15. Endliche Körper

Ziel:

Klassifikation endlicher Körper und ihrer Beziehungen.

15.1. Situation:

K sei eine endliche Erweiterung des Körpers $\mathbb{F}_p = \mathbb{Z}/p$, $p \in \mathbb{P}$, $[K\colon \mathbb{F}_p] = n$

- $\#(K) = p^n =: q$
- K^* ist zyklisch (7.21.) der Ordnung $q-1$
- Jedes $a \in K$ erfüllt $a^q = a$
- In $K[X]$ gilt: $X^q - X = \prod\limits_{a \in K} (X-a) = f$
- $K = Z_{\mathbb{F}_p, f}$
- Jedes $K\,|\mathbb{F}_p$ ist normal

  Jedes $L|K$ (L, K endliche Körper) ist normal
- Zu $q = p^n$ existiert bis auf $\mathbb{F}_p$-Isomorphie genau ein Körper K mit $\#(K) = q$.

15.2. Satz:

i. Zu jeder Primzahlpotenz $q = p^n$ gibt es bis auf $\mathbb{F}_p$-Isomorphie genau einen Körper der Ordnung q. Wir nennen ein Modell dieses Körpers $\mathbb{F}_q$.

ii. $\mathbb{F}_q$ ist Zerfällungskörper von $f(X) = X^q - X$.

iii. $\mathbb{F}_q$ ist normal über $\mathbb{F}_p$ also auch über jedem Unterkörper L von $\mathbb{F}_q$.

iv. $\mathbb{F}_q$ ist einfach über $\mathbb{F}_p$, z.B. ist $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, falls α eine primitive $(q-1)$-te Einheitswurzel in $\mathbb{F}_q$ ist.

15.3. Beispiel:

$p = 5$; $q = 5^2$, $\quad f_1 = X^2 - 2$, $\quad f_2 = X^2 + X + 1$

$f_i \in \mathbb{F}_5[X]$ irreduzibel $(i = 1, 2)$

$K_1 = N_{\mathbb{F}_5, f_1} = Z_{\mathbb{F}_5, f_1} = \mathbb{F}_5[\eta] = \{a + b\,\eta \,|\, a, b \in \mathbb{F}_5\}$, $\quad \eta$ Nullstelle von f_1, d.h. $\eta^2 = 2$

$K_2 = N_{\mathbb{F}_5, f_2} = Z_{\mathbb{F}_5, f_2} = \mathbb{F}_5[\omega] = \{a + b\,\omega \,|\, a, b \in \mathbb{F}_5\}$, $\quad \omega$ Nullstelle von f_2, d.h. $\omega^2 = -\omega - 1$

$K_1 \underset{\mathbb{F}_5}{\cong} K_2$. Es gibt genau zwei Nullstellen $\alpha_1 \neq \alpha_2$ von f_1 in K_2.

$\alpha_i = ?$ Für $a, b \in \mathbb{F}_5$ gilt:

$$\begin{aligned}
& (a + b\,\omega)^2 = 2 \\
\Leftrightarrow\ & a^2 + 2\,a\,b\,\omega + b^2\,\omega^2 = 2 \\
\Leftrightarrow\ & a^2 + 2\,a\,b\,\omega - b^2(\omega + 1) = 2 \\
\Leftrightarrow\ & a^2 - b^2 + (2\,a\,b - b^2)\,\omega = 2 \\
\Leftrightarrow\ & a^2 - b^2 = 2 \ \wedge 2\,a\,b - b^2 = 0 \\
\Leftrightarrow\ & a^2 - b^2 - 2 = 0 \wedge (2\,a - b)\not{b} = 0 \\
\Leftrightarrow\ & b = 2\,a \ \wedge a^2 = 1 \\
\Leftrightarrow\ & (a, b) = (1, 2) \vee (a, b) = (\underset{=-1}{4}, 3)
\end{aligned}$$

D.h. $\{\alpha_1, \alpha_2\} = \{a + 2\omega, 4\,a + 3\omega\}$, d.h. die beiden Isomorphismen von K_1 und K_2 sind gegeben durch:

$$\begin{array}{lll}
a + b\eta \ \longmapsto\ a + b(a + 2w) & & K_1 \xrightarrow{\cong} K_2 \\
a + b\eta \ \longmapsto\ a + b(4a + 3\omega) = a - b(4a + 2\omega) & & K_1 \xrightarrow{\cong} K_2
\end{array}$$

Ab jetzt wählen wir einen festen algebraischen Abschluss $\bar{\mathbb{F}}_p$ von $\mathbb{F}_p$ und wählen als Modell für einen Körper mit $q = p^n$ Elementen den Teilkörper

$$\mathbb{F}_q := \{a \in \bar{F}_p \,|\, a^q = a\}$$

Dann ist ((in folgender Formel ist $(\mathbb{N}, |)$ gemeint, also $\mathbb{N}$, mit der Ordnungsrelation "teilbar")

$$\bar{\mathbb{F}}_p = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$$

15.4. Korollar:

Seien $q = p^r$, $q' = p^{r'}$ zwei Potenzen von p. Es gilt:

$$\mathbb{F}_q \subset \mathbb{F}_{q'} \Leftrightarrow q' = q^s \ (s \in \mathbb{N}) \Leftrightarrow r' = r \cdot s \ (s \in \mathbb{N})$$

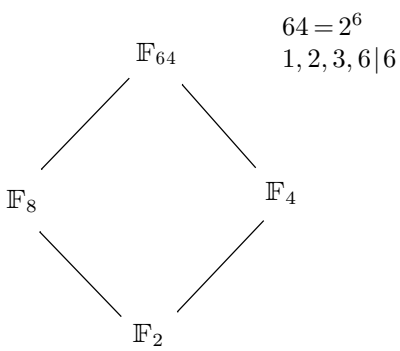
Beweis.

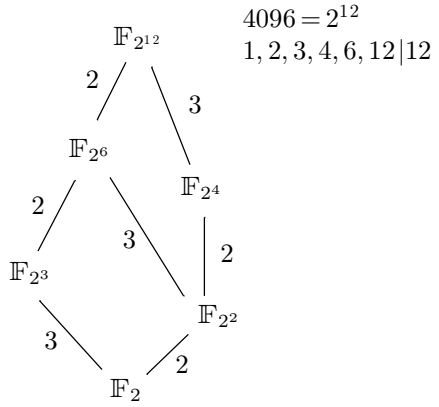
„$\Rightarrow$" klar.

„ $\Leftarrow$" Für $x \in \mathbb{F}_q$ ist $x^{q'} = x^{q^s} = \underbrace{\big(\cdots\big((x^q)^q\big)\cdots\big)^q}_{s-\text{mal}} = x$, also $x \in \mathbb{F}_{q'}$

□

Beispiel:





15.5. Korollar:

Zu jedem endlichen Körper $\mathbb{F}_q$ und jedem $n \in \mathbb{N}$ existieren irreduzible Polynome $f \in \mathbb{F}_q[X]$ vom Grad n.

Beweis.

Sei $\alpha \in \mathbb{F}_{q^n}$ mit $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Dann ist $f = m_{\mathbb{F}_q,\alpha}$ wie erwünscht. □

15.6. Definition:

i. Ist $L|K$ eine Erweiterung endlicher Körper, so sei

$$\mathrm{Aut}(L|K) = \left\{ \sigma\colon L \longrightarrow L \;\middle|\; \begin{array}{l} \sigma \text{ ist } K\text{-Automorphismus} \\ \text{und } \sigma|_K = \mathrm{id}_K \end{array} \right\}$$
$$= \text{Automorphismengruppe von } L \text{ über } K$$

$$\mathrm{Aut}(L) = \left\{ \sigma\colon L \xrightarrow{\cong} L \right\} = \mathrm{Aut}(L|\mathbb{F}_p)$$

$$\mathrm{Aut}(L|K) \hookrightarrow \mathrm{Aut}(L)$$

Beispiel:

Für die Körper K_i aus 15.3. gilt
$$\begin{array}{rclcl} \mathrm{Aut}(K_1) & = & \{1,\sigma\}, & \sigma\colon a+b\eta & \longmapsto & a-b\eta \\ \mathrm{Aut}(K_2) & = & \{1,\tau\}, & \tau\colon a+b\omega & \longmapsto & a+b(-1-\omega) \end{array}$$

ii. Ist K ein endlicher Körper der Charakteristik p, so sei

$$\begin{array}{rclcl} \varphi & = & \varphi_p\colon & K & \longrightarrow & K \\ & & & a & \longmapsto & a^p \end{array}$$

der Frobenius-Automorphismus.

Ist $q = p^n$, so sei

$$\begin{array}{rclcl} \varphi_q\colon & K & \longrightarrow & K \\ & a & \longmapsto & a^q \end{array}, \qquad \varphi_q = \varphi_{p^n} = (\varphi_p)^n = \underbrace{(\varphi_p \circ \ldots \circ \varphi_p)}_{n-\text{mal}}$$

Eigenschaften von φ_p bzw. φ_q:

i. $\varphi_{p^n} = (\varphi_p)^n$

ii. Für $a, b \in K$ gelten

$$\begin{array}{rcl} \varphi_q(a+b) & = & \varphi_q(a) + \varphi_q(b) \\ \varphi_q(a \cdot b) & = & \varphi_q(a) \cdot \varphi_q(b) \end{array}$$

Um die Additivität von φ_q zu zeigen, reicht es, dies für die Abbildung von φ_p zu zeigen. Diese liegt an:

$$(a+b)^p = \sum_{0 \leqslant i \leqslant p} \underbrace{\binom{p}{i}}_{\substack{\equiv 0, \\ p \\ \text{falls } 1 \leqslant i \leqslant p-1}} a^i b^{p-i} = a^p + b^p \quad \text{in } K$$

iii. Also ist φ_q ein Ringhomomorphismus, sogar $\varphi_p \in \mathrm{Aut}(K)$.

iv. Ist $\#(K) = q = p^n$, so sind die $\varphi_p^i \quad (0 \leqslant i \leqslant n-1)$ auf K alle verschieden.

$$\begin{array}{rcl} \varphi_{p^i} = \varphi_p^i \colon & K & \longrightarrow & K \\ & a & \longmapsto & a^{p^i} \end{array}$$

eingeschränkt auf $(K^*, \cdot\,)$ sind Gruppenautomorphismen.

$(K^*, \cdot\,) \cong (\mathbb{Z}/q-1, +\,), \quad (q-1) = (p-1)\,(1 + p + \ldots + p^{n-1})$

$\varphi_p^i \longleftrightarrow$ Multiplikation mit p^i, die p^i $(0 \leqslant i \leqslant p-1)$ alle verschieden modulo $(q-1)$.

Dagegen ist $\varphi_q|_K = (a \longmapsto a^q)$ die Identität.

v. Ist wieder $\#(K) = q = p^n$, so ist

$$\mathrm{Aut}(K) = \left\{ \varphi_p^i \mid 0 \leqslant i \leqslant n-1 \right\} = \begin{array}{l} \text{zyklische Gruppe } \langle \varphi_p \rangle \\ \text{der Ordnung } n, \text{ erzeugt} \\ \text{von } \varphi_p \end{array}$$

Denn: $K = \mathbb{F}_p(\alpha)$, $\alpha \in K$ geeignet. Dann ist mit $m(X) := m_{\mathbb{F}_p, \alpha}(X)$

$$\begin{aligned} \#(\mathrm{Aut}(K)) = \#(\mathrm{Aut}(K|\mathbb{F}_p)) &= \#\left\{ \begin{array}{l} \text{verschiedene Nullstellen} \\ \text{von } m \text{ in } K \end{array} \right\} \\ &\leqslant \deg(m) = [K \colon \mathbb{F}_p] = n \end{aligned}$$

Wegen (iv) gilt die Gleichheit.

vi. Das Minimalpolynom jedes $\alpha \in K|\mathbb{F}_p$ zerfällt in K in lauter verschiedene Linearfaktoren über K (d.h. das Polynom ist <u>separabel</u>).

vii. Sei $L|K$, $\#(K) = q$, $[L \colon K] = r$, $\#(L) = q^r = p^{rn}$

$$\begin{array}{ccccccc} \mathrm{Aut}(L|K) = & \left\{ \varphi^i \;\middle|\; \begin{array}{c} 0 \leqslant i < r\,n \\ i \equiv 0 \,(\mathrm{mod}\, n) \end{array} \right\} = & \{ \varphi_q^j \mid 0 \leqslant j < r \} = & \langle \varphi_q \rangle = & \begin{array}{l} \text{zyklische Gruppe} \\ \text{der Ordnung } r \end{array} \\ \downarrow & & & & \\ \mathrm{Aut}(K|\mathbb{F}_p) = & \left\{ \varphi^i \mid 0 \leqslant i < r\,n \right\} & = & \langle \varphi \rangle = & \begin{array}{l} \text{zyklische Gruppe} \\ \text{der Ordnung } r\,n \end{array} \end{array}$$

$$\mathrm{Aut}(L|K) \longhookrightarrow \mathrm{Aut}(L|\mathbb{F}_p)$$

$$\begin{array}{c} L \\ |r \\ K \\ |n \\ \mathbb{F}_p \end{array}$$

15.7. Satz:

i. Ist $L|K$ eine Erweiterung endlicher Körper, $[L \colon K] = n$, so ist $\mathrm{Aut}(L|K)$ zyklisch, erzeugt vom Frobenius-Automorphismus φ_q mit $q = \#(K)$.

ii. Ist $L|M|K$ mit $[L\colon M]=s$, $[M\colon K]=t$, so ist $\mathrm{Aut}(L|M)$ die wohlbestimmte Untergruppe von $\mathrm{Aut}(L|K)$ der Ordnung s.

iii. Die Untergruppen H von $\mathrm{Aut}(L|K)$ entsprechen eineindeutig den Zwischenkörpern M von $L|K$ durch:

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{Untergruppen von}\\ \mathrm{Aut}(L|K)\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{Körper } M \text{ mit}\\ K\subset M\subset L\end{array}\right\} \\ H & \longmapsto & \{a\in L\,|\,\forall\sigma\in H \text{ ist } \sigma(a)=a\} \;=:L^H \\ \mathrm{Aut}(L|M) & \longleftarrow & M \end{array}$$

Der Körper L^H heißt der Fixkörper von H.

Diese Bijektion ist ordungsvertauschend.

Beweis.

i. , ii. gezeigt (mit zum Teil verschiedenen Bezeichnungen).

iii. Es ist klar, dass $H\longmapsto L^H$ und $M\longmapsto \mathrm{Aut}(L|M)$ wohldefinierte Abbildungen in die behaupteten Mengen sind. Die Bijektivität (und Injektivität) folgt daraus, dass beide Mengen eineindeutig den Teilern von $n=[L\colon K]$ entsprechen. □

15.8. Korollar:

Sei $[L\colon K]=r$, $\#(K)=q$. Es gilt:

$$X^{q^r}-X=\prod_{\substack{f\in K[X]\\ f\text{ normiert,}\\ \text{irreduzibel}\\ \deg(f)|r}} f$$

Beweis.

i. Für $\alpha\in L$ gilt $\alpha^{q^r}=\alpha$, also $X^{q^r}-X=\prod\limits_{\alpha\in L}(X-\alpha)$.

ii. $G:=\mathrm{Aut}(L|K)$ operiert auf L, also auch koeffizientenweise auf $L[X]$. Zerlege $L=\dot{\bigcup} B_i$ in Bahnen unter G. Für jede dieser Bahnen B ist:

$$f_B(X)=\prod_{\alpha\in B}(X-\alpha)\quad\in K[X],$$

da für $\sigma\in G$ gilt:

$$(\sigma f_B)(X)=\prod_{\alpha\in B}(X-\sigma(\alpha))\underset{\substack{\sigma\text{ bewirkt nur eine}\\ \text{Permutation von } B}}{=}\prod_{\alpha\in B}(X-\alpha)=f_B(X)$$

Wegen $L^G=K$, gehört $f_{B(X)}$ zu $L^G[X]=K[X]$.

iii. Jedes der $f_B\in K[X]$ ist irreduzibel.

Schreibe $f_B=g\cdot h$, $g,h\in K[X]$, normiert und $\deg(g),\deg(h)\geqslant 1$.

$$\begin{array}{rcll} g(X) & = & \prod & (X-\gamma_i) \\ h(X) & = & \prod & (X-\eta_j) \end{array} \qquad ,\{\gamma_i\}\dot{\cup}\{\eta_j\}=B.$$

Wegen $g, h \in K[X]$ ist für $\sigma \in G$: $\sigma(g) = g, \sigma(h) = h$, was impliziert:

$$\begin{array}{rcl} \sigma(\{\gamma_i\}) & = & \{\gamma_i\} \\ \sigma(\{\eta_j\}) & = & \{\eta_j\} \end{array}$$ *Widerspruch*, da G transitiv auf B operiert.

iv. Für jede Bahn B ist $\deg(f_B) = \#(B) \mid \#(G) = [L\colon K] = r$. D.h. jedes f_B ist ein irreduzibler Teiler von $X^{q^r} - X$, dessen Grad r teilt.

v. Umgekehrt:

Ist f normiert, irreduzibel, $t := \deg(f) \mid r$, so ist $M := N_{K,f} = Z_{K,f}$ eine Körpererweiterung des Grades t von K, d.h. M besitzt eine K-Einbettung nach L (da $t \mid r = [L\colon K]$).

$\rightsquigarrow f$ zerfällt vollständig über L, $f(X) = \prod\limits_{1 \leqslant i \leqslant t} (X - \alpha_i)$, α_i die Nullstellen von f in L, alle verschieden. Es gibt genau t K-Automorphismen von $M \mid K$, gegeben durch

$\alpha_1 \longmapsto \alpha_i$ $(1 \leqslant i \leqslant t)$. Diese können zu K-Automorphismen von L fortgesetzt werden. Deshalb ist $B := \{\alpha_1, ..., \alpha_t\}$ eine Bahn von G.

Also ist $f = f_B$.

□

Beispiel:

Ist r selbst prim, so ist

$$X^{q^r} - X = \left(\prod_{\substack{f \text{ normiert} \\ f \text{ irreduzibel} \\ \deg(f) = r}} f \right) \cdot \left(\prod_{\substack{g \text{ normiert} \\ g \text{ irreduzibel} \\ \deg(g) = 1}} g \right)$$

$$\rightsquigarrow q^r = r \cdot \#\left\{ f \;\middle|\; \begin{array}{l} f \text{ normiert vom} \\ \text{Grad } r \end{array} \right\} + q$$

$$\rightsquigarrow \frac{q^r - q}{r} = \#\left\{ f \;\middle|\; \begin{array}{l} f \text{ normiert vom} \\ \text{Grad } r \end{array} \right\}$$

15.9. Definition:

i. $\pi_q(r)$:= Zahl der irreduziblen, normierten Polynome $f \in \mathbb{F}_q[X]$ vom Grad r

ii. Ist $f\colon \mathbb{N} \longrightarrow A$ eine beliebige Abbildung in eine abelsche Gruppe $(A, +)$, so heißt

$$F\colon \mathbb{N} \longrightarrow A, \text{definiert durch } F(n) = \sum_{\substack{d \in \mathbb{N} \\ d \mid n}} f(d)$$

die Möbius-Transformierte von f.

iii. Die Möbius-Funktion $\mu\colon \mathbb{N} \longrightarrow \{0, \pm 1\}$ ist definiert durch:

$$f(n) := \begin{cases} (-1)^s & \text{, falls } n \text{ Produkt von } s \text{ verschiedenen Primzahlen ist} \\ 0 & \text{, falls } n \text{ teilbar durch } m^2 \text{ mit } m > 1 \end{cases}$$

Insbesondere ist $\mu(1)=1$.

15.10. Lemma:

μ erfüllt:

$$\sum_{d|n}\mu(d)=\begin{cases}1 & ,\text{falls } n=1\\ 0 & ,\text{falls } n>1\end{cases}$$

Beweis.

Offensichtlich ist μ schwach multiplikativ, d.h. $\mu(m\cdot n)=\mu(m)\cdot\mu(n)$, falls $\mathrm{ggT}(m,n)=1$ und $\mu(1)=1$.

Induktion nach der Zahl r der verschiedenen Primteiler von n.

$r=1$:

$n=p^s,\ s\geqslant 1.\ \sum\limits_{d|n}\mu(d)=\underbrace{\mu(1)}_{=1}+\underbrace{\mu(p)}_{=-1}+\underbrace{\mu(p^2)+\ldots+\mu(p^s)}_{=0}=0$.

$r>1$:

Zerlege $n=n'\cdot p^s$ mit $(n',p)=1,\ n'>1, s\geqslant 1$.

$$\sum_{d|n}\mu(d)=\sum_{\substack{d'|n'\\0\leqslant t\leqslant s}}\mu(d'\cdot p^t)=\sum_{\substack{d'|n'\\0\leqslant t\leqslant s}}\mu(d')\cdot\mu(p^t)=\underbrace{\left(\sum_{d'|n'}\mu(d')\right)}_{=0}\underbrace{\left(\sum_{0\leqslant t\leqslant s}\mu(p^t)\right)}_{=0}=0$$

□

15.11. Korollar (Möbius-Inversionsformel):

Sei $f:\mathbb{N}\longrightarrow A$ wie in 15.9. Dann gilt:

$$f(n)=\sum_{d|n}\mu\Big(\frac{n}{d}\Big)F(d)$$

Beweis.

$$\sum_{d|n}\mu\Big(\frac{n}{d}\Big)F(d)=\sum_{d|n}\mu\Big(\frac{n}{d}\Big)\cdot\sum_{c|d}f(c)=\sum_{c|n}\underbrace{\left(\sum_{\substack{d\in\mathbb{N}\\ c|d|n}}\mu\Big(\frac{n}{d}\Big)\right)}_{\substack{=\sum\limits_{d'|\frac{n}{c}}\mu(d')=0\\ \text{außer bei } \frac{n}{c}=1}}f(c)=f(n)$$

□

Betrachtung der Grade in 15.8. liefert:

$$q^r=\sum_{d|r}d\cdot\pi_q(d)$$

Mit anderen Worten:

Die Funktion $\begin{array}{rccc} f\colon & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & n\cdot\pi_q(n) \end{array}$ hat als Möbiustransformierte $F(r)=q^r$.

Nach 15.11. also:

$$n\cdot\pi_q(n)=f(n)=\sum_{d|n}\mu\Big(\frac{n}{d}\Big)q^d.$$

Also:

15.12. Satz:

$$\pi_q(n)=\frac{1}{n}\cdot\sum_{d|n}\mu\Big(\frac{n}{d}\Big)\,q^d=\frac{q^n}{n}+\mathcal{O}(q^{\frac{n}{2}})$$

Bemerkung: Daraus ergibt sich insbesondere $\pi_q(n)=\frac{q^n}{n}+\mathcal{O}(q^{\frac{n}{2}})$. Anschaulich ist also die Wahrscheinlichkeit für $f\in\mathbb{F}_q[X]$ vom Grad n, prim zu sein, ungefähr durch $\frac{1}{n}$ gegeben.

Beispiele:

$$\begin{aligned}
\pi_q(2) &= \frac{1}{2}(q^2-q)\\
\pi_q(3) &= \frac{1}{3}(q^3-q)\\
\pi_q(4) &= \frac{1}{4}(q^4-q^2)\\
\pi_q(5) &= \frac{1}{5}(q^5-q)\\
\pi_q(6) &= \frac{1}{6}(q^6-q^3-q^2+q)\\
\pi_q(24) &= \frac{1}{24}(q^{24}-q^{12}-q^8+q^4)
\end{aligned}$$

Weitere Beispiele für die Anwendung von (15.11.):

Betrachte $g_n(X)=\prod_{\substack{\omega\text{ ist }n\text{-te}\\ \text{Einheitswurzel}}}(X-\omega)\qquad\in\mathbb{C}[X]$, dann ist $g_n(X)=X^n-1$.

$f_n(X)=\prod_{\substack{\omega\text{ ist primitive}\\ n\text{-te Einheitswurzel}}}(X-\omega)$

$$g_n(X)=\prod_{d|n}f_d(X)$$

$$\left(\begin{array}{rcl} f_1(X) &=& (X-1)\\ f_2(X) &=& (X+1)\\ \overset{\sim}{z.B.}\ f_3(X) &=& (X^2+X+1)\\ f_4(X) &=& (X^2+1) \end{array}\right)$$

$$\begin{array}{rcl} f\colon\mathbb{N} &\longrightarrow& (C(X))^*\\ n &\longmapsto& f_n\\ g\colon n &\longmapsto& g_n \end{array}$$

$$g\colon n\longmapsto g_n$$

g ist die Möbiustransformierte von f. Also gilt:

$$(15.13.) \qquad f_n = \prod_{d|n} g_d^{\mu(\frac{n}{d})}$$

Beispiel:

$$f_{24} = \frac{g_4 \cdot g_{24}}{g_{12} \cdot g_8} = \frac{(X^{24}-1)}{(X^{12}-1)} \cdot \frac{(X^4-1)}{(X^8-1)} = \frac{(X^{12}+1)}{(X^4+1)} = X^8 - X^4 + 1$$

$\big(d|24 : d = \not{1}, \not{2}, \not{3}, 4, \not{6}, 8, 12, 24\big)$

Betrachten wir die Grade der beteiligten Polynome, so ergibt sich:

$$\varphi(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, n \qquad \left(\begin{array}{c} \text{die Umkehrformel zu} \\ n = \sum_{d|n} \varphi(d) \end{array} \right)$$

(15.3.) bleibt richtig, wenn man $\mathbb{C}$ durch einen beliebigen Körper K ersetzt mit $(\mathrm{Char}(K), n) = 1$.

Frage:

Wieviele $n \in \mathbb{N}$ mit $n \leqslant x$ gibt es, die quadratfrei sind?

Wieviele $n \in \mathbb{N}$ mit $n \leqslant x$ gibt es, die frei von k-ten Potenzen sind?

[1]

$$\begin{array}{rcl} P(\text{„}n \text{ quadratfrei“}) & := & \lim\limits_{x \longrightarrow \infty} \dfrac{\#\{n \in \mathbb{N} \,|\, n \leqslant x, \square \not| \, n\}}{\#\{n \in \mathbb{N} \,|\, n \leqslant x\}} \\ & =^{[2]} & \Big(1 - \dfrac{1}{4}\Big)\Big(1 - \dfrac{1}{9}\Big)\Big(1 - \dfrac{1}{25}\Big)... \\ & = & \prod\limits_{p \in \mathbb{P}} \Big(1 - \dfrac{1}{p^2}\Big) \\ & = & (\zeta(2))^{-1} \\ & \underset{\substack{\text{Euler 1735} \\ \zeta(2) = \frac{\pi^2}{6}}}{=} & \dfrac{6}{\pi^2} \\ & \approx & 60,5\% \end{array}$$

$$\prod_{p \in \mathbb{P}} \big(1 - p^{-s}\big)^{-1} \quad = \quad \prod_{p \in \mathbb{P}} \big(1 + p^{-s} + p^{-2s} + p^{-3s} + ...\big) \quad (1 < s \in \mathbb{R})$$

$$\underset{\substack{\text{eindeutige} \\ \text{Primfaktor-} \\ \text{zerlegung}}}{=} \quad \sum_{n \in \mathbb{N}} n^{-s} \quad =: \zeta(s)$$

$\zeta(s)$ ist die Riemannsche Zeta-Funktion.

1. $\square \not| \, n$ heißt „n wird nicht von einem Quadrat geteilt“ = „n ist quadratfrei“

2. Dieses Gleichheitszeichen ist hier nur plausibel, nicht wirklich bewiesen. Es kann aber begründet werden nach Durchführung der einschlägigen Abschätzungen

Statt reeller Argumente $s > 1$ verwendet man besser komplexe Argumente s mit $\mathrm{Re}(s) > 1$.

$$P(\text{„}n \text{ frei von } k\text{-ten Potenzen“}) = (\zeta(k))^{-1}$$

$\zeta(k)$ ist bekannt für gerade k: z.B. $\zeta(4) = \dfrac{\pi^4}{90}$
$\zeta(k)$ ist unbekannt für ungerade k: Bewiesen ist lediglich: $\zeta(3) \notin \mathbb{Q}$.

15.14. Definition:

Zu fester Primzahlpotenz q seien:

$\mathbb{F}_q$	„der‘ Körper‘ mit $\#(\mathbb{F}_q) = q$
A	$:= \mathbb{F}_q[X]$
A_+	$:= \{\text{normierte Elemente von } A\}$
$A_{+,n}$	$:= \{a \in A_+ \mid \deg(a) = n\}$
$A_{+,n,k}$	$:= \{a \in A_{+,n} \mid a \text{ ist frei von } k\text{-ten Potenzen}\}$
α_n	$:= \#\{a \in A_+ \mid \deg(a) = n\} = q^n$
$\alpha_{n,k}$	$:= \#A_{+,n,k}$

Außerdem gelten die Beziehungen:

$$A \supset A_+ \supset A_{+,n} \supset A_{+,n,k}$$

Für $a \in A$ sei $|a| := \begin{cases} q^{\deg(a)} & , a \neq 0 \\ 0 & , a = 0 \end{cases}$

$$\zeta_A(s) := \sum_{a \in A_+} |a|^{-s} \quad s \in \mathbb{C} \quad \text{(zunächst nur als formale Summe.)}$$

Ziel:

Berechnung von $\alpha_{n,k}$.

Analogie von Zahlen und Polynomen:

$$\begin{array}{ccc} A & \longleftrightarrow & \mathbb{Z} \\ A_+ & \longleftrightarrow & \mathbb{N} \\ \mathbb{P}_A & \longleftrightarrow & \mathbb{P} \\ |\cdot| & \longleftrightarrow & |\cdot| \\ \zeta_A & \longleftrightarrow & \zeta \end{array}$$

15.15. Proposition:

i. Die Summe für $\zeta_A(s)$ konvergiert absolut für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$

und

ii. stimmt dort mit dem Produkt $\prod_{\wp \in \mathbb{P}_A} \left(1 - |\wp|^{-s}\right)^{-1}$ überein

und

iii. erfüllt $\zeta_A(s) = \frac{1}{1-q^{1-s}}$.

Beweis.

i. und iii.

Für $1 < s \in \mathbb{R}$ ist:

$$\zeta_A(s) = \sum_{n \geqslant 0} \sum_{a \in A_{+,n}} |a|^{-s} = \sum_{n \geqslant 0} \alpha_n q^{-ns} = \sum_{n \geqslant 0} q^n q^{-ns} = \sum_{n \geqslant 0} q^{n(1-s)} = \frac{1}{1-q^{1-s}}.$$

Wegen $|q|^{-s} = q^{-\mathrm{Re}(s)}$ gilt dies auch für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$, d.h. (i) und (iii).

ii.

$$\begin{aligned} \prod_{\wp \in \mathbb{P}_A} \frac{1}{1-|\wp|^{-s}} &= \prod_{\wp \in \mathbb{P}} \left(1 + |\wp|^{-s} + |\wp|^{-2s} + |\wp|^{-3s} + \ldots\right) \\ &= \prod_{\wp \in \mathbb{P}} \left(1 + |\wp|^{-s} + |\wp^2|^{-s} + |\wp^3|^{-s} + \ldots\right) \\ &\overset{!}{=} \sum_{a \in A_+} |a|^{-s} \\ &\text{(absolut konvergent für } \mathrm{Re}(s) > 1) \end{aligned}$$

Wieder gilt - wie im Fall der Riemannschen Zeta-Funktion - die letzte Gleicheit wegen der eindeutigen Primfaktorzerlegung in A_+.

□

15.16. Korollar:

Sei $1 < k \in \mathbb{N}$. Für $\mathrm{Re}(s) > 1$ gilt auch:

$$\prod_{\wp \in \mathbb{P}_A} \left(\sum_{0 \leqslant i < k} |\wp|^{-is} \right) = \sum_{n \geqslant 0} \alpha_{n,k} q^{-ns}$$

Beweis.

$\sum\limits_{0 \leqslant i < k} |\wp|^{-is}$ ist Teilsumme von $\sum\limits_{i=0}^{\infty} |\wp|^{-is} = \frac{1}{1-|\wp|^{-s}}$. D.h. die Konvergenz links gilt, da es sich um eine Teilsumme der Summe in 15.15.(ii) handelt. Die Teilsumme von $\sum\limits_{a \in A_+} |a|^{-s}$, die so entsteht, ist genau über die $a \in A_+$, die frei von k-ten Potenzen sind.

D.h.

$$\text{Linke Seite} = \sum_{n \geqslant 0} \sum_{a \in A_{+,n,k}} |a|^{-s} = \sum_{n \geqslant 0} \alpha_{n,k} q^{-ns}$$

□

15.17. Satz:

Es gilt:

$$\alpha_{n,k} = \begin{cases} \zeta_A^{-1}(k)\, q^n & , n \geqslant k \\ q^n & , n < k \end{cases}$$

Bemerkung:

i. Für $n \geqslant k$ ist also $P(\text{„}a \in A_{+,n}, a \text{ ist frei von } k\text{-ten Potenzen“}) = \zeta_A^{-1}(k)$

ii. $\zeta_A^{-1}(k) = 1 - q^{1-k}$. Mit anderen Worten:

$$P(a \in A_+ \,|\, \square \not| a) = \frac{q-1}{q} \qquad (\longleftrightarrow \frac{6}{\pi^2})$$

Beweis.

Für $k \geqslant 1$ und $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ ist:

$$\begin{aligned} 1 - q^{1-ks} = \zeta_A^{-1}(k\,s) &= \prod_{\wp \in \mathbb{P}_A} \left(1 - |\wp|^{-ks}\right) \\ = \prod_{\wp \in \mathbb{P}_A} \Big(1 + |\wp|^{-s} + |\wp|^{-2s} + |\wp|^{-3s} + \ldots + |\wp|^{-(k-1)s}\Big)\big(1 - |\wp|^{-s}\big) & \\ = \zeta_A^{-1}(s) \sum_{n \geqslant 0} \alpha_{n,k}\, q^{-ns} & \end{aligned}$$

Setze $u := q^{-s}$. Dann

$$1 - q\,u^k = (1 - q\,u) \cdot \sum_{n \geqslant 0} \alpha_{n,k}\, u^n$$

$$\rightsquigarrow (1 - q\,u^k)(1 + q\,u + q^2\,u^2 + \ldots) = \sum_{n \geqslant 0} \alpha_{n,k}\, u^n$$

Der Koeffizient von u^n auf der linken Seite ist $\begin{cases} q^n & , n < k \\ q^n - q^{n-k+1} & , n \geqslant k. \end{cases}$

□