Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

6. Studienbrief zur Diskreten Mathematik

In dieser Woche wird ein weiterer Nichtexistenzsatz behandelt, und zwar für (kombinatorische) projektive Ebenen. Das generische Beispiel einer endlichen algebraischen projektiven Geometrie wird auf der ersten Seite dargestellt. Rufen Sie sich Ihre Kenntnisse über Vektorräume in Erinnerung. Dazu sollte gehören, daß der Grundkörper nicht nur reell oder komplex sein kann, sondern eben ein ganz beliebiger Körper und auch, daß jeder d-dimensionale Vektorraum über dem Körper K isomorph zum Vektorraum K^d ist (manchmal wird K^d als „Koordinatenraum" bezeichnet).

Aus der elementaren Algebra entlehnen wir den Satz von LAGRANGE: Ist H eine Untergruppe von G so sind die Linksnebenklassen $aH := \{ax : x \in H\}$ disjunkt und gleichmächtig zu H; ist G endlich, so folgt daraus $|G| = |H||G/H|$, worin G/H die Menge der Linksnebenklassen bezeichnet. Insbesondere ist $|H|$ ein Teiler von $|G|$.

Und außerdem: Ist $\varphi : G \to H$ ein (Gruppen-) Homomorphismus (das heißt: $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$, mit den entsprechenden Multiplikationen in G bzw. H), so ist die Gruppe Kern$\varphi := \{x \in G : \varphi(x) = 1\}$ ein Normalteiler von G (das heißt: $aH = Ha := \{xa : x \in H\}$ für alle $a \in G$); infolgedessen bilden die Linksnebenklassen $G/$Kernφ eine Gruppe mit aKern$\varphi \cdot b$Kern$\varphi := (ab)$Kernφ. Der Homorphiesatz besagt nun, daß die Bildgruppe $\varphi(G)$ isomorph zu $G/$Kernφ ist.

Beide Sätze kann man in der deutschen Wikipedia nebst Beweisen nachlesen.

Ferner werden im Beweis von Satz 1.11 Grundregeln der Teilbarkeit sowie des Rechnens im Körper $\mathbb{Z}_p$ bzw. der Arithmetik modulo p (p Primzahl) verwendet.

Ilmenau, den 24. Mai 2020 · Matthias Kriesell

(Fortsetzung Kapitel 1: Mengensysteme mit Symmetrieeigenschaften)

Sei K ein endlicher Körper und $d \geq 2$. Wir betrachten

$$\begin{aligned}
\langle x \rangle &= \{\lambda x : \lambda \in K\} \text{ für } x \in K^{d+1} \setminus \{0\}, \\
P &:= \{\langle x \rangle : x \in K^{d+1} \setminus \{0\}\}, \\
\langle z \rangle^{\perp} &= \{x \in K^{d+1} : x^{\top} z = 0\} \text{ und} \\
B_z &:= \{\langle x \rangle \in P : \langle x \rangle \subseteq \langle z \rangle^{\perp}\} \text{ für } z \in K^{d+1} \setminus \{0\}, \text{ sowie} \\
\mathfrak{B} &:= \{B_z : z \in K^{d+1} \setminus \{0\}\}.
\end{aligned}$$

Wegen $\langle x \rangle \cong K^1$ für $x \neq 0$ und $\langle z \rangle^{\perp} \cong K^d$ für $z \neq 0$ folgt $|\langle x \rangle| = |K|$ bzw. $|\langle z \rangle^{\perp}| = |K|^d$. Zwei verschiedene Geraden $\langle x \rangle \neq \langle y \rangle$ ($0 \neq x \neq y \neq 0$) haben nur 0 gemeinsam, daher zerfällt $K^{d+1} \setminus \{0\}$ in disjunkte $(|K|-1)$-elementige Mengen $\langle x \rangle \setminus \{0\}$, $\langle x \rangle \in P$. Ebenso zerfällt $\langle z \rangle^{\perp}$ in disjunkte $(|K|-1)$-elementige Mengen $\langle x \rangle \setminus \{0\}$ mit $\langle x \rangle \in B_z$. Daher ist $(P, \mathfrak{B})$ eine v-punktige, k-uniforme Inzidenzstruktur mit

$$\begin{aligned}
v &= |P| = \frac{|K|^{d+1}-1}{|K|-1} = |K|^d + |K|^{d-1} + \cdots + |K|^2 + |K| + 1 \text{ und} \\
k &= |B_z| = \frac{|K|^d - 1}{|K|-1} = |K|^{d-1} + |K|^{d-2} + \cdots + |K|^2 + |K| + 1.
\end{aligned}$$

Genau dann sind $\langle x \rangle \neq \langle y \rangle$ aus P Elemente desselben B_z, wenn gilt $x^{\top} z = 0$ und $y^{\top} z = 0$; diejenigen $z \in K^{d+1} \setminus \{0\}$ mit $\langle x \rangle, \langle y \rangle \in B_z$ bilden also mit 0 einen $(d-1)$-dimensionalen Unterraum von K^{d+1}, der wiederum in disjunkte $(|K|-1)$-elementige Mengen $\langle z \rangle \setminus \{0\}$ zerfällt. Weil $B_z = B_{z'}$ genau dann gilt, wenn $\langle z \rangle = \langle z' \rangle$ ist, sind zwei Punkte aus P in genau

$$\lambda = \frac{|K|^{d-1}-2}{|K|-1} = |K|^{d-2} + |K|^{d-3} + \cdots + |K|^2 + |K| + 1$$

vielen der B_z aus $\mathfrak{B}$ enthalten. Folglich ist

$$PG_d(K) := (P, \mathfrak{B})$$

ein 2-(v, k, λ)-Design. — Sind allgemein $d, n \geq 2$ Zahlen, so heißt ein

$$2\text{-}(\tfrac{n^{d+1}-1}{n-1}, \tfrac{n^d-1}{n-1}, \tfrac{n^{d-1}-1}{n-1})\text{-Design}$$

eine (kombinatorische) *d-dimensionale projektive Geometrie der Ordnung n*. Im Fall $d = 2$ spricht man von einer (kombinatorischen) *projektiven Ebene der Ordnung n*. Eine projektive Ebene der Ordnung n ist also ein

$$2\text{-}(n^2 + n + 1, n + 1, 1)\text{-Design.}$$

Die obige Konstruktion zeigt, daß es d-dimensional projektive Geometrien der Ordnung n gibt wann immer es einen Körper der Ordnung n gibt, auf jeden Fall also dann, wenn n eine Primzahlpotenz ist.

Es ist eine der wichtigsten offenen Fragen der Kombinatorik, ob eine projektive Ebene der Ordnung n für eine Nicht-Primzahlpotenz n existiert. Der folgende Satz von BRUCK und RYSER verneint das für unendlich viele n. Er kann leicht mit Satz 1.10 bewiesen werden.

Wir stellen einen Sachverhalt aus der Zahlentheorie voran:

Für eine Primzahl $p \equiv 3 \bmod 4$ ist -1 kein Quadrat mod p, das heißt die Gleichung $x^2 = -1 \bmod p$ hat keine Lösung.

Beweis. Durch $\varphi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $\varphi(x) := x^2$ wird ein Homomorphismus von der multiplikativen Gruppe $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ des Körpers $\mathbb{Z}_p$ in sich definiert. Das Polynom $x^2 - 1 = (x+1)(x-1)$ hat die beiden Nullstellen $+1$ und -1, daher ist Kern$\varphi = \{+1, -1\}$. Aus dem Satz von LAGRANGE über die Zerlegung in Nebenklassen und dem Homomorphiesatz folgt

$$|\mathbb{Z}_p^*| = |\text{Kern}\varphi||\mathbb{Z}_p^*/\text{Kern}\varphi| = 2|\varphi(\mathbb{Z}_p^*)|.$$

Wäre nun -1 ein Quadrat mod p, so wäre $\{-1, 1\}$ eine Untergruppe der Ordnung 2 der Gruppe $\varphi(\mathbb{Z}_p^*)$ aller Quadrate mod p; nach dem Satz von LAGRANGE wäre dann $|\varphi(\mathbb{Z}_p^*)|$ gerade, also $p - 1 = |\mathbb{Z}_p^*| = 2|\varphi(\mathbb{Z}_p^*)| \equiv 0 \bmod 4$, also $p \equiv 1 \bmod 4$, Widerspruch. □

Satz 1.11 (BRUCK & RYSER 1949)

Existiere eine projektive Ebene der Ordnung $n \geq 2$. Dann gilt:

(i) Ist $n \equiv 1 \bmod 2$ oder $n \equiv 2 \bmod 4$, so hat jeder Primfaktor $p \equiv 3 \bmod 4$ gerade Vielfachheit in der Primfaktorzerlegung von n, und:

(ii) $n \not\equiv 6 \bmod 8$.

Beweis. Gebe es ein

$$2\text{-}(\underbrace{n^2+n+1}_{=:v}, \underbrace{n+1}_{=:k}, \underbrace{1}_{=:\lambda})\text{-Design.}$$

Zum Nachweis von (i) betrachten wir n mit $n \equiv 1 \bmod 2$ oder $n \equiv 2 \bmod 4$. In beiden Fällen kommt $v = n^2 + n + 1 \equiv 3 \bmod 4$. Nach Satz 1.10 besitzt dann die Gleichung

$$x^2 = ny^2 - z^2$$

eine nichttriviale ganzzahlige Lösung. Nehmen wir an, n habe einen Primfaktor $p \equiv 3 \bmod 4$ von *ungerader* Vielfachheit. Dann können wir $n = aq$ in eine Quadratzahl $q = t^2$ und eine quadratfreie Zahl a (ohne quadratzahlige Teiler) zerlegen und feststellen, daß p ein (einfacher) Teiler von a ist. (x, ty, z) ist dann eine nichttriviale Lösung der Gleichung

$$x^2 = ay^2 - z^2,$$

und unter diesen Lösungen wählen wir (x, y, z) ohne gemeinsamen Teiler > 1. Es ist $p \not| z$ (sonst wäre $p^2|z^2$, also $p|x$, also $p^2|x^2$, also $p^2|ay^2$, also $p|y$, Widerspruch). Aus $x^2 \equiv -z^2 \bmod p$ folgt $(xz^{-1})^2 \equiv -1 \bmod p$, also ist -1 ein Quadrat mod p, im Widerspruch zur Vorbemerkung.

Zum Nachweis von (ii) nehmen wir $n \equiv 6 \bmod 8$ an. Dann ist $n \equiv 2 \bmod 4$, also $n^2 + n + 1 \equiv 3 \bmod 4$, und nach Satz 1.10 besitzt abermals die Gleichung

$$x^2 = ny^2 - z^2$$

eine nichttriviale ganzzahlige Lösung — also auch eine nichttriviale Lösung (x, y, z) ohne gemeinsamen Teiler > 1. Da $0, 1, 4$ die einzigen Quadrate mod 8 sind (tabellieren!), gilt $x^2, y^2 \equiv 0, 1, 4 \bmod 8$ und $ny^2 \equiv 6y^2 \equiv 0, 6 \bmod 8$. Die Gleichung $x^2 + y^2 \equiv ny^2 \bmod 8$ erzwingt dann $x^2, y^2 \equiv 0, 4 \bmod 8$ und $6y^2 \equiv 0 \bmod 8$, woraus auch $y^2 \equiv 0, 4 \bmod 8$ folgt. Dann aber ist 4 ein gemeinsamer Teiler von x^2, y^2, z^2 und folglich 2 ein gemeinsamer Teiler von x, y, z, Widerspruch. □

Unter den Zahlen bis 30, die keine Primzahlpotenzen sind, kann schon für $n \in \{10, 12, 15, 18, 20, 24, 26, 28\}$ nicht mit Hilfe von Satz 1.11 auf die Nichtexistenz einer projektiven Ebene der Ordnung n geschlossen werden. Tatsächlich gehen *alle* bis heute bekannten Nichtexistenzaussagen für projektive Ebenen einer Ordnung n, n keine Primzahlpotenz, auf den immerhin schon 71 Jahre alten Satz von BRUCK und RYSER zurück, mit Ausnahme von $n = 10$: Die Nichtexistenz eines 2-$(111, 11, 1)$-Designs wurde 1989 von LAM, THIEL und SWIERCZ durch einen stark computergestützten Beweis erbracht; interessanterweise schätzen sie in ihrer Arbeit die Möglichkeit von Hard- oder Softwarefehlern ab; man solle ihre Ergebnisse nicht als „traditionellen Beweis" betrachten.