mathbb{K}$ Körper
s.t

Schnitt von Kreis und Gerade
Punkte a, b, c, Radius r

(2)



$z = s \cdot a + (1-s) \cdot b$

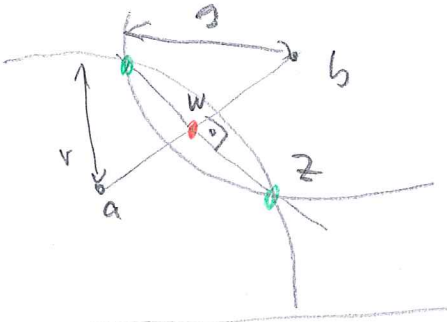
$|z-c|^2 = r^2$

quadratische Gleichung für s

Da $\mathbb{K}$ algs. abg. folgt $s \in \mathbb{K}$, wenn $r, a, b, c \in \mathbb{K} \Rightarrow z \in \mathbb{K}$

Schnitt zweier Kreise
Punkte $a, b \in$, Radien r, s

(3)



$w = t \cdot a + (1-t) b$

$s^2 = |b-w|^2 + |w-z|^2$

$r^2 = |a-w|^2 + |w-z|^2$

$\Rightarrow t \in \mathbb{K} \Rightarrow z \in \mathbb{K}$

Wieder quadratische Gleichung; wenn $a, b, r, s \in \mathbb{K}$, dann auch $z \in \mathbb{K}$.

□

Bemerkung Sei $\mathcal{C} \subseteq \mathbb{C}$ die Menge aller mit Zirkel und Lineal konstruierbaren Punkte. Dann gilt:

(a) $\mathbb{Q} \subseteq \mathcal{C}$, $\sqrt{2} \in \mathcal{C}$

(b) $\mathcal{C}$ ist Körper

(c) $\mathcal{C} \subsetneq \mathbb{K}$ ($\rightarrow$ Algebra: Galois-Theorie!)