Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 28 (1973)
Heft: 4

Artikel: Irreduzible Polynome als kombinatorische Figuren
Autor: Jeger, M.
DOI: https://doi.org/10.5169/seals-29455

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 14.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Anhang (Beweis des Lemmas). Es seien $q_1, q_2, \ldots$ die Primzahlen mit $q_i \equiv -1 \pmod{p}$. Nach dem Dirichletschen Satz gilt $\sum q_i^{-1} = \infty$. Somit divergiert die Reihe $\sum v_i$ mit $v_i = (q_i - 1)\, q_i^{-2}$. Das unendliche Produkt $\Pi\,(1 - v_i)$ strebt daher gegen Null. Man kann also $\eta > 0$ beliebig und r so gross wählen, dass

$$\prod_{i=1}^{r} (1 - v_i) < \eta/2\,. \tag{11}$$

Wenn für irgend ein i $q_i \mid n$ und $q_i^2 \nmid n$ gilt, so folgt $\sigma(n) \equiv 0 \pmod{p}$. Nun sei $B_r = \prod_{i=1}^{r} q_i$. Wenn für ein u in $1 \leq u < B_r^2$ und ein $i \leq r$ $q_i \mid u$ und $q_i^2 \nmid u$ gilt, dann folgt aus $n \equiv u \pmod{B_r^2}$, dass $\sigma(n) \equiv 0 \pmod{p}$. Für die Anzahl der Restklassen $u \pmod{B_r^2}$, die diese Eigenschaft *nicht* haben, erhält man sofort aus dem Sieb des Eratosthenes den Ausdruck

$$B_r^2 \prod_{i=1}^{r} \left(1 - \frac{q_i - 1}{q_i^2}\right),$$

der nach (11) $< 0{,}5\, \eta\, B_r^2$ ist. Daher ist für $x > x_0\,(\eta, r)$ die Anzahl der Zahlen $n \leq x$ mit $\sigma(n) \not\equiv 0 \pmod{p}$ kleiner als

$$0{,}5\, \eta\, B_r^2 \cdot x\, B_r^{-2} + 0{,}5\, \eta\, B_r^2 < \eta x\,. \tag{12}$$

Da (12) für jedes $\eta > 0$ gilt, ist der Beweis fertig. P. Erdös

Irreduzible Polynome als kombinatorische Figuren

Der folgende Beitrag behandelt ein Abzählproblem aus der klassischen Algebra, das erstmals von Gauss gelöst worden ist. Gelegentlich taucht es auch in der neueren Literatur wieder auf (Vgl. [1] und [2]). Mit der Darlegung der folgenden Lösung soll ein Einblick in die modernen Methoden der abzählenden Kombinatorik vermittelt werden.

1. Die Problemstellung

Die endlichen Körper oder *Galois-Felder* werden in der algebraischen Literatur meist damit abgetan, dass an einer geeigneten Stelle ein kurzer und eleganter Existenzbeweis eingeflochten wird. Die neueren Entwicklungen in der sogenannten *finiten Mathematik*[1]) bringen es mit sich, dass die Galois-Felder mehr und mehr explizit benötigt werden. So kann zum Beispiel auf Grund einer Darstellung des Galois-Feldes $GF(p^n)$[2]) die endliche Desarguessche affine Ebene von der Ordnung $s = p^n$ leicht konstruiert werden. Damit im Zusammenhang steht die Aufgabe, orthogonale lateinische Quadrate von der Ordnung $s = p^n$ zu finden. An lateinischen Verteilungen

[1]) Im angelsächsischen Raum treffender als Combinatorial Mathematics bezeichnet.

[2]) p ist eine Primzahl, n eine beliebige natürliche Zahl.

ist der Statistiker sehr interessiert; er verwendet sie gelegentlich bei der Planung von Versuchen.

Um eine Darstellung des Galois-Feldes $GF(p^n)$ zu erhalten, kann man vom Polynomring über dem Restklassenkörper mod p ausgehen. Man greift aus dem Polynomring über $GF(p)$ ein *irreduzibles Polynom vom Grad n* heraus und betrachtet dann die Restklassen in bezug auf dieses Polynom. Wir wollen dieses an sich elementare Konstruktionsverfahren an einem Beispiel genauer verfolgen.

Es soll etwa das Galois-Feld $GF(2^3)$ gewonnen werden. Ausgangsbasis ist der Restklassen-Körper $GF(2)$. Seine beiden Elemente seien mit 0 (Nullelement) und 1 (Einselement) bezeichnet. Ein irreduzibles Polynom 3. Grades mit Koeffizienten aus $GF(2)$ ist

$$g(x) = x^3 + x + 1 .$$

Wegen $g(0) = 1$ und $g(1) = 1$ lässt sich nämlich kein Linearfaktor abspalten. Die Elemente von $GF(2^3)$ sind nun die Polynome

	neue Bezeichnung
0	α_0
1	α_1
x	α_2
$x + 1$	α_3
x^2	α_4
$x^2 + 1$	α_5
$x^2 + x$	α_6
$x^2 + x + 1$	α_7

α_0 ist das Nullelement, α_1 das Einselement.

Für die Summe und das Produkt von Polynomen mod $g(x)$ erhält man leicht die folgenden Verknüpfungstafeln:

$\oplus$	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_0	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_1	α_1	α_0	α_3	α_2	α_5	α_4	α_7	α_6
α_2	α_2	α_3	α_0	α_1	α_6	α_7	α_4	α_5
α_3	α_3	α_2	α_1	α_0	α_7	α_6	α_5	α_4
α_4	α_4	α_5	α_6	α_7	α_0	α_1	α_2	α_3
α_5	α_5	α_4	α_7	α_6	α_1	α_0	α_3	α_2
α_6	α_6	α_7	α_4	α_5	α_2	α_3	α_0	α_1
α_7	α_7	α_6	α_5	α_4	α_3	α_2	α_1	α_0

$\odot$	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_1	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_2	α_2	α_4	α_6	α_3	α_1	α_7	α_5
α_3	α_3	α_6	α_5	α_7	α_4	α_1	α_2
α_4	α_4	α_3	α_7	α_6	α_2	α_5	α_1
α_5	α_5	α_1	α_4	α_2	α_7	α_3	α_6
α_6	α_6	α_7	α_1	α_5	α_3	α_2	α_4
α_7	α_7	α_5	α_2	α_1	α_6	α_4	α_3

Allgemein ist die Konstruktion von $GF(p^n)$ möglich, sobald ein irreduzibles Polynom n-ten Grades über $GF(p)$ bekannt ist. Es existiert stets ein solches Polynom. Wir stellen uns nun die Aufgabe, ihre Anzahl zu bestimmen.

Ein Polynom n-ten Grades über $GF(p)$

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

heisst genormt, wenn $a_n = 1$ ist. Im Lichte unserer Köprer-Erweiterungen sind natürlich nur die verschiedenen genormten irreduziblen Polynome n-ten Grades von Interesse. Wir wollen daher das Abzählproblem wie folgt präzisieren: *Es soll die Anzahl der genormten irreduziblen Polynome n-ten Grades über dem Restklassen-Körper $GF(p)$ ermittelt werden.* Diese Anzahl wird anschliessend mit f_n bezeichnet.

2. Ein Satz über abzählende Potenzreihen

Es sei $\boldsymbol{F}$ eine abzählbare *Menge von kombinatorischen Figuren*

$$\boldsymbol{F} = \{\Phi_1, \Phi_2, \Phi_3, \ldots\ldots\}$$

wobei der Figur Φ_i die nicht-negative ganze Zahl m_i als *Index* zugeordnet ist. Die *formale Potenzreihe* in der Unbestimmten z

$$\varphi(z) = \sum_{\boldsymbol{F}} z^{m_i}$$

heisst dann die *abzählende Potenzreihe der Figurenmenge* $\boldsymbol{F}$.

Beispiel: Mit einer bestimmten Sorte von 10-Rappen-Briefmarken werde die Figurenmenge

$$\boldsymbol{B} = \{-, \square, \square\square, \square\square\square, \ldots\ldots\}$$

gebildet. Das erste Zeichen in der Klammer kennzeichnet die sogenannte leere Figur, die gelegentlich sehr zweckmässig ist. Hat eine Figur in $\boldsymbol{B}$ den Frankatur-Wert $10n$ Rappen, so wollen wir ihr den Index n zuordnen. Dann gehört zur Figurenmenge $\boldsymbol{B}$ offenbar die abzählende Potenzreihe

$$\beta(z) = 1 + z + z^2 + \cdots\cdot = \frac{1}{1-z}$$

Wir betrachten jetzt zwei Figurenmengen

$$\boldsymbol{F}_1 = \{\Phi_1, \Phi_2, \ldots\ldots\} \quad \text{und} \quad \boldsymbol{F}_2 = \{\psi_1, \psi_2, \ldots\ldots\}\,.$$

Wird der Figur ϕ_i der Index m_i, der Figur ψ_j der Index n_j zugeschrieben, dann gehören zu F_1 und F_2 die abzählenden Potenzreihen

$$\varphi_1(z) = \sum_{\boldsymbol{F}_1} z^{m_i}\,; \quad \varphi_2(z) = \sum_{\boldsymbol{F}_2} z^{n_j}$$

Aus $\boldsymbol{F}_1$ und $\boldsymbol{F}_2$ lässt sich nun die neue Figurenmenge

$$\boldsymbol{F}_1 \times \boldsymbol{F}_2 = \{(\Phi_i, \psi_j)/\Phi_i \in \boldsymbol{F}_1 \wedge \psi_j \in \boldsymbol{F}_2\}$$

ableiten. Gibt man darin der Figur (ϕ_i, ψ_j) den Index $m_i + n_j$, so gilt

$$\sum_{\boldsymbol{F}_1 \times \boldsymbol{F}_2} z^{m_i + n_j} = \left(\sum_{\boldsymbol{F}_1} z^{m_i}\right)\left(\sum_{\boldsymbol{F}_2} z^{n_j}\right)$$

d. h. die Figurenmenge $\boldsymbol{F} = \boldsymbol{F}_1 \times \boldsymbol{F}_2$ hat die abzählende Potenzreihe

$$\varphi(z) = \varphi_1(z) \cdot \varphi_2(z) .$$

Daraus kann man den folgenden Satz über abzählende Potenzreihen entnehmen.

Satz: *Haben die Figurenmengen $\boldsymbol{F}_1$ und $\boldsymbol{F}_2$ die abzählenden Potenzreihen $\varphi_1(z)$ und $\varphi_2(z)$ und ist der Index der Figuren bei der Paarbildung additiv, dann hat die Figurenmenge $\boldsymbol{F}_1 \times \boldsymbol{F}_2$ die abzählende Potenzreihe $\varphi_1(z) \cdot \varphi_2(z)$.*
Der Satz sei anschliessend an einem Beispiel illustriert.

Aufgabe: Zu einem gewissen Zeitpunkt hat die Schweizerische Postverwaltung 5 verschiedene 10er Marken, 3 verschiedene 20er Marken, eine 30er Marke und zwei verschiedene 50er Marken im Verkehr. Auf wie viele Arten kann man ein Ausland-Briefporto von 50 Rappen zusammenstellen, wenn von der Art des Aufklebens der Marken abgesehen wird?

Es stehen insgesamt 11 Sorten Briefmarken zur Verfügung. Mit der k-ten Markenart bilde man dann die Figurenmenge

$$\boldsymbol{B}_k = \{-, \boxed{k}, \boxed{k}\boxed{k}, \boxed{k}\boxed{k}\boxed{k}, \ldots\} .$$

Hat die zugrunde liegende Marke den Frankatur-Wert $10n_k$, dann gehört zur Menge $\boldsymbol{B}_k$ die abzählende Potenzreihe

$$\beta_k(z) = 1 + z^{n_k} + z^{2n_k} + \cdots = \frac{1}{1 - z^{n_k}} .$$

Die Menge aller möglichen Frankaturen mit den 11 Markenarten ist

$$\boldsymbol{B} = \boldsymbol{B}_1 \times \boldsymbol{B}_2 \times \cdots\cdots \times \boldsymbol{B}_{10} \times \boldsymbol{B}_{11} .$$

Dabei ist die Annahme getroffen, dass jede Markenart unbeschränkt zur Verfügung steht. Da der Index (Frankatur-Wert) additiv ist, lässt sich unser Satz über abzählende Potenzreihen anwenden. Man erhält für die abzählende Potenzreihe der Menge $\boldsymbol{B}$

$$\beta(z) = \left(\frac{1}{1-z}\right)^5 \left(\frac{1}{1-z^2}\right)^3 \left(\frac{1}{1-z^3}\right) \left(\frac{1}{1-z^5}\right)^2 .$$

Unter Berücksichtigung von

$$\left(\frac{1}{1-z^k}\right)^s = \sum_{j=0}^{\infty} \binom{s-1+j}{s-1} z^{j \cdot k}$$

können die ersten Glieder von $\beta(z)$ leicht erhalten werden:

$$\beta(z) = (1 + 5z + 15z^2 + 35z^3 + 70z^4 + 126z^5 + \ldots)\,(1 + 3z^2 + 6z^4 + \ldots)$$
$$\times\,(1 + z^3 + \ldots)\,(1 + 2z^5 + \ldots) = 1 + 5z + 18z^2 + 51z^3 + 126z^4 + 281z^5 + \ldots .$$

In unserer Aufgabenstellung ist nach der Anzahl der Figuren in $\boldsymbol{B}$ vom Index 5 gefragt. Aus der abzählenden Potenzreihe $\beta(z)$ liest man die Anzahl 281 heraus. Es gibt also bei den 11 verfügbaren Markenarten 281 verschiedene Frankaturen im Wert von 50 Rappen.

3. Abzählung der normierten irreduziblen Polynome über GF(p)

Es sei $\boldsymbol{F}^{(n)}$ die Menge der genormten irreduziblen Polynome n-ten Grades über $GF(p)$:

$$\mathbf{F}^{(n)} = \{\Phi_1^{(n)}, \Phi_2^{(n)}, \ldots, \Phi_{f_n}^{(n)}\}$$

Der Figur $\Phi_j^{(n)}$ ordnen wird den Grad n als Index zu. Mit einer Figur $\Phi^{(n)} \in \boldsymbol{F}^{(n)}$ bilden wir nun die Figurenmenge

$$\boldsymbol{F}_j^{(n)} = \{-, \Phi_j^{(n)}, \Phi_j^{(n)}\Phi_j^{(n)}, \Phi_j^{(n)}\Phi_j^{(n)}\Phi_j^{(n)}, \ldots\}$$

Dazu gehört offenbar die abzählende Potenzreihe

$$\varphi_j^{(n)}(z) = 1 + z^n + z^{2n} + \cdots = \frac{1}{1 - z^n}; \qquad 1 \leq j \leq f_n .$$

Nun ist

$$\boldsymbol{F} = \boldsymbol{F}_1^{(1)} \times \boldsymbol{F}_2^{(1)} \times \cdots \times \boldsymbol{F}_{f_1}^{(1)} \times \boldsymbol{F}_1^{(2)} \times \boldsymbol{F}_2^{(2)} \cdots \times \boldsymbol{F}_{f_2}^{(2)} \times \boldsymbol{F}_1^{(3)} \times \cdots .$$

die Menge aller genormten Polynome über $GF(p)$. Da bei der Multiplikation zweier Polynome der Grad additiv ist, kann unser Satz über abzählende Potenzreihen angewendet werden. Man schliesst daraus für die abzählende Potenzreihe von $\boldsymbol{F}$

$$\varphi(z) = \left(\frac{1}{1 - z}\right)^{f_1} \left(\frac{1}{1 - z^2}\right)^{f_2} \left(\frac{1}{1 - z^3}\right)^{f_3} \cdots .$$

Nun gibt es aber genau p^n genormte Polynome vom Grad n, denn in

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

kann jeder Koeffizient p verschiedene Werte annehmen. Es ist daher zugleich

$$\varphi(z) = 1 + pz + p^2 z^2 + \cdots = \frac{1}{1 - pz} .$$

Die beiden Darstellungen für $\varphi(z)$ lassen nun die Beziehung

$$\prod_{n=1}^{\infty} \left(\frac{1}{1 - z^n}\right)^{f_n} = \frac{1}{1 - pz} \tag{1}$$

entnehmen, aus der die Zahlen f_n bestimmt werden können. Zunächst sei noch darauf hingewiesen, dass das unendliche Produkt auf der linken Seiten von (1) definiert ist. Man kann sich leicht überlegen, dass eine *multiplizierbare Familie von formalen Potenzreihen* vorliegt.

Zur weitern Vereinfachung gehen wir vorerst zu den reziproken Reihen über:

$$\prod_{n=1}^{\infty} (1 - z^n)^{f_n} = 1 - pz .$$

Leitet man beidseitig logarithmisch ab, so folgt

$$\sum_{n=1}^{\infty} \frac{n \cdot f_n}{1 - z^n} z^{n-1} = \frac{p}{1 - pz} . \tag{2}$$

Aus (2) können jetzt die Zahlen f_n viel einfacher gewonnen werden. Um die in (2) verborgene Bindung zwischen den Zahlen f_n besser erkennen zu können, schreiben wir die linke Seite von (2) aus; sie lautet

$$\begin{array}{lllllllllll}
f_1 + f_1 z + f_1 z^2 + f_1 z^3 + f_1 z^4 + f_1 z^5 + f_1 z^6 + f_1 z^7 + f_1 z^8 + f_1 z^9 & + \dots \\
\quad + 2f_2 z & + 2f_2 z^3 & + 2f_2 z^5 & + 2f_2 z^7 & + 2f_2 z^9 + \dots \\
\qquad + 3f_3 z^2 & & + 3f_3 z^5 & & + 3f_3 z^8 & + \dots \\
\qquad\quad + 4f_4 z^3 & & & + 4f_4 z^7 & & + \dots \\
\qquad\qquad + 5f_5 z^4 & & & & + 5f_5 z^9 + \dots \\
\qquad\qquad\quad + 6f_6 z^5 & & & & & + \dots \\
\qquad\qquad\qquad + 7f_7 z^6 & & & & & + \dots
\end{array}$$

Hierbei zeichnet sich deutlich ab, dass eine *summierbare Familie von formalen Potenzreihen* vorliegt; die unendliche Summe auf der linken Seiten von (2) hat also einen Sinn.

Addiert man nun kolonnenweise, so folgt

$$\sum_{n=1}^{\infty} \left(\sum_{t/n} t\, f_t \right) z^{n-1} = \sum_{n=1}^{\infty} p^n z^{n-1} .$$

Man schliesst daraus auf die Beziehung

$$\sum_{t/n} t \cdot f_t = p^n \tag{3}$$

aus der sich die f_n sukzessive bestimmen lassen. Wir wollen aber gleich zu einer expliziten Formel für die Zahlen f_n vorstossen.

Zur Auflösung von (3) nach den Zahlen f_n benötigen wir die sogenannte *Möbiusfunktion*, die wie folgt definiert ist:

$$\mu(n) \overset{def}{=} \begin{cases} 1 & \text{für } n = 1 \\ (-1)^r & \text{für } n = p_1 p_2 \dots p_r;\ \text{die } p_i \text{ sind verschiedene Primzahlen} \\ 0 & \text{sonst.} \end{cases}$$

Sind $g(n)$ und $h(n)$ beliebige Funktionen auf der Menge der natürlichen Zahlen, die der Beziehung

$$\sum_{t/n} g(t) = h(n)$$

genügen, dann gilt bekanntlich die Umkehrung

$$g(n) = \sum_{t/n} \mu(t)\ h\left(\frac{n}{t}\right).$$

Es ist daher

$$n\, f_n = \sum_{t/n} \mu(t)\, p^{n/t}$$

oder

$$f_n = \frac{1}{n} \sum_{t/n} \mu(t)\, p^{n/t}\,. \tag{4}$$

Die Formel (4) liefert für den Anfang der f_n-Folge die Terme

$$f_1 = p;\; f_2 = \frac{1}{2}\,(p^2 - p);\; f_3 = \frac{1}{3}\,(p^3 - p)\;;\; f_4 = \frac{1}{4}\,(p^4 - p^2)\;;$$

$$f_5 = \frac{1}{5}\,(p^5 - p)\;;\; f_6 = \frac{1}{6}\,(p^6 - p^3 - p^2 + p)\,.$$

Ist n eine Primzahl, dann gilt allgemein $f_n = \frac{1}{n}\,(p^n - p)$.

Aus der Formel (4) kann jetzt auch entnommen werden, dass $f_n \geq 1$ für alle n; es gibt also zu jedem vorgegebenen Grad mindestens ein irreduzibles Polynom. Die Summe

$$\sum_{t/n} \mu(t)\, p^{n/t}$$

ist nämlich ein Polynom n-ten Grades in p mit lauter Koeffizienten aus der Menge $\{-1, 0, +1\}$:

$$\sum_{t/n} \mu(t)\, p^{n/t} = p^m\,(p^{n-m} + \ldots \pm 1)$$

Betrachtet man das entsprechende Polynom in der reellen Variablen ξ, also

$$\xi^m\,(\xi^{n-m} + \ldots \pm 1)$$

so hat dieses allfällige ganzzahlige Nullstellen in $\xi = 0$ und $\xi = \pm 1$. Da sämtliche Primzahlen ausserhalb der Menge $\{-1, 0, +1\}$ liegen, ist $f_n \geq 1$ für alle $n \in \boldsymbol{N}$.

Im Hinblick auf die Gewinnung des Galois-Feldes $GF(p^n)$ interessiert natürlich nur die Anzahl der irreduziblen Polynome n-ten Grades über $GF(p)$. Es sei aber darauf hingewiesen, dass mit derselben Überlegung auch die Anzahl der irreduziblen Polynome n-ten Grades über $GF(p^r)$ erhalten werden kann. Sie beträgt

$$f_n^{(r)} = \frac{1}{n} \sum_{t\,|\,n} \mu(t)\, p^{n\,r/t};\quad f_n^{(1)} = f_n\,.$$

Man gelangt zu dieser Beziehung, wenn man in (4) p durch p^r ersetzt.

Diese Ergänzung verdanke ich E. Trost, der mich zugleich auch auf einige interessante Literaturstellen aufmerksam gemacht hat.

M. Jeger, Zürich

LITERATURVERZEICHNIS

[1] S. I. Borevicz und I. R. Šafarevič: Zahlentheorie. Basel 1966 (p. 431).
[2] L. E. Dickson: Linear Groups with an exposition of the Galois Field Theory. New York 1958
[3] M. Hall, *Combinatorial Theory*, Waltham, Massachusetts 1967.
[4] G.H. Hardy, and E.M. Wright, *Einführung in die Zahlentheorie*, München 1958.
[5] I. Niven, *Formal Power Series*, Am. math. Mon. *76*, 1969.
[6] G. Polya, *On Picture-Writing*, Am. math. Mon. *63*, 1956.