Eine zahlentheoretische Konstruktion der Galois-Felder GF(p2)

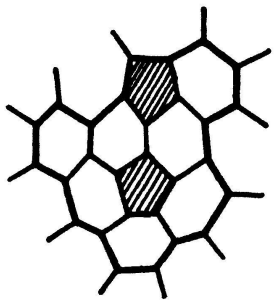

Fig. 9

$a = 12$

$e = 8$

$f_5 = 2$

Für gerades n wird eine Kantenfolge als *geodätisch* definiert, wenn zu jedem Zwischenknoten B_j gilt $s_j = n/2$, also

$$\frac{1}{2} - \frac{s_j}{n} = 0 \tag{18}$$

ist. Da eine geodätische Kantenfolge jeden Knoten höchstens $n/2$ mal treffen kann, ist in einem endlichen ebenen Netz jede geodätische Kantenfolge (i. a. nicht einfach) geschlossen.

Hans Walser, Zürich

LITERATURVERZEICHNIS

[1] B. Grünbaum: *Convex Polytopes*, New York 1967.
[2] M. Jeger: *Elementare Begriffe und Sätze aus der Theorie der Graphen*. Der Mathematikunterricht *20* (1974), Heft 4, S. 11–64.
[3] E. Kreyszig: *Differentialgeometrie*, Leipzig 1957.
[4] H. Sachs: *Einführung in die Theorie der endlichen Graphen*, Teil II, Leipzig 1972.

Eine zahlentheoretische Konstruktion der Galois-Felder GF(p^2)

In jüngster Zeit interessiert man sich vermehrt für die explizite Konstruktion von Galois-Feldern (siehe etwa [1]). In der Literatur wird gewöhnlich auf das Verfahren mit Hilfe eines irreduziblen Polynoms verwiesen. Hier soll gezeigt werden, wie sich die Galois-Felder von der Ordnung p^2, $p \geq 3$, auf zahlentheoretischem Weg herstellen lassen.

Für eine Primzahl $p \geq 3$ sei

$$Z_p^2 = \{(r, i) \mid r, i \text{ ganz} \wedge 0 \leq r, i \leq p - 1\}.$$

In dieser Menge definieren wir nach dem Vorbild der komplexen Zahlen eine Addition $\oplus$ und eine Multiplikation $\odot$:

$$(r_1, i_1) \oplus (r_2, i_2) = (r_1 + r_2, i_1 + i_2), \tag{1}$$

$$(r_1, i_1) \odot (r_2, i_2) = (r_1 r_2 - i_1 i_2, r_1 i_2 + r_2 i_1). \tag{2}$$

Die Operationen $+$, $-$, $\cdot$ bedeuten dabei die Addition, Subtraktion und Multiplikation modulo p. Die Elemente bilden mit der in (1) definierten Addition, wie leicht ersichtlich, eine Abelsche Gruppe mit dem Nullelement (0,0). Das Einselement ist das Element (1,0), und da sowohl die Restklassen modulo p als auch die komplexen Zahlen einen Körper bilden, sind das Kommutativgesetz der Multiplikation, das Assoziativgesetz der Multiplikation und die Distributivgesetze erfüllt. Diese Motivierung versagt aber im Fall des inversen Elementes.

Die Auflösung von $(r_1, i_1) \odot (r, i) = (r_2, i_2)$ führt auf

$$r(r_1^2 + i_1^2) = r_1 r_2 + i_1 i_2 \wedge i(r_1^2 + i_1^2) = r_1 i_2 - i_1 r_2 .$$

Damit die Existenz eines Inversen gewährleistet ist, muss der Term $r_1^2 + i_1^2$ für alle Elemente von null verschieden sein. Dies ist gleichbedeutend mit der Unlösbarkeit der Kongruenz

$$x^2 + y^2 \equiv 0 \pmod{p} , \quad (x, y) \neq (0,0) \tag{3}$$

Beh.: Die Kongruenz (3) ist genau dann unlösbar, wenn $p \equiv 3 \pmod 4$ ist.
Bew.: Da aus $x \equiv 0$ auch $y \equiv 0$ folgt, ist $x \not\equiv 0 \wedge y \not\equiv 0$.

Dividiert man (3) durch y^2, so ergibt sich, dass die Kongruenz (3) zur Kongruenz

$$(xy^{-1})^2 \equiv -1 \pmod{p}$$

äquivalent ist. Diese Kongruenz ist genau dann unlösbar, wenn -1 quadratischer Nichtrest von p ist, und wie man aus der Zahlentheorie entnimmt (z.B. [2], S. 16), ist das genau dann der Fall, wenn $p \equiv 3 \pmod 4$ ist.

Schliesslich ist $1^2 + 1^2 \equiv 0$ für $p = 2$, und wir erhalten somit den

Satz 1

$[Z_p^2; \oplus, \odot]$ ist genau für $p \equiv 3 \pmod 4$ ein Galois-Feld $GF(p^2)$.

Offenbar ist für das Vorliegen eines Galois-Feldes wesentlich, dass -1 quadratischer Nichtrest von $p \equiv 3 \pmod 4$ ist. Um für beliebige p ein Galois-Feld zu erhalten, kann man versuchen, die durch (2) definierte Multiplikation so abzuändern, dass man an Stelle von -1 einen beliebigen quadratischen Nichtrest von p einsetzt.

Wir definieren also eine neue Multiplikation $\odot_q$ durch

$$(r_1, i_1) \odot_q (r_2, i_2) = (r_1 r_2 + q i_1 i_2, r_2 i_1 + r_1 i_2) , \tag{2'}$$

worin q einen quadratischen Nichtrest von p bedeutet.

Das Einselement bleibt (1,0), und ebenso ist das Kommutativgesetz erfüllt. Ebenfalls gültig bleiben das Distributiv- und das Assoziativgesetz. Der Nachweis dafür ist eine routinemässige Angelegenheit und darf dem Leser überlassen werden.

Die Ausrechnung von $(r_1, i_1) \odot_q (r, i) = (r_2, i_2)$ führt auf das Gleichungssystem

$$r_1 r + q i_1 i = r_2 \wedge i_1 r + r_1 i = i_2 .$$

Die Frage, wann dessen Determinante $r_1^2 - q i_1^2 \neq 0$ ist, kann wieder formuliert werden als: Wann ist die Kongruenz

$$x^2 + (-q) y^2 \equiv 0 \pmod{p} , \quad (x,y) \neq (0,0)$$

unlösbar ?

Analog zur Herleitung des Satzes 1 ist diese Kongruenz äquivalent zur Kongruenz $(xy^{-1})^2 \equiv q (\mathrm{mod}\ p)$, und diese ist genau dann unlösbar, wenn q quadratischer Nichtrest von p ist.

Als Verallgemeinerung des Satzes 1 erhalten wir also den

Satz 2

Ist q quadratischer Nichtrest von p, so ist $[Z_p^2; \oplus, \odot_q]$ ein Galois-Feld $\mathrm{GF}(p^2)$.

P. Hohler, Olten

LITERATUR

[1] M. Jeger, *Irreduzible Polynome als kombinatorische Figuren*, El. Math. *28* (1973), 86–92.
[2] E. Trost, Primzahlen, Birkhäuser Basel 1953.

Aufgaben

Aufgabe 741. In einem Dreieck ABC seien A', B', C' und A_1, B_1, C_1 die Mittelpunkte bzw. die Höhenfusspunkte der Seiten BC, CA, AB. In der Dreiecksebene seien noch ein Punkt P und die zu P symmetrischen Punkte P_a, P_b, P_c in bezug auf $B'C'$, $C'A'$, $A'B'$ gegeben. Man zeige, dass die Kreise mit den Durchmesserstrecken A_1P_a, B_1P_b, C_1P_c und der Feuerbachsche Neunpunktekreis des Dreiecks ABC sich in einem Punkt schneiden. G. Bercea, München, BRD

Lösung: Es sei d der durch P gehende Durchmesser des Umkreises ω (Mittelpunkt M) von ΔABC und A^* der Fusspunkt des Lotes durch A auf d. Der Kreis mit der Durchmesserstrecke AM geht durch A^*. Das Spiegelbild dieses Kreises in bezug auf $B'C'$ ist der Neunpunktekreis ν des Dreiecks ABC, d.h. der Umkreis von $\Delta A'B'C'$. Deshalb liegt das Spiegelbild D von A^* an $B'C'$ auf ν. Daraus folgt, dass die Spiegelbilder B^* und C^* von D an $A'C'$ bzw. $A'B'$ in einer Geraden liegen mit A^*. Diese Gerade geht bekanntlich durch den Höhenschnittpunkt von $\Delta A'B'C'$, d.h. also durch M. Es liegen B^* und C^* deshalb auf d. Man hat offenbar: $C'A^* = C'D = C'B^*$. Wird die Mitte der Strecke A^*B^* mit E bezeichnet, so ist folglich $C'E \perp A^*B^*$; deshalb: $C'E \parallel AA^*$. Dann ist auch $BB^* \parallel AA^*$, also $BB^* \perp d$. Ebenso gilt: $CC^* \perp d$. Weil $A^*D \perp BC$, $B^*D \perp CA$ und $C^*D \perp AB$, folgert man aus dem Obigen, dass D der Orthopol der Geraden d ist in bezug auf ΔABC. Der Kreis mit der Durchmesserstrecke A_1P_a ist offenbar das Spiegelbild an $B'C'$ des durch A^* hindurchgehenden Kreises mit der Durchmesserstrecke AP. Der zuerst genannte Kreis geht deshalb durch D. Dasselbe gilt für die Kreise mit den Durchmesserstrecken B_1P_b bzw. C_1P_c.

Bemerkungen: 1. Die obige Lösung enthält zugleich einen Beweis für den bekannten Satz: Der geometrische Ort der Orthopole der Durchmesser des Umkreises ist der Neunpunktekreis.

2. Man zeigt unschwer, dass auch der Fusspunktekreis von P bezüglich ΔABC durch P geht.

O. P. Lossers, Eindhoven, Niederlande