Werk

Titel: Mathematische Annalen
Ort: Berlin
Jahr: 1934
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235181684_0109
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0109

LOG Id: LOG_0007
LOG Titel: Die Seltenheit der Gleichungen mit Affekt
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN235181684
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235181684
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235181684

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Die Seltenheit der Gleichungen mit Affekt.

Von

B. L. van der Waerden in Leipzig.

Im folgenden soll bewiesen werden, daß asymptotisch 100 % aller ganzzahligen Gleichungen in bezug auf den rationalen Zahlkörper keinen Affekt haben. Das heißt, wenn man alle Gleichungen $f(x) = 0$ bildet, wo

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

ein ganzzahliges Polynom ist, dessen Koeffizienten dem Betrage nach $\leqq N$ sind, so strebt der Bruchteil dieser Gleichungen, deren Galoissche Gruppe die symmetrische ist, mit wachsendem N gegen Eins.

Die bisherigen Beweise ähnlicher Seltenheitssätze[1]) stützen sich meistens auf den Hilbertschen Irreduzibilitätsatz und erfordern daher transzendente Hilfsmittel. Der hier darzustellende Beweis dagegen ist rein elementar. Er beruht auf der bekannten Dedekind-Bauerschen Methode zur Bildung affektloser Gleichungen mittels Zerlegungen modulo verschiedener Primzahlen[2]). Es läßt sich nämlich beweisen, daß die nach dieser Methode gebildeten Gleichungen schon 100 % aller ganzzahligen Gleichungen ausmachen. Das ist übrigens nicht verwunderlich, denn auf Grund der Kronecker-Frobeniusschen Dichtigkeitstheorie weiß man ja, daß das nachstehend zu erwähnende Dedekindsche Kriterium für Affektlosigkeit nicht nur hinreichend, sondern auch notwendig ist, sobald nur zu jeder Gleichung passende Primzahlen herangezogen werden.

Die erwähnte Methode beruht auf dem folgenden Dedekindschen Satz, für dessen elementaren Beweis ich auf mein Buch Moderne Algebra I, § 56 verweise:

Wenn ein ganzzahliges Polynom $f(x)$ vom Grade n modulo Primzahlen p_1, p_2, p_3 folgendermaßen zerfällt: modulo p_1 in irreduzible Faktoren

[1]) Vgl. K. Dörge, Die Seltenheit der reduziblen Polynome und der Normalgleichungen, Math. Annalen **95** (1925), S. 247—256.

[2]) M. Bauer, Ganzzahlige Gleichungen ohne Affekt, Math. Ann. **64** (1907), S. 325—327.

der Grade $n-1$ und 1, modulo p_2 in einen quadratischen Faktor und einen oder zwei Faktoren ungeraden Grades, während modulo p_3 das Polynom irreduzibel und vom Grade n ist, so hat die Gleichung $f(x) = 0$ keinen Affekt.

Ich werde die drei im Satz genannten Arten der Zerfällung eines Polynoms Zerfällungen erster, zweiter und dritter Art nennen. Es soll nun gezeigt werden, daß asymptotisch 100 % aller ganzzahligen Polynome die Eigenschaft haben, daß es eine Primzahl gibt, modulo welcher sie in irgendeiner vorgeschriebenen Weise (also insbesondere von der ersten, zweiten oder dritten Art) zerfallen.

Zuerst möge die Anzahl der modulo p irreduziblen inkongruenten Polynome n-ten Grades berechnet werden. Diese zerfallen im Galois-Feld $GF(p^n)$ vollständig in Linearfaktoren. Jedes Element Θ des $GF(p^n)$, das nicht schon einem Unter-Galoisfeld $GF(p^m)$ angehört, ist Wurzel eines solchen irreduziblen Polynoms, genauer von $p-1$ solchen Polynomen, da die Restklasse von a_0 mod p noch beliebig gewählt werden kann. Die Anzahl dieser Θ ist mindestens

$$p^n - \sum_{m|n}{}' p^m \geqq p^n - \sum_{m=1}^{n-1} p^m > p^n - \frac{p^n}{p-1} = \frac{p^n(p-2)}{p-1}.$$

Da jedes mod p irreduzible Polynom n solche Wurzeln Θ hat, so ist die Anzahl dieser Polynome gleich dem n-ten Teil der eben berechneten Anzahl der Θ, multipliziert mit $(p-1)$ wegen der Willkür von a_0. Die Anzahl der irreduziblen Polynome mod p ist also größer als

$$\frac{p^n(p-2)}{n} = \frac{p^{n+1}}{n}\left(1-\frac{2}{p}\right) \geqq \frac{p^{n+1}}{3n} \quad \text{für} \quad p \geqq 3,$$

also größer als der $3n$-te Teil aller mod p verschiedenen Polynome.

Um nun z. B. die Anzahl der Polynome abzuschätzen, die von der ersten Art sind, also in einen Linearfaktor und einen Faktor $(n-1)$-ten Grades zerfallen, hat man die Anzahl p der möglichen (normierten) Linearfaktoren $x-a$ mit der eben berechneten Mindestzahl der irreduziblen Polynome $(n-1)$-ten Grades zu multiplizieren. Man findet so, daß von den p^{n+1} möglichen mod p verschiedenen Polynomen mehr als $\frac{p^{n+1}}{3(n-1)}$, also mehr als der Bruchteil $\frac{1}{3(n-1)}$ von der ersten Art zerfällt.

In ganz entsprechender Weise findet man für jede mögliche Zerfällungsart (insbesondere für die drei im obigen Satz angeführten Zerfällungsarten) einen festen (von p unabhängigen) Bruch, der angibt, welcher Bruchteil von den p^{n+1} möglichen Polynomen mindestens diese Zerfällungsart besitzt, wobei eventuell einige sehr kleine Primzahlen ausgenommen sein

können. Für die erste, zweite und dritte Zerfällungsart sind diese Brüche z. B.

$$\frac{1}{3(n-1)}, \quad \frac{1}{6\cdot 3(n-2)}, \quad \frac{1}{3n} \quad (p > 2).$$

Ist $\frac{1}{k}$ der kleinste von diesen drei Brüchen, so können wir zusammenfassend den Satz aussprechen: *Modulo jeder Primzahl $p > 2$ zerfallen mindestens $\frac{1}{k}$ aller mod p inkongruenten Polynome n-ten Grades in einer vorgegebenen, ersten, zweiten oder dritten Art.*

Es seien jetzt $p_1, p_2, p_3, \ldots$ alle ungeraden Primzahlen. Wir fragen, wie viele modulo $p_1 p_2$ inkongruente Polynome sowohl p_1 als mod p_2 *nicht* von der ersten Art zerfallen. Von den p_1^n Restklassen von Polynomen mod p_1 zerfallen höchstens $\frac{k-1}{k} p_1^n$ nicht von der ersten Art, ebenso mod p_2 höchstens $\frac{k-1}{k} p_2^n$. Die $(p_1 p_2)^n$ Restklassen von Polynomen mod $p_1 p_2$ sind Durchschnitte von je einer Restklasse mod p_1 und einer mod p_2; unter diesen Durchschnitten gibt es höchstens

$$\frac{k-1}{k} p_1^n \cdot \frac{k-1}{k} p_2^n = \left(\frac{k-1}{k}\right)^2 (p_1 p_2)^n,$$

welche weder mod p_1 noch mod p_2 von der ersten Art zerfallen.

Ebenso gibt es unter den $(p_1 p_2 p_3)^n$ Restklassen von Polynomen mod $p_1 p_2 p_3$ höchstens $\left(\frac{k-1}{k}\right)^3 (p_1 p_2 p_3)^n$, welche weder mod p_1, noch mod p_2, noch mod p_3 von der ersten Art zerfallen, usw.

Wir wählen nun bei gegebenem ε eine Zahl m so groß, daß

$$\left(\frac{k-1}{k}\right)^m < \varepsilon$$

ist. Dann haben von den $P^n = (p_1 p_2 \ldots p_m)^n$ Restklassen von Polynomen mod $P = p_1 p_2 \ldots p_m$ höchstens εP^n die Eigenschaft, modulo keiner Primzahl p_i von der ersten Art zu zerfallen. Ebenso haben höchstens εP^n die Eigenschaft, modulo keinem p_i von der zweiten bzw. dritten Art zu zerfallen. Die übrigen Restklassen, mindestens $(1 - 3\varepsilon) P^n$ an Zahl, zerfallen modulo mindestens einer Primzahl p_i von der ersten, modulo einer anderen von der zweiten, modulo einer dritten von der dritten Art. Auf Grund des anfangs angeführten Satzes sind alle Gleichungen $f(x) = 0$, die zu diesen Restklassen mod P gehören, Gleichungen ohne Affekt.

Wir wählen jetzt $2N + 1 \geqq P$. Von den $2N + 1$ Zahlen a mit $|a| \leqq N$ liegen höchstens $\left[\frac{2N+1}{P}\right] + 1$ in einer Restklasse modulo P; also liegt in den $3\varepsilon P^n$ Restklassen, welche Gleichungen mit Affekt

ergeben können, höchstens die folgende Anzahl von Polynomen mit Koeffizientenbeträgen $\leqq N$:

$$3\,\varepsilon\,P^n\left(\frac{2N+1}{P_n}+1\right)^n = 3\,\varepsilon(2N+1+P)^n \leqq 3\cdot 2^n\,\varepsilon\,(2N+1)^n.$$

Die übrigen $(1-3\cdot 2^n\,\varepsilon)\,(2N+1)^n$ Polynome mit Koeffizientenbeträgen $\leqq N$ ergeben sicher Gleichungen ohne Affekt. Der Bruchteil $(1-3\cdot 2^n\,\varepsilon)$ kann aber beliebig nahe an Eins gebracht werden. Damit ist die am Anfang formulierte Behauptung bewiesen.

Die im vorstehenden Beweis enthaltene Abschätzung des Bruchteils der Gleichungen, welche einen Affekt besitzen können, ließe sich noch etwas verschärfen. Es hat aber wenig Sinn, das auszuführen, da die vermutlich richtige Größenordnung $\frac{1}{N^\alpha}$ dieses Bruchteils (vgl. die analogen Abschätzungen in der unter [1]) zitierten Arbeit) mit dieser Methode anscheinend nicht erreicht werden kann.

(Eingegangen am 24. 2. 1933).