Ganzzahlige Funktionen natürlicher Zahlen

Autor(en): **Gruenberg, Karl W.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **50 (1995)**

PDF erstellt am: **19.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-46343

El. Math. *50* (1995)

0013-6018/95/020065-11$1.50 + 0.20/0

Ganzzahlige Funktionen natürlicher Zahlen

Karl W. Gruenberg

Karl Gruenberg wurde 1928 in Wien geboren. Er studierte an der Universität in Cambridge, wo er bei Philip Hall mit einer Arbeit über unendliche Gruppen promovierte. Von 1953 bis 1993 war er am Queen Mary College (heute Queen Mary and Westfield College) der University of London tätig, zuerst als Lecturer, später als Professor. In seinen Forschungsarbeiten beschäftigt er sich vor allem mit der Gruppentheorie, insbesondere mit der Cohomologie-Theorie und mit der ganzzahligen Darstellungstheorie. Seine vielfältigen Interessen erstrecken sich ausserdem auf die bildende Kunst, besonders die Architektur, auf das Theater und auf die Musik. In seiner Freizeit gehören Bergwanderungen zu seinen liebsten Beschäftigungen.

Funktionen, die natürlichen Zahlen ganze Zahlen zuordnen, scheinen auf den ersten Blick einfache mathematische Objekte zu sein, die wenig Interesse verdienen. Wenn man sich damit etwas näher beschäftigt, wird aber gleich klar, dass die Behandlung nicht so einfach ist und dass sich schon hinter den einfachsten solchen Funktionen ganz Interessantes verstecken kann. Dies lässt sich durch das folgende Beispiel illustrieren. Einer Funktion ϕ von den natürlichen Zahlen in die ganze Zahlen kann die Potenzreihe $\sum_{n=0}^{\infty} a_n x^n$ mit $a_n = \phi(n)$ zugeordnet werden. Man nennt sie die *Poincaré-Reihe* der Funktion ϕ. Zur trivialen und deshalb uninteressanten Funktion, die jeder natürlichen Zahl die ganze Zahl 1 zuordnet, gehört die Poincaré-Reihe $\sum_{n=0}^{\infty} x^n$. Man erkennt die geometrische Reihe mit Faktor x, welche im Intervall $(-1, 1)$ die Funktion $x \mapsto 1/(1-x)$ darstellt: Unbestreitbar ein interessantes mathematisches Objekt.

Der vorliegende Beitrag beginnt mit der Behandlung einiger Fragen, zu welchen der Übergang von der Funktion ϕ zur zugehörigen Poincaré-Reihe Anlass gibt. Es liegt nahe, zuerst Funktionen zu betrachten, die polynomial definiert sind. Eine Funktion ϕ heisst polynomial definiert, wenn es ein rationales Polynom $f(X)$ gibt mit $\phi(n) = f(n)$ für $n = 0, 1, 2, \ldots$ Es stellt sich unmittelbar die folgende elementare Frage:

Wie sehen die rationalen Polynome aus, deren Werte auf allen natürlichen Zahlen ganzzahlig sind?

Eine interessante und überraschende Antwort erwartet den Leser (siehe Satz 1). Polynomial definierte Funktionen ϕ besitzen offensichtlich höchstens polynomiales Wachstum:

es ist $\phi(n)$ für alle n durch eine feste Potenz von n beschränkt. Es stellt sich dann die Frage:

Es sei ϕ polynomial definiert oder, allgemeiner, es besitze ϕ polynomiales Wachstum. Was für Funktionen werden durch die Poincaré-Reihen solcher ϕ dargestellt?

Die Antworten auf diese zweite Frage sind nicht mehr so einfach und eindeutig. Mit ganz elementaren Methoden lassen sich aber auch hier interessante und überraschende Aussagen gewinnen (Sätze 2, 3 und 4).

Es gibt viele konkrete mathematische Situationen, die in natürlicher Weise zu einer ganzahligen Funktion natürlicher Zahlen Anlass geben. Die Erfahrung zeigt, dass diese Funktionen nicht selten die speziellen Eigenschaften aufweisen, von denen oben die Rede war. Die zugehörige Poincaré-Reihe kann dann wesentliche Erkenntnisse über die zugrunde liegende mathematische Situation liefern.

Der Beitrag von Karl Gruenberg beginnt mit der Darstellung derartiger konkreter mathematischer Situationen. Für diesen Teil des Beitrages sind einige Kenntnisse der entsprechenden Gebiete von Vorteil. Der anschliessende Teil, in dem die oben beschriebenen Fragestellungen mit elementaren Methoden behandelt werden, ist direkt zugänglich.

Eine englische Fassung dieses Artikels ist 1989 in der Zeitschrift *Mathematical Medley* erschienen. Die *Elemente der Mathematik* danken der *Singapore Mathematical Society* für die freundliche Erlaubnis zur Veröffentlichung dieser leicht erweiterten deutschen Version. *ust*

Wir werden uns in diesem Beitrag mit der Menge **X** der Funktionen ϕ beschäftigen, die auf den nichtnegativen ganzen Zahlen definiert sind und Werte in den ganzen Zahlen annehmen. Die Ringstruktur der ganzen Zahlen induziert in folgender natürlicher Weise eine Ringstruktur in **X**:

$$(\phi + \psi)(n) = \phi(n) + \psi(n) \quad \text{und} \quad (\phi \cdot \psi)(n) = \phi(n) \cdot \psi(n) \ .$$

Die konstante Funktion, die überall den Wert 1 annimmt, ist das Einselement von **X**. Solche Funktionen kommen in allen Gebieten der Mathematik vor. Ihre Wichtigkeit leitet sich daraus her, dass sie in vielen Fällen gerade die wesentlichen Informationen über die Situation enthalten, aus der sie konstruiert worden sind. Ich will hier drei illustrative Beispiele herausgreifen, und da ich ein Algebraiker bin, stammen sie alle aus dem Gebiet der Algebra.

1. Es sei R ein kommutativer Noetherscher lokaler Ring. "Noethersch" bedeutet, dass R die Maximalbedingung für Ideale erfüllt, und "lokal" heisst, dass R genau ein maximales Ideal besitzt. Wir bezeichen dieses maximale Ideal mit I. Für eine Primzahl p ist z.B. der Ring $\mathbb{Z}_{(p)}$, der aus allen rationalen Zahlen a/b mit $p \nmid b$ besteht, ein derartiger kommutativer Noetherscher lokaler Ring; das maximale Ideal I von $\mathbb{Z}_{(p)}$ ist $p \cdot \mathbb{Z}_{(p)}$. Da I maximal ist, ist R/I ein Körper, den wir mit K bezeichnen wollen. Wegen der Noetherschen Eigenschaft ist jedes I^r als Ideal endlich erzeugt. Deshalb ist I^r/I^{r+1} ein

endlichdimensionaler Vektorraum über K. Durch die Festsetzung $r \mapsto \dim_K I^r/I^{r+1}$ wird also eine Funktion in **X** definiert.

2. Es sei G eine endlich erzeugte Gruppe; und S sei eine endliche Erzeugendenmenge von G. Dann kann jedes Element $g \in G$ in der Form $g = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}$ mit $s_i \in S$ und $\epsilon_i = \pm 1$ ausgedrückt werden. Wir nennen n die Länge dieses Ausdruckes. Natürlich lässt sich unser Element g im allgemeinen durch viele verschiedene solche Ausdrücke beschreiben, so dass n durch das Element g nicht bestimmt ist. Für jede nichtnegative ganze Zahl sei $G(n)$ die Menge aller Elemente $g \in G$, die durch einen Ausdruck der Länge $\leq n$ beschrieben werden können. Da S endlich ist, ist $G(n)$ endlich, und wir schreiben $l(n)$ für die Mächtigkeit von $G(n)$. Mit l ist eine Funktion in **X** definiert.

3. Es seien K ein Körper, G eine endliche Gruppe und A ein endlich erzeugter KG-Modul. Wir wählen eine *endlich erzeugte projektive Resolution* von A über KG:

$$\cdots \to P_{i+1} \to P_i \to \cdots \to P_1 \to P_0 \to A \to 0 \,. \tag{1}$$

Dies bedeutet, dass jedes P_i ein endlich erzeugter projektiver KG-Modul ist und dass (1) eine exakte Folge von Moduln und Modulhomomorphismen ist. Eine Folge heisst dabei exakt, wenn an jeder Stelle das Bild des ankommenden Pfeiles gleich dem Kern des weggehenden Pfeiles ist. Da G endlich ist, ist jeder endlich erzeugte KG-Modul insbesondere ein endlichdimensionaler Vektorraum über K. Deshalb definiert $n \mapsto \dim_K P_n$ eine Funktion in **X**.

Wir werden später auf diese drei Beispiele noch einmal zurückkommen. Aber zuvor wollen wir einige allgemeine Bemerkungen über unseren Ring **X** machen.

Die einfachsten Funktionen, die in **X** liegen, sind diejenigen, die *polynomial definiert* werden können. Wir sagen, dass ϕ polynomial definiert ist, wenn es ein Polynom $f(X) \in \mathbb{Q}[X]$ gibt mit $\phi(n) = f(n)$ für alle $n \geq 0$. Man beachte dabei, dass $f(X)$ nicht notwendigerweise ganzzahlige Koeffizienten haben muss. Dies wird illustriert durch das folgende Beispiel. Für jede positive ganze Zahl k nimmt das sogenannte binomiale Polynom

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}$$

für alle ganzzahligen Argumente nur ganzzahlige Werte an. Wenn **P** die Menge aller polynomial definierten Funktionen bezeichnet, dann ist **P** ein Unterring von **X**. Wir behaupten jetzt, dass jede Funktion in **P** additiv aus den binomialen Polynomen $\binom{X}{k}$, $k \geq 0$, zusammengesetzt werden kann. Dabei setzen wir $\binom{X}{0} = 1$.

Satz 1. *Die Polynome* $\binom{X}{k}$ *für* $k \geq 0$ *bilden eine* $\mathbb{Q}$*-Basis von* $\mathbb{Q}[X]$, *und sie erzeugen additiv die Gruppe* **P**.

Beweis: Die Basiseigenschaft folgt mit Induktion nach dem Grad, denn es gilt

$$\binom{X}{k} = \frac{X^k}{k!} + g(X) \,,$$

wobei der Grad von $g(X)$, wir bezeichnen ihn mit $\deg g$, echt kleiner ist als k. Wir beweisen die zweite Behauptung ebenfalls mit Induktion nach dem Grad. Es sei $\phi \in \mathbf{P}$ durch das Polynom $f(X)$ gegeben. Nach dem ersten Teil des Satzes gilt

$$f(X) = \sum_{k=0}^{r} a_k \binom{X}{k}$$

mit $a_k \in \mathbb{Q}$. Wir müssen beweisen, dass jedes a_k eine ganze Zahl ist. Für ein beliebiges Polynom $g(X)$ sei

$$\delta g(X) = g(X+1) - g(X) .$$

Dann gilt $\delta\binom{X}{k} = \binom{X}{k-1}$ und deshalb

$$\delta f(X) = \sum_{k=1}^{r} a_k \binom{X}{k-1} .$$

Nun hat δf einen kleineren Grad als f und nimmt wie dieses auf den nichtnegativen ganzen Zahlen ganzzahlige Werte an. Deshalb gilt nach Induktion, dass die Koeffizienten $a_1, a_2, \ldots, a_r$ ganzzahlig sind. Wegen

$$a_0 = f(X) - \sum_{k=1}^{r} a_k \binom{X}{k}$$

und da die rechte Seite nur ganzzahlige Werte annimmt, ist also auch a_0 ganzzahlig.

Polynomial definierte Funktionen treten in den Anwendungen, die wir im Auge haben, nur selten auf. Eine geringfügige Verallgemeinerung führt aber zu einer Klasse von Funktionen, die häufig auftreten. Es sei q eine positive ganze Zahl. Wir sagen die Funktion $\phi \in \mathbf{X}$ sei *polynomial auf den Restklassen* mod q, oder kurz "PORC mod q"[1]), wenn Polynome $f_0(X), f_1(x), \ldots, f_{q-1}(X) \in \mathbb{Q}[X]$ existieren, so dass für jedes $0 \leq r < q$ und jedes $n \in \mathbb{Z}$ gilt

$$\phi(nq + r) = f_r(n).$$

Man beachte, dass die polynomial definierten Funktionen PORC mod 1 sind.

Wir sagen, zwei Funktionen ϕ, ψ seien *letztlich gleich*, falls eine ganze Zahl N existiert, so dass für $n \geq N$ stets $\phi(n) = \psi(n)$ gilt; wir bezeichen dies mit $\phi \sim \psi$. Die Funktion ϕ heisst *letztlich* PORC mod q, falls eine PORC mod q Funktion ψ existiert mit $\phi \sim \psi$.

Jeder Funktion $\phi \in \mathbf{X}$ können wir eine formale Potenzreihe

$$P(\phi, X) = \sum_{n \geq 0} \phi(n) X^n$$

zuordnen. Diese wird *Poincaré-Reihe* von ϕ genannt. Zwei Funktionen sind genau dann letztlich gleich, wenn die Differenz der zugehörigen Poincaré-Reihen ein ganzzahliges Polynom ist. Die Poincaré-Reihe einer PORC Funktion hat eine besonders einfache Form:

1) PORC ist eine Abkürzung für "**p**olynomial **o**n **r**esidue **c**lasses"

Satz 2. *Die Funktion ϕ ist genau dann letztlich* PORC mod q, *wenn ein ganzzahliges Polynom $g(X)$ und eine positive ganze Zahl t existieren, so dass die Poincaré-Reihe $P(\phi, X)$ von der Form*

$$P(\phi, X) = \frac{g(X)}{(1 - X^q)^t}$$

ist.

Beweis: Laut Voraussetzung gibt es zu ϕ eine PORC mod q Funktion ψ mit $\phi \sim \psi$. Es seien $f_0, f_1, \ldots, f_{q-1}$ die zu ψ gehörigen Polynome. Es genügt zu zeigen, dass die Poincaré-Reihe $P(\psi, X)$ die verlangte Form hat. Es gilt

$$\begin{aligned} P(\psi, X) &= \sum_{m \geq 0} \psi(m) X^m \\ &= \sum_{r=0}^{q-1} \sum_{n \geq 0} \psi(nq + r) X^{nq+r} \\ &= \sum_{r=0}^{q-1} X^r \left(\sum_{n \geq 0} f_r(n) X^{nq} \right) . \end{aligned}$$

Wir weisen jetzt nach, dass $\sum_{n \geq 0} f_r(n) X^{nq}$ für jedes r die verlangte Form hat. Dann hat natürlich auch $P(\psi, X)$ die verlangte Form. Nach Satz 1 gilt

$$f_r(X) = \sum_{i=0}^{d} a_i \binom{X}{i} ,$$

mit $a_i \in \mathbb{Z}$ und $\deg f_r = d$. Es bleibt deshalb nur zu zeigen, dass für jedes i das Polynom

$$\sum_{n \geq 0} \binom{n}{i} X^{nq}$$

die verlangte Form hat. Wir haben

$$\frac{1}{(1 - X^k)^s} = \sum_{n \geq 0} \binom{-s}{n} (-X^k)^n$$

und

$$\begin{aligned} \binom{-s}{n} &= (-1)^n \frac{s(s+1) \cdots (s+n-1)}{n!} \\ &= (-1)^n \frac{(n+s-1)!}{n!(s-1)!} \\ &= (-1)^n \binom{n+s-1}{s-1} . \end{aligned}$$

Deshalb gilt

$$\frac{1}{(1-X^k)^s} = \sum_{n\geq 0} \binom{n+s-1}{s-1} X^{kn} . \tag{2}$$

Wegen $\binom{n}{i} = 0$ für $n < i$ folgt daraus

$$\sum_{n\geq 0} \binom{n}{i} X^{nq} = \sum_{m\geq 0} \binom{m+i}{i} X^{mq+iq} = \frac{X^{iq}}{(1-X^q)^{i+1}} .$$

Dies war zu zeigen.

Nehmen wir umgekehrt an, dass $P(\phi, X)$ von der Form

$$P(\phi, X) = \frac{g(X)}{(1-X^q)^t}$$

ist, so gilt nach Formel (2)

$$\frac{1}{(1-X^q)^t} = \sum_{n\geq 0} \binom{n+t-1}{t-1} X^{nq} .$$

Die Koeffizientenfunktionen sind offensichtlich PORC mod q; die zugehörigen Polynome sind

$$\binom{X+t-1}{t-1}, \ 0, \ 0, \ldots, \ 0 .$$

Wir betrachten nun zuerst den Spezialfall, wo $g(X)$ ein ganzzahliges Polynom mit $\deg g < q$ ist. Es sei also

$$g(X) = \sum_{i=0}^{q-1} b_i X^i .$$

Dann gilt

$$\frac{g(X)}{(1-X^q)^t} = \sum_{i=0}^{q-1} \sum_{n\geq 0} \binom{n+t-1}{t-1} b_i X^{qn+i} .$$

Dies ist aber offensichtlich die Poincaré-Reihe einer PORC mod q Funktion mit Polynomen

$$b_i \binom{X+t-1}{t-1} , \quad 0 \leq i < q .$$

Im allgemeinen Fall schreiben wir $g(X)$ in der Form

$$g(X) = \sum_{i\geq 0} g_i(X)(1-X^q)^i$$

mit $\deg g_i < q$. Dann folgt

$$\frac{g(X)}{(1-X^q)^t} = h(X) + \sum_{i=0}^{t-1} \frac{g_i(X)}{(1-X^q)^{t-i}} . \tag{3}$$

Wie wir oben gezeigt haben, ist die Koeffizientenfunktion des zweiten Terms auf der rechten Seite von (3) PORC mod q. Deshalb ist die linke Seite dieser Gleichung letztlich PORC mod q. Damit ist Satz 2 vollständig bewiesen.

Wir fügen zusätzlich noch an, dass aus unserem Beweis folgt, dass für t in Satz 2 die ganze Zahl $1+d$ mit

$$d = \max(\deg f_0, \deg f_1, \ldots, \deg f_{q-1})$$

genommen werden kann.

Funktionen, die letztlich PORC sind, wachsen nur polynomial. Wir sagen, dass die Funktion ϕ *polynomiales Wachstum* $c \geq 0$ aufweist, wenn eine positive reelle Zahl a und eine positive ganze Zahl N existieren, so dass für $n \geq N$ stets die Ungleichung $|\phi(n)| \leq an^{c-1}$ erfüllt ist, und wenn c die kleinste solche ganze Zahl ist.

Satz 3. *Die Funktion $\phi \in \mathbf{X}$ sei letztlich* PORC mod q. *Es seien $f_0, f_1, \ldots, f_{q-1}$ die zugehörigen Polynome und es sei d das Maximum ihrer Grade. Dann hat ϕ polynomiales Wachstum $d+1$.*

Beweis: Wir nehmen an, dass für $n \geq N$ die Funktion ϕ PORC mod q sei. Für $n \geq N$ und $n = kq + r$ gilt dann

$$|\phi(n)| = |f_r(k)| \leq \left(\sum_{i=0}^{d_r} |a_i| \right) k^{d_r}$$

mit $f_r(X) = \sum_{i=0}^{d_r} a_i X^i$. Wir setzen $\sum_{i=0}^{d_r} |a_i| = A_r$ und definieren $a = \max(A_0, A_1, \ldots, A_{q-1})$. Dann folgt $|\phi(n)| \leq an^d$ für alle $n \geq N$.

Es sei umgekehrt $|\phi(n)| \leq an^{c-1}$ für alle $n \geq N$, und es sei d der Grad von f_r. Dann folgt

$$|f_r(k)| = |\phi(kq+r)| \leq a(kq+r)^{c-1}$$

für alle $k \geq K$, K genügend gross. Für $g(X) = a(qX+r)^{c-1}$ gilt $\deg g = c-1$ und $|f_r(k)| \leq g(k)$ für alle $k \geq K$. Dies impliziert $\deg f_r \leq \deg g$, und folglich $d \leq c-1$. Damit ist Satz 3 vollständig bewiesen.

Die Umkehrung von Satz 3 ist falsch. Ein Gegenbeispiel ist gegeben durch die folgende Funktion:

$$\phi(n) = \begin{cases} 0 & \text{falls } n \text{ eine Primzahl ist,} \\ n & \text{sonst.} \end{cases}$$

Es gilt $\phi(n) \leq n^{2-1}$, so dass ϕ von polynomialem Wachstum 2 ist. Wäre aber ϕ für $n \geq N$ PORC mod q mit Polynomen $f_0, f_1, \ldots, f_{q-1}$, so hätte man für $qk + r \geq N$

$$f_r(k) = \phi(qk+r).$$

Die rechte Seite wäre also 0, wenn $qk+r$ eine Primzahl ist. Nun gibt es aber nach dem berühmten Theorem von Dirichlet in $q\mathbb{Z}+r$ unendlich viele Primzahlen. Deshalb müsste $f_r(X)$ unendlich viele Nullstellen besitzen, was offensichtlich unmöglich ist.

Nichtsdestoweniger kann eine Umkehrung von Satz 3 erhalten werden, wenn man die Bedingung hinzufügt, dass die Poincaré-Reihe von ϕ rational ist, also die Form $g(X)/f(X)$ hat, wo $g(X)$, $f(X)$ Polynome mit Koeffizienten in $\mathbb{Q}$ sind. Den folgenden Satz verdanke ich Fritz Grunewald.

Satz 4. *Die Funktion $\phi \in \mathbf{X}$ habe polynomiales Wachstum, und es sei $P(\phi, X)$ eine rationale Funktion. Dann ist ϕ letztlich* PORC.

Beweis: Laut Voraussetzung hat man $P(\phi, X) = \lambda \cdot g(X)/f(X)$ mit $\lambda \in \mathbb{Q}$ und $g(X)$, $f(X) \in \mathbb{Z}[X]$. Ferner darf man annehmen, dass g und f in $\mathbb{Q}[X]$ teilerfremd sind. Wir müssen zeigen, dass $P(\phi, X)$ die in Satz 2 angegebene Form hat. Natürlich genügt es nachzuweisen, dass $g(X)/f(X)$ diese Form hat. Das letztere ist aber offenbar genau dann der Fall, wenn jede Nullstelle von $f(X)$ eine Einheitswurzel ist.

Da g und f teilerfremd sind, existieren u, v in $\mathbb{Q}[X]$ mit $fu+gv = 1$. Multipliziert man diese Gleichung mit einer geeigneten ganzen Zahl d, so erhält man $hf + kg = d$ mit $h, k \in \mathbb{Z}[X]$. Damit können wir $e = h+k\cdot(g/f)$ als formale Potenzreihe mit ganzzahligen Koeffizienten schreiben, wobei $e(X)f(X) = d$ gilt. Ist p ein Primteiler von d, so folgt $e(X)f(X) \equiv 0 \pmod{p}$, und daher $e \equiv 0$ oder $f \equiv 0$, weil der Potenzreihenring $\mathbb{F}_p[[X]]$ ein Integritätsbereich ist. Daher sind alle Koeffizienten von e oder alle Koeffizienten von f durch p teilbar. Führen wir dieses Verfahren der Reihe nach mit allen Primteilern von d durch, so erhalten wir Polynome $e_1(X) = \frac{1}{m}e(X)$ und $f_1(X) = \frac{1}{n}f(X)$ in $\mathbb{Z}[X]$ mit $mn = d$. Daraus folgt $e_1(X)f_1(X) = 1$. Ist $f_1(X) = a_0 + a_1x + \cdots + a_nX^n$, dann sind alle $a_i \in \mathbb{Z}$ und $a_0 = \pm 1$.

Es bezeichne nun ρ den Konvergenzradius der Potenzreihe g/f; es ist also

$$\frac{1}{\rho} = \limsup_{n\to\infty} \sqrt[n]{\left|\frac{1}{\lambda}\phi(n)\right|}\,.$$

Da ϕ polynomiales Wachstum hat, existieren eine positive reelle Zahl a und positive ganze Zahlen b, N mit

$$\left|\frac{1}{\lambda}\phi(n)\right| \leq an^b$$

für $n \geq N$. Wir haben also

$$\sqrt[n]{\left|\frac{1}{\lambda}\phi(n)\right|} \leq (an^b)^{\frac{1}{n}}$$

für $n \geq N$. Aus $(an^b)^{\frac{1}{n}} \to 1$ für $n \to \infty$ folgt $1/\rho \leq 1$, und daher $\rho \geq 1$. Dies besagt, dass g/f in $|z| \leq 1$ keine Pole besitzt. Daher hat auch

$$\frac{1}{f_1} = e_1 = \frac{1}{m}\left(h + k\cdot\frac{g}{f}\right)$$

keine Pole in $|z| \leq 1$. Das Polynom f_1 besitzt deshalb in $|z| < 1$ keine Nullstellen. Ist nun ζ eine Nullstelle von f_1, so ist $1/\zeta$ eine Nullstelle von

$$a_n + a_{n-1}X + \cdots + a_1 X^{n-1} \pm X^n ,$$

und es gilt $|1/\zeta| \leq 1$. Daraus folgt $a_n = \pm 1$. Alle Nullstellen haben deshalb notwendigerweise den absoluten Betrag 1 und sind ganze algebraische Zahlen. Aus einem Satz von Kronecker folgt dann, dass sie Einheitswurzeln sein müssen. Damit ist der Satz 4 bewiesen.

Wir kehren nun zu unseren drei Beispielen zurück.

1. Wir rufen in Erinnerung, dass der Ring R ein einziges maximales Ideal I hat und dass unsere Funktion durch $\phi(n) = \dim_K I^n/I^{n+1}$ gegeben ist. Das grundlegende Resultat in diesem Zusammenhang ist wie folgt: *Die zu ϕ gehörige Poincaré-Reihe ist durch die Formel*

$$P(\phi, X) = \frac{g(x)}{(1-X)^t}$$

gegeben. Dabei können wir nach Kürzungen annehmen, dass $1 - X$ kein Faktor von $g(X)$ ist. Die hier auftretende ganze Zahl t ist dabei gerade die ringtheoretisch wichtige *Krull-Dimension* des lokalen Ringes R (also das Supremum der Längen von Ketten von Primidealen im Ring R). Es folgt aus unseren früheren Überlegungen, dass die Funktion ϕ letztlich polynomial ist; das zugehörige Polynom heisst das *Hilbert-Polynom* des Ringes. Im Beispiel $R = \mathbb{Z}_{(p)}$ gilt $P(\phi, X) = 1/(1-X)$, und das Hilbert-Polynom ist die Konstante 1.

Eine gute Darstellung dieser Theorie ist in [1], Chapter 11 zu finden.

2. In diesem Beispiel ist $G = \langle S \rangle$, wo S endlich ist. Der Wert der Funktion l an der Stelle n ist definiert als die Anzahl der Elemente der Gruppe G, die als S-Wörter der Länge $\leq n$ geschrieben werden können. Ein wichtiges Theorem von Gromov [7] besagt, dass *die Funktion $l(n)$ genau dann polynomiales Wachstum aufweist, wenn G eine nilpotente Untergruppe von endlichem Index besitzt.* Erst kürzlich hat Grunewald zeigen können, dass es Beispiele von Gruppen gibt, wo die Funktion l zwar polynomiales Wachstum aufweist, aber nicht letztlich PORC ist. (Ein sehr schöner Beweis des Theorems von Gromov mit Methoden der Non-Standard-Analysis stammt von van den Dries und Wilkie [4].)

Grunewalds Beispiel ist von der Art der Heisenberg-Gruppe. Es sei H_k die Heisenberg-Gruppe, d.h. die Gruppe mit Erzeugenden $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k, z$ und den Relationen

$$[x_i, y_j] = 1 \text{ für } i \neq j,$$

$$[x_i, y_i] = z,$$

z ist zentral,

die x's kommutieren,

die y's kommutieren.

Es sei $S = \{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k\}$. Dann ist H_1 die freie nilpotente Gruppe vom Rang 2 und der Klasse 2, und man weiss, dass $P(l, X)$ von der Form

$$\frac{g(X)}{(1 - X^{12})^5}$$

ist. Dies wurde von R. Bödeker vermutet und unabhängig voneinander von N. Shapiro [8] und B. Weber [10] bewiesen. Nach unserem Satz 2 ist für H_1 die Funktion l also letztlich PORC mod 12. Dagegen konnte Grunewald zeigen, dass für H_2 die Poincaré-Reihe von l nicht rational ist und dass sie daher wegen Satz 4 auch nicht letztlich PORC sein kann.

3. Für unseren KG-Modul A wählen wir eine projektive Resolution

$$\cdots \to P_{i+1} \to P_i \to \cdots \to P_1 \to P_0 \to A \to 0$$

mit der Eigenschaft, dass für jedes i das Bild von P_i in P_{i-1} keinen projektiven direkten Summanden enthält. Eine derartige projektive Resolution von A existiert immer; sie ist in einem wohldefinierten Sinn die kleinstmögliche projektive Resolution von A. Wie man zeigen kann, ist sie bis auf Isomorphie eindeutig bestimmt. Wir behaupten nun, dass *die Funktion* $n \mapsto \dim_K P_n$ *letztlich PORC ist.*

Dieses Resultat folgt aus der Kombination von zwei andern tiefliegenden Resultaten, nämlich:

(i) $\mathrm{Ext}_{KG}(K, K)$ ist eine graduierte Noethersche Algebra (Evens [5]), und für jeden KG-Modul M ist $\mathrm{Ext}_{KG}(K, M)$ ein endlich erzeugter Modul über $\mathrm{Ext}_{KG}(K, K)$.

(ii) Falls $V = \{V_n\}$ ein endlich erzeugter graduierter Modul über der graduierten kommutativen Noetherschen K-Algebra Λ ist, dann ist die Funktion $n \mapsto \dim_K V_n$ letztlich PORC. Dieses Resultat wird üblicherweise als Theorem von Hilbert-Serre bezeichnet. Ein Spezialfall davon liegt dem Satz über lokale Ringe im Beispiel 1 zugrunde (siehe [1]).

Aus den Resultaten (i) und (ii) folgt, dass die Funktion

$$n \mapsto \dim_K \mathrm{Ext}^n_{KG}(K, M)$$

letztlich PORC ist. Dann gilt dasselbe auch für die Funktion

$$n \mapsto \dim_K \mathrm{Ext}^n_{KG}(A, B) \ ,$$

wo A, B beliebige KG-Moduln sind, denn es ist

$$\mathrm{Ext}_{KG}(A, B) \simeq \mathrm{Ext}_{KG}(K, \mathrm{Hom}\,(A, B)) \ .$$

Ein verhältnismässig einfaches Argument zeigt dann, dass

$$\dim_K P_n = \sum_S r_S \cdot \dim_K \mathrm{Ext}^n_{KG}(A, S)$$

gilt, wo S über alle einfachen KG-Modulen variiert und r_S positive ganze Zahlen sind. Die Folgerung, dass die Funktion $n \mapsto \dim_K P_n$ letztlich PORC ist, ergibt sich daraus sofort, weil die Menge derartiger Funktionen unter der Addition abgeschlossen ist. In der Tat ist diese Menge sogar ein Unterring von **X**.

Die Ideen, die dem Beispiel 3 zugrunde liegen, gehen zurück auf Swan [9]; eine gute Einführung in diese Theorie ist das kleine Büchlein von Carlson [3].

Hinweisen möchte ich, zusätzlich zur schon zitierten Literatur, auf den Übersichtsartikel von Babenko [2] über Wachstumsfunktionen in der Algebra und der algebraischen Geometrie sowie auf den Artikel von Grigorchuk [6].

Literatur

[1] M.F. Atiyah and I.G. Macdonald, Introduction to commutative algebra, Addison-Wesley 1969.

[2] I.K. Bakenko, Problems of growth and rationality in algebra and topology, Uspekhi Mat. Nauk 41:2 (1986) 95–142 (Russian Math. Surveys 41: 2 (1986) 117–175).

[3] J.F. Carlson, Module varieties and cohomology rings of finite groups, Vorlesungen der Univ. Essen 13 (1985).

[4] L. van den Dries and A.J. Wilkie, Gromov's theorem on groups of polynomial growth and elementary logic, J. Algebra 89 (1984) 349–374.

[5] L. Evens, The cohomology ring of a finite group, Trans. Amer. Math. Soc. 101 (1961) 224–239.

[6] R.I. Grigorchuk, On growth in group theory, Proc. Intern. Congress of Mathematicians, Kyoto, vol. i (1990) 325–328.

[7] M. Gromov, Groups of polynomial growth and expanding maps, Publ. Math. IHES 53 (1981) 53–78.

[8] M. Shapiro, A. geometric approach to the almost convexity and growth of some nilpotent groups, Math. Annalen (to appear).

[9] R.G. Swan, Groups with no odd dimensional cohomology, J. Algebra 17 (1971) 401-3.

[10] B. Weber, Zur Rationalität polynomialer Wachstumsfunktionen, Bonner Math. Schr. 197 (1989).

Eine englische Fassung dieses Artikels ist 1989 in der Zeitschrift *Mathematical Medley* erschienen. Der Autor dankt der *Singapore Mathematical Society* für die freundliche Erlaubnis zur Veröffentlichung dieser leicht erweiterten deutschen Version. Der Autor dankt ferner Fritz Grunewald und Aidan Schofield für Bemerkungen zu einer früheren Fassung und Urs Stammbach für die Übersetzung aus dem Englischen.

Karl W. Gruenberg
Queen Mary and Westfield College
Mile End Road
London E1 4NS