§ 6 Die Transzendenz von e und π

1. Def Eine komplexe Zahl $z \in \mathbb{C}$ heißt algebraisch, wenn es ein Polynom $f \in \mathbb{Q}[T]$ gibt mit $\deg(f) \geq 1$ und $f(z) = 0$ gilt.

Bsp • Jede rationale Zahl $q \in \mathbb{Q}$ ist algebraisch, denn q ist Nullstelle von $f = T - q \in \mathbb{Q}[T]$

• $\sqrt{2}$ ist nicht rational, aber algebraisch, denn $\sqrt{2}$ ist Nullstelle von $g = T^2 - 2 \in \mathbb{Q}[T]$

⌐ Wäre $\sqrt{2} = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $b \neq 0$, so setze $d = ggT(a,b)$, $a = a' \cdot d$, $b = b' \cdot d \Rightarrow$
$\sqrt{2} = \frac{a'}{b'}$ und $ggT(a', b') = 1$

$\Rightarrow (a')^2 = 2 \cdot (b')^2$. Es folgt $2 \mid (a')^2$

$\underset{\S 1.13}{\Rightarrow} 2 \mid a'$, $a' = 2^l \cdot \tilde{a}$ $\quad \tilde{a}$ ungerade, $l \geq 1$.

Da $ggT(a', b') = 1$ ist b' ungerade, also

$$2^{2l} \cdot \tilde{a}^2 = 2 \cdot b'^2 \Rightarrow b'^2 = 2^{2l-1} \cdot \tilde{a}^2$$

$$\Rightarrow 2 \mid b'^2 \underset{\S 1.13}{\Rightarrow} 2 \mid b' \quad ⚡$$

⌟

2. Def Sei $A \subseteq \mathbb{C}$ die Menge aller algebraischen Zahlen. Eine komplexe (oder reelle) Zahl $z \in \mathbb{C}$ heißt transzendent, falls z nicht algebraisch ist, $z \in \mathbb{C} - A$.

Heuristische Überlegung: $\mathbb{Q}$ ist abzählbar, jedes Polynom $F \in \mathbb{Q}[T]$ hat endlich viele Koeffizienten $\Rightarrow \mathbb{Q}[T]$ ist auch abzählbar. Jedes Polynom $f \in \mathbb{Q}[T]$ mit $f \neq 0$ hat höchstens $\deg(f)$ verschiedene Nullstellen $\Rightarrow A$ ist abzählbar. Da $\mathbb{C}$ und $\mathbb{R}$ nicht abzählbar sind, ist "fast jede" reelle oder komplexe Zahl transzendent.

3. Erinnerung: partielle Integration (= Produktregel rückwärts) $\int_u^v (f \cdot g)' = f \cdot g \Big|_u^v = \int_u^v f \cdot g' + \int_u^v f' \cdot g$

Falls $f(u) = f(v) = 0$ also $\int_u^v f \cdot g' = \int_u^v f' \cdot g$ (*)

(Lambert 1761)

4. Theorem Die Zahl π ist irrational.

Beweis Sei $\alpha \in \mathbb{R}$ fest. Wir setzen

$$I_n = \int_{-1}^{1} (1-x^2)^n \cos(\alpha x)\, dx$$

Es folgt $I_0 = \int_{-1}^{1} \cos(\alpha x)\, dx = \frac{1}{\alpha} \sin(\alpha x) \Big|_{-1}^{1} = \frac{2}{\alpha} \sin(\alpha)$,

$$I_1 = \int_{-1}^{1} (1-x^2) \cos(\alpha x)\, dx \overset{(*)}{=} - \int_{-1}^{1} (-2x) \frac{1}{\alpha} \sin(\alpha x) dx = \frac{2}{\alpha} \int_{-1}^{1} x \cdot \sin(\alpha x)\, dx$$

$$\overset{(*)}{=} \frac{2}{\alpha^2} \int_{-1}^{1} \cos(\alpha x) dx - \frac{2}{\alpha^2} x \cdot \cos(\alpha x) \Big|_{-1}^{1}$$

$$= \frac{4}{\alpha^3} \sin(\alpha) - \frac{4}{\alpha^2} \cos(\alpha)$$

Für $n \geq 2$: $I_n = \int_{-1}^{1} (1-x^2)^n \cos(\alpha x\, dx) \overset{(*)}{=} - \int_{-1}^{1} n(1-x^2)^{n-1} (-2x) \frac{1}{\alpha} \sin(\alpha x) dx$

$$= \frac{2n}{\alpha} \int_{-1}^{1} x (1-x^2)^{n-1} \sin(\alpha x)\, dx$$

$$\overset{(*)}{=} \frac{-2n}{\alpha} \int_{-1}^{1} \left((1-x^2)^{n-1} + x(n-1)(1-x^2)^{n-2}(-2x) \right) \frac{-1}{\alpha} \cos(\alpha x)\, dx$$

$$= \frac{2n}{\alpha^2} \int_{-1}^{1} \left((1-x^2)^{n-1} - 2(n-1)\, x^2 (1-x^2)^{n-2} \right) \cos(\alpha x)\, dx$$

$$= \frac{2n}{\alpha^2} \int_{-1}^{1} 2(n-1)(1-x^2)^{n-1} \cos(\alpha x)\, dx$$

$$+ \frac{2n}{\alpha^2} \int_{-1}^{1} \left((1-x^2)^{n-1} - 2(n-1)(1-x^2)^{n-2} \right) \cos(\alpha x) dx$$

$$= \frac{1}{\alpha^2} 2n(2n-1)\, I_{n-1} - \frac{1}{\alpha^2} 4n(n-1)\, I_{n-2}$$

Mit Induktion folgt daraus

$$I_n = \frac{n!}{\alpha^{2n+1}} \left(f_n(\alpha) \cdot \sin(\alpha) + g_n(\alpha) \cos(\alpha) \right)$$

mit Polynomen $f_n, g_n \in \mathbb{Z}[T]$ und

$\deg(f_n), \deg(g_n) \leq 2n+1$

Angenommen, $\pi \in \mathbb{Q}$. Dann gibt es $a, b \in \mathbb{Z}$, $a, b > 0$ mit $\frac{\pi}{2} = \frac{a}{b}$. Es folgt mit $\alpha = \frac{\pi}{2}$ für jedes $n \geq 0$

$$\frac{1}{n!} \frac{a^{2n+1}}{b^{2n+1}} I_n = f_n\left(\frac{a}{b}\right) \underbrace{\sin\left(\frac{\pi}{2}\right)}_{=1} \qquad \Big| \cdot b^{n+1}$$

$$\frac{1}{n!} a^{2n+1} I_n = \underline{f_n\left(\frac{a}{b}\right) \cdot b^{n+1}} \in \mathbb{Z}$$

Es gilt weiter $|I_n| \leq 4$, also wegen $\lim_{n \to \infty} \frac{a^{2n+1}}{n!} = 0$

$f_n\left(\frac{a}{b}\right) b^{n+1} = 0$ für $n \gg 0$. Andererseits ist $|I_n| > 0$, da der Integrand im Bereich $[-1, 1]$ fast überall positiv ist.

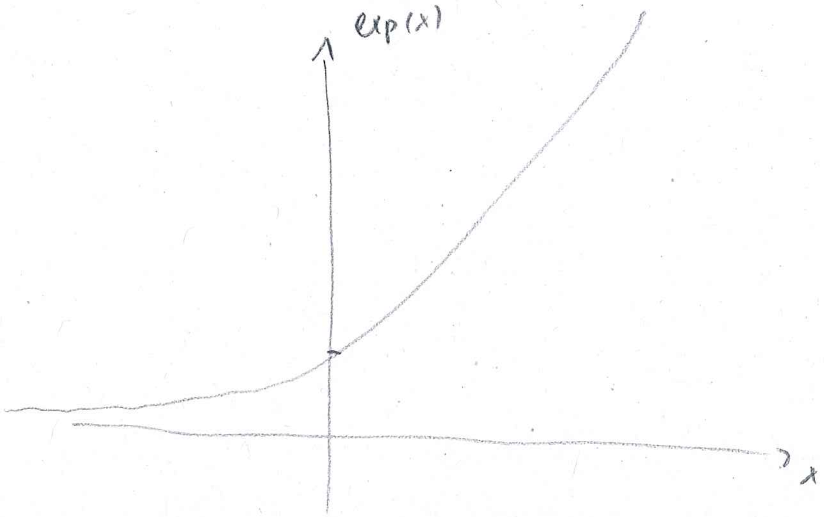
$\lightning$

$\square$

5. <u>Erinnerung</u> Die <u>Exponentialfunktion</u> ist gegeben durch

$$\exp(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} \qquad \text{(für } z \text{ reell oder komplex)}$$

Es gilt $\exp(0) = 1$, $\exp(u+v) = \exp(u) \cdot \exp(v)$ und $\exp' = \exp$



Die Eulersche Zahl ist $e = \exp(1) = 2.71\ldots$

6. Lemma Sei $h: \mathbb{R} \to \mathbb{R}$ unendlich oft diffbar. Sei $l \geq 0$ und sei $f(x) = (x-\lambda)^l h(x)$. Dann gilt

$$f^{(k)}(\lambda) = \begin{cases} 0 & 0 \leq k < l \\ \frac{k!}{(k-l)!} h^{(k-l)}(\lambda) & k \geq l \end{cases}$$

Beweis Mit Taylor-Reihe um λ

$$Tf = \sum_{j=0}^{\infty} \frac{1}{j!} f^{(j)}(\lambda)(x-\lambda)^j \qquad Th = \sum_{k=0}^{\infty} \frac{1}{k!} h^{(k)}(x-\lambda)^k$$

$$\Rightarrow Tf = \sum_{k=0}^{\infty} \frac{1}{k!} h^{(k)} (x-\lambda)^{k+l}$$ jetzt Koeffizienten vergleich. $\square$

7. Theorem (Hermite 1879) Die Euler'sche Zahl $e = \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} \approx 2.71\ldots$ ist transzendent.

Beweis Angenommen, e wäre algebraisch. Dann gibt es $a_0, \ldots, a_m \in \mathbb{Q}$ mit $a_m \neq 0$ und $m \geq 1$ und

$$0 = a_m e^m + a_{m-1} e^{m-1} + \ldots + a_0$$

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

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

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

Setze $f = f_p = \frac{1}{(p-1)!} T^{p-1}(T-1)^p(T-2)^p \cdots (T-m)^p$

Es folgt für $0 \leq x \leq m$, dass $|f_p(x)| \leq \frac{1}{(p-1)!} m^{p-1} m^{m \cdot p}$

$\leq \frac{1}{(p-1)!} (m^{m+1})^p$, also konvergiert die Funktionfolge $(f_p)_{p \in \mathbb{P}}$ auf $[0, m]$ gleichmäßig gegen Null.

Sei $F(x) = \sum_{k=0}^{\infty} f^{(k)}(x) = f(x) + f'(x) + f''(x) + \ldots + f^{(mp+p-1)}(x) + 0$

Es gilt $\frac{d}{dx}\Big(\exp(-x) F(x)\Big) = -\exp(-x)F(x) + \exp(-x)F'(x)$

$= \exp(-x)\big(F'(x) - F(x)\big) = -\exp(-x) \cdot f(x)$, also

$$\int_0^j \exp(-x) f(x)\, dx = \underbrace{\exp(-0)}_{=1} F(0) - \exp(-j) F(j)$$

$$\Rightarrow \exp(j) \int_0^j \exp(-x) f(x)\, dx = e^j \cdot F(0) - F(j)$$

$$\sum_{j=0}^{m} a_j \cdot e^j \int_0^j \exp(-x) \cdot f(x)\, dx = \underbrace{\sum_{j=0}^{m} a_j e^j F(0)}_{=0} - \sum_{j=0}^{m} a_j F(j)$$

Mit Lemma §6.6 folgt für $j = 1, 2, \ldots, m$, dass

$$F^{(k)}(j) = \begin{cases} 0 & 0 \leq k < p \\ \text{ganzzahliges Vielfaches von } p & k \geq p \end{cases}$$

$$f^{(k)}(0) = \begin{cases} 0 & 0 \leq k < p-1 \\ (-1)(-2)(-3)\cdots(-m) & k = p-1 \\ \text{ganzzahliges Vielfaches von } p & k \geq p \end{cases}$$

Also $F(j) \in \mathbb{Z}$ für $j = 0, 1, \ldots m$ und

$F(j) \equiv 0 \pmod p$ für $j = 1, 2, \ldots m$

$F(0) \equiv (-1)^m m! \pmod p$

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

Für $p > m, |a_0|$ (und $a_0 \neq 0$) folgt $\sum_{j=0}^{m} a_j F(j) \in \mathbb{Z} - \{0\}$

Andererseits gilt

$$\lim_{p \in \mathbb{P}} \sum_{j=0}^{m} a_j e^j \int_0^j \exp(-x) f_p(x)\,dx = 0,$$ da die f_p

gleichmäßig gegen Null konvergieren – ein

Widerspruch.

$\square$

9. <u>Def</u> Ein Polynom $f(u_1, \dots, u_n)$ in n Variablen $u_1, \dots, u_n$ heißt <u>symmetrisch</u>, wenn für jede Permutation g der Indizes $\{1, \dots, n\}$ gilt $f(u_1, \dots, u_n) = f(u_{g(1)}, \dots, u_{g(n)})$

<u>Bsp</u> $n = 1$: Jedes Polynom in einer Variable ist symmetrisch

$n=2$: $u_1^3 + u_2^3$ ist symmetrisch

$u_1 u_2^2 + u_2^2$ ist nicht symmetrisch

$\neq u_2 u_1^2 + u_1^2$

Betrachte

$$(T-u_1) \cdots (T-u_n) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} \dots + (-1)^n \sigma_n$$

$$\sigma_1 = u_1 + u_2 + \dots + u_n$$

$$\sigma_2 = u_1 + u_2 + u_2 \cdot u_3 + \dots = \prod_{i<j} u_i u_j$$

$$\vdots$$

$$\sigma_n = u_1 \cdot u_2 \cdots u_n$$

Diese n Polynome heißen <u>elementare symmetrische Polynome</u>. Ist $g(u_1, \dots, u_n)$ ein beliebiges Polynom, so ist $g(\sigma_1, \dots, \sigma_n)$ symmetrisch. #

10. <u>Lemma (Newton)</u> Sei R ein kommutativer Ring (etwa $R=\mathbb{Z}$), sei $f(u_1,\dots,u_n)$ ein symmetrisches Polynom mit Koeffizienten in R. Dann gibt es ein Polynom $h(u_1,\dots,u_n)$ mit Koeffizienten in R so, dass $h(\sigma_1,\dots,\sigma_n)=f(u_1,\dots,u_n)$.

<u>Beweis</u> Wir ordnen die Monome in f

$a\, u_1^{l_1}\cdots u_n^{l_n}$ so, dass stets

$u_1^{l_1}\cdots u_n^{l_n}$ links von $u_1^{m_1}\cdots u_n^{m_n}$ steht genau dann, wenn $l_1=m_1,\ l_2=m_2,\dots,\ l_j>m_j$.

Da f symmetrisch ist, gilt für den Term ganz links

$$l_1\geq l_2\geq\dots\geq l_n\ ,\quad f=a\cdot u_1^{l_1}u_2^{l_2}\cdots u_n^{l_n}+\dots$$

Im Polynom

$$p_1=a\cdot\sigma_1^{l_1-l_2}\sigma_2^{l_2-l_3}\cdots\sigma_n^{l_n}$$ steht am Anfang der gleiche Term. Betrachte $f_1=f-p_1$ und schaffe davon den ersten Term weg, usw. Das Verfahren terminiert nach endlich vielen Schritten, da $\deg(p_1)\leq\deg(f)$ und $\deg(f_1)\leq\deg(f)$ $\square$

Bsp $n=2$ $f = u_1^2 + u_2^2$ $\sigma_1 = u_1 + u_2$, $\sigma_2 = u_1 \cdot u_2$

$\rightsquigarrow p_1 = \sigma_1^2 \cdot \sigma_2^0 = u_1^2 + 2u_1u_2 + u_2^2$

$f_1 = -2u_1u_2$ $p_2 = -2\sigma_1^{1-1}\sigma_2^1 = -2u_1u_2$

$f_2 = f_1 - p_2 = 0$ $\rightsquigarrow f = p_1 + p_2 = \sigma_1^2 - 2\sigma_2$

11. Erinnerung: Für $i = \sqrt{-1} \in \mathbb{C}$ und $t \in \mathbb{R}$ gilt

Eulers Formel

$$\exp(it) = \cos(t) + i \cdot \sin(t)$$

insbesondere gilt $\exp(i\pi) = -1$

12. Theorem (von Lindemann 1882)

Die Zahlen π und $i\pi$ sind transzendent.

Beweis Angenommen, π ist algebraisch;

$a_m\pi^m + \ldots + a_0 = 0$ $a_j \in \mathbb{Q}$, $m \geq 1$, $a_m \neq 1$.

Dann ist $i\pi$ Nullstelle des Polynoms

$(a_m(iT)^m + \ldots + a_0)(a_m(-iT)^m + \ldots + a_0) \in \mathbb{Q}[T]$,

also ist auch $i\pi$ algebraisch.

Folglich reicht es zu zeigen, dass $i\pi$ nicht algebraisch ist. Wir nehmen an, $i\pi$ wäre algebraisch und führen das zu einem Widerspruch.

Dann gibt es ein Polynom $h_1 \in \mathbb{Q}[T]$ mit $\deg(h_1) \geq 1$ und $h_1(i\pi) = 0$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, gibt es $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ mit

$$h_1 = (T-\lambda_1)(T-\lambda_2)\cdots(T-\lambda_n) \qquad \text{OE } \lambda_1 = i\pi$$

$$= T^n + a_{n-1}T^{n-1} + \ldots + a_0 \qquad a_j \in \mathbb{Q}$$

$$= T^n - \sigma_1(\lambda_1, \ldots, \lambda_n)T^{n-1} + \ldots + (-1)^n \sigma_n(\lambda_1, \ldots, \lambda_n)$$

d.h. die elementarsymmetrischen Polynome in den λ_i sind rationale Zahlen.

Weiter gilt $\exp(i\pi) = -1$, also

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

$\|$ (ausmultiplizieren)

$$\exp(\lambda_1 + \ldots + \lambda_n) + \quad \ldots \quad + \sum_{j<k} \exp(\lambda_j + \lambda_k) + \sum_j \exp(\lambda_j) + 1$$

Betrachte nun die Polynome

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

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

$$\vdots$$

$$h_n = T - \underbrace{(\lambda_1 + \ldots + \lambda_n)}_{\sigma_1(\lambda_1, \ldots, \lambda_n)}$$

Jedes dieser n Polynome ist symmetrisch in den λ_i, λ_j. Da $\sigma_1(\lambda_1, \ldots, \lambda_n), \ldots, \sigma_n(\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}$ gilt, folgt mit Newtons Lemma §6.10, dass $h_1, \ldots, h_n \in \mathbb{Q}[T]$. Sei $h = h_1 \cdots h_n$. Multiplizieren mit dem Hauptnenner c_0 der Koeffizienten

$\Rightarrow$ $c_0 \cdot h \in \mathbb{Z}[T]$ und die Nullstellen dieses Polynoms sind genau die Exponenten in $(*)$

Schreibe $c_0 \cdot h = c_0 T^N + \ldots + c_r T^{N-r}$

$$c_j \in \mathbb{Z}, \quad c_0, c_r \neq 0$$

$$= g \cdot T^{N-r}$$

$g \in \mathbb{Z}[T]$ $\deg(g) = r \geq 1$ und $g(0) \neq 0$

$g = c_0 T^r + \ldots + c_r$

Damit schreibt sich (*) als

(**)

$$\exp(\beta_1)+\dots+\exp(\beta_r)+\underbrace{\exp(0)\cdots+\exp(0)+1}_{=K\geq 1}=0$$

$$c_0(T-\beta_1)(T-\beta_2)\cdots(T-\beta_r)=g\in\mathbb{Q}[T].$$

Jetzt ähnlich wie in §6.7 weitermachen: $p\in\mathbb{P}$

$$f=f_p=c_0^{s}\cdot T^{p-1}\cdot\frac{1}{(p-1)!}(T-\beta_1)^p\cdots(T-\beta_r)^p$$

$$F=F_p=f+f'+f''+\dots \qquad s=r\cdot p-1$$

$$\frac{d}{dx}\big(\exp(-x)F(x)\big)=\exp(-x)\big(-F(x)+F'(x)\big)=-\exp(-x)\cdot f(x)$$

$$\rightsquigarrow\quad \exp(-x)F(x)-F(0)=-\int_0^x \exp(-y)f(y)\,dy$$

$$(y=t\cdot x\quad dy=dt\cdot x)\qquad =-x\int_0^1 \exp(-tx)f(tx)\,dt$$

$$\rightsquigarrow\quad F(x)-\exp(x)\cdot F(0)=-x\int_0^1 \exp(1-tx)f(tx)\,dt$$

Diese Integrale hängen von $p\in\mathbb{P}$ ab, für $p\rightsquigarrow\infty$ und festes x konvergiert der Ausdruck gegen Null.

Betrachte nun

(**)

$$\sum_{j=1}^{r} F(\beta_j) - \exp(\beta_j)\cdot F(0) = \sum_{j=1}^{r} F(\beta_j) + \underbrace{K}_{K\geq 1}\cdot F(0)$$

$$= \underbrace{-\sum_{j=1}^{r} \beta_j \int_0^1 \exp(1-\beta_j\cdot t)\, F(t\beta_j)\, dt}$$

konvergiert gegen Null für $p\in\mathbb{P}$, $p\to\infty$

Es gilt $F^{(k)}(\beta_1) = 0$ für $0\leq k \leq p$

Für $k\geq p$ ist $F^{(k)}(\beta_1)$ ein Produkt aus

$p\cdot c_0^{s}$ und ein ganzzahlig Polynom in den β_j

vom Grad $\leq r\cdot p-1$.

Folglich ist $\sum_{j=1}^{r} F^{(k)}(\beta_j)$ ein Produkt aus

$p\cdot c_0^{s}$ und ein symmetrisch ganzzahlig Polynom in den β_j.

Seien $\tilde{\sigma}_1,\ldots,\tilde{\sigma}_r$ die elementar symmetrischen Polynome in

r Variablen $\Rightarrow$

$$(T-\beta_1)\cdots(T-\beta_r) = T^r - \tilde{\sigma}_1(\beta_1)T^{r-1}\cdots + (-1)^r\tilde{\sigma}_r(\beta_1\ldots\beta_r)$$

$$= T^r - \frac{c_1}{c_0}T^{r-1}\cdots + (-1)^r\frac{c_r}{c_0}$$

$$\Rightarrow \sum_{j=1}^{r} F^{(k)}(\beta_j) \in p\cdot\mathbb{Z} \Rightarrow \sum_{j=1}^{r} F(\beta_j) \in p\cdot\mathbb{Z}$$

Weiter gilt $F^{(k)}(0) = 0 \quad 0 \leq k < p-1$

$$F^{(p-1)}(0) = c_0^s \cdot (-\beta_1)^p \cdots (-\beta_r)^p = c_0^s \left(\frac{c_r}{c_0}\right)^p$$

$$= c_0^{rp-p-1} \cdot c_r^p \in \mathbb{Z}$$

und $F^{(k)}(0) \in p\mathbb{Z}$ für $k \geq p$.

Damit

$$\sum_{j=1}^{r} F(\beta_j) + k \cdot F(0) \equiv \underbrace{K}_{\neq 0} \cdot \underbrace{c_0^{(r-1)p-1}}_{\neq 0} \cdot \underbrace{c_r^p}_{\neq 0} \pmod p$$

Für $p > K, |c_0|, |c_r|$ ist diese Zahl nicht durch p teilbar, ein Widerspruch $\square$

#

13. Ausblick: "Die Quadratur des Kreises ist unmöglich".

Sei $K \subseteq \mathbb{R}^2$ die Menge aller Punkte, die sich mit Zirkel und Lineal aus Punkten mit rationalen Koordinaten konstruieren lassen. Wie sehen die Koordinaten solcher Punkte aus? Wenn man zwei Geraden schneidet, löst man ein linearen Gleichungssystem. Wenn man zwei Kreise schneidet oder ein Kreis und ein Gerade schneidet, löst man quadratische Gleichungen. Man kann zeigen (→ Einführung in die Algebra): Die Menge L der x- und y-Koordinaten der Punkte in K bildet einen Körper, mit

$\mathbb{Q} \subseteq L \subseteq A$, A Menge aller algebraischen Zahlen in $\mathbb{C}$.

Nach Theorem §6.12 gilt $\pi, e \notin L$. Wenn man mit Zirkel und Lineal ein Rechteck mit Seitenlängen a, b mit $a \cdot b = \pi$ konstruieren könnte, so wäre $a, b \in L \Rightarrow a \cdot b = \pi \in L$ ↯. Das ist der Grund, warum die "Quadratur des Kreises" unmöglich ist.