Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

7. Studienbrief zur Diskreten Mathematik

And now for something completely different: Im zweiten Kapitel werden wir uns mit lateinischen und griechischen Quadraten befassen. Dabei wird über das EULERsche Offiziersproblem zu reden sein, aber auch (in den kommenden Wochen), wie die Existenz gewisser Mengen von Quadraten der „Ordnung" n mit der Existenz projektiver Ebenen zusammenhängt und für eine stabile Brücke zum ersten Kapitel sorgt.

Ilmenau, den 25. Mai 2020 · Matthias Kriesell

Kapitel 2
Orthogonale lateinische Quadrate

Seien K, X, Y Mengen. Eine $X \times Y$-*Matrix über* K ist eine Abbildung

$$Q : X \times Y \to K.$$

Für $x \in X$ heißt die durch $Q(x, \cdot)(y) := Q(x, y)$ für $y \in Y$ definierte Abbildung $Q(x, \cdot) : Y \to K$ die *x-te Spalte* von Q. Analog heißt für $y \in Y$ die durch $Q(\cdot, y)(x) := Q(x, y)$ für $x \in X$ definierte Abbildung $Q(\cdot, y) : X \to K$ die *y-te Spalte* von Q. Wir werden im folgenden stets annehmen, daß X und Y endlich sind und konventionelle Matrizenschreibweise verwenden, wobei wir uns X, Y jeweils mit einer festen linearen Ordnung versehen denken.

Im Fall $|X| = |Y| = n$ heißt Q ein *Quadrat* der *Ordnung* n. Eine $X \times Y$-Matrix über K heißt ein *lateinisches Quadrat*, falls jede Zeile und jede Spalte bijektiv ist. Alternativ: Für alle $x \in X, c \in K$ besitzt die Gleichung $Q(x, y) = c$ genau eine Lösung $y \in Y$ und für alle $y \in Y, c \in K$ besitzt die Gleichung $Q(x, y) = c$ genau eine Lösung $x \in X$. Das bedeutet, daß in jeder Zeile von Q jedes Symbol aus K an genau einer Stelle auftritt und in jeder Spalte von Q jedes Symbol aus K an genau einer Stelle. Lateinische Quadrate über K sind also Quadrate der Ordnung $|K|$. Im Fall $X = Y = K$ nennt man ein lateinisches Quadrat auch eine *Quasigruppe* auf K (ist nämlich K mit $\cdot$ eine endliche Gruppe, so ist $\cdot : K \times K \to K$ ein lateinisches Quadrat).

Ist Q eine X, Y-Matrix über K und Q' eine X, Y-Matrix über K', so heißt die durch

$$(Q, Q')(x, y) := (Q(x, y), Q'(x, y)) \text{ für } x \in X \text{ und } y \in Y$$

definierte X, Y-Matrix (Q, Q') über $K \times K'$ die *Superposition* oder auch *Überlagerung* von Q und Q'. Sind zum Beispiel für $X = Y = K = K' = \{1, 2, 3\}$ die beiden Quasigruppen

$$Q := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \text{ und } Q' := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

gegeben, so ist die Superposition von Q und Q' gleich

$$(Q, Q') = \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}.$$

Die Superposition von Q und Q selbst ist dagegen gleich

$$(Q, Q) := \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,2) & (3,3) & (1,1) \\ (3,3) & (1,1) & (2,2) \end{pmatrix}.$$

Statt (x, y) wird dabei auch gerne die *Wortschreibweise*, also xy, verwendet. Wie man sieht, werden alle neun möglichen Paare aus $\{1, 2, 3\} \times \{1, 2, 3\}$ in der Superposition (Q, Q') angenommen. $(Q, Q') : X \times Y \to K \times K'$ ist also bijektiv. Dagegen werden nur die drei Paare $(1, 1), (2, 2), (3, 3)$ in der Superposition (Q, Q) angenommen, $(Q, Q) : X \times Y \to K \times K$ ist also nicht bijektiv.

Zwei lateinische Quadrate $Q : X \times Y \to K$ und $Q' : X \times Y \to K'$ heißen *orthogonal*, wenn ihre Superposition bijektiv ist.[1] Das bedeutet: Für alle $c \in K$ und $c' \in K'$ besitzt die Gleichung $(Q, Q')(x, y) = (c, c')$ genau eine Lösung $(x, y) \in X \times Y$. Alternativ: Jedes Symbolpaar $(c, c') \in K \times K'$ tritt in der Superposition (Q, Q') an genau einer Stelle auf. Gelegentlich wird die Superposition zweier orthogonaler lateinischer Quadrate auch ein *griechisch-lateinisches Quadrat* oder ein EULER*sches Quadrat* genannt.

Man sieht sofort, daß ein lateinisches Quadrat dann und nur dann zu sich selbst orthogonal ist, wenn seine Ordnung ≤ 1 ist. Ein lateinisches Quadrat der Ordnung 2 ist dagegen stets von der Form

$$Q = \begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

und ist

$$R = \begin{pmatrix} c & d \\ d & c \end{pmatrix}$$

ein weiteres lateinisches Quadrat der Ordnung 2, so ist die Überlagerung

$$(Q, R) = \begin{pmatrix} (a, c) & (b, d) \\ (b, d) & (a, c) \end{pmatrix},$$

also niemals bijektiv: Es gibt daher keine zwei orthogonalen Quadrate der Ordnung 2. (Man sieht an diesem Argument außerdem, daß es auf die „Namen der Symbole" in den beteiligten Quadraten nicht ankommt.) Die beiden eingangs genannten lateinischen Quadrate der Ordnung 3 sind dagegen orthogonal. Gibt es ein drittes, das zu beiden orthogonal ist?

Mit Fragen dieser Art hat sich EULER intensiv im Zusammenhang mit dem EULERschen Offiziersproblem befaßt. Wir geben ein paar Konstruktionen an.

Sei G (mit $\cdot$) eine Gruppe ungerader Ordnung. Dann besitzt für jedes $c \in G$ die Gleichung $x^2 = c$ genau eine Lösung. (In der Algebra wird ja $a^{|G|} = 1$ ganz allgemein bewiesen, und somit ist $x = c^{(|G|+1)/2}$ eine Lösung. Die Abbildung $x \mapsto x^2$ von G nach G ist daher surjektiv, und wegen der Endlichkeit von G auch bijektiv.) Damit läßt sich nun beweisen, daß die beiden durch

$$Q(x, y) := x \cdot y \text{ und } R(x, y) := x^{-1} \cdot y$$

[1] Weil $f : K \times K' \to K' \times K$, $f(c, c') := (c', c)$ *immer* bijektiv ist, ist mit (Q, Q') auch $(Q', Q) = f \circ (Q, Q')$ bijektiv; auf die Reihenfolge der an der Superposition beteiligten Quadrate kommt es also bei der Orthogonalität nicht an.

definierten Quasigruppen auf G orthogonale lateinische Quadrate sind:

Zunächst lassen sich ja $x \cdot y = c$ und $x^{-1} \cdot y = c$ wahlweise nach x oder y umstellen (auflösen), daher sind Q, R lateinische Quadrate. Für $c, d \in G$ kann man andererseits aus $Q(x, y) = c$ und $R(x, y) = d$ die Werte von x, y bestimmen: Die beiden Gleichungen besagen $x \cdot y = c$ und $x^{-1} \cdot y = d$, somit

$$c \cdot d^{-1} = x \cdot y \cdot (x^{-1} \cdot y)^{-1} = x \cdot y \cdot y^{-1} \cdot x = x^2,$$

woraus sich nach der Vorbemerkung zwangsläufig

$$x = (c \cdot d^{-1})^{(|G|+1)/2}$$

ergibt, und hieraus folgt mit $x^{-1} \cdot y = d$ sofort

$$y = x \cdot d = (c \cdot d^{-1})^{(|G|+1)/2} \cdot d.$$

Die zweite Konstruktion liefert auf einen Schlag sehr viele paarweise orthogonale lateinische Quadrate. Dazu sei K ein endlicher Körper und für jedes $a \in K \setminus \{0\}$ sei durch

$$Q_a(x, y) := ax + y$$

eine Quasigruppe auf K definiert. Da sich bei festem $a \neq 0$ und b die Gleichung $ax + b$ wahlweise nach x oder y umstellen läßt, ist Q_a ein lateinisches Quadrat. Sind nun $a \neq b$ aus $K \setminus \{0\}$, so läßt sich für $c, d \in K$ aus den Gleichungen

$$Q_a(x, y) = c \text{ und } Q_b(x, y) = d$$

eindeutig auf x, y zurückschließen: Die beiden Gleichungen sind ja äquivalent zu dem linearen Gleichungssystem

$$\begin{array}{rcrl} ax & + & y & = c, \\ bx & + & y & = d, \end{array}$$

also, in Matrixschreibweise der linearen Algebra:

$$\begin{pmatrix} a & 1 \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix},$$

was ja bekanntlich genau dann eine eindeutige Lösung besitzt, wenn die Koeffizientenmatrix invertierbar ist; das *ist* sie aber, denn ihre Determinante ist gleich $a \cdot 1 - b \cdot 1 = a - b \neq 0$. Wir erhalten also $|K| - 1$ paarweise orthogonale lateinische Quadrate! Da es genau dann einen endlichen Körper der Ordnung n gibt, wenn n eine Primzahlpotenz ist, ergeben sich auf diese Weise $n - 1$ paarweise orthogonale lateinische Quadrate der Ordnung n für $n = 3, 4, 5, 7, 8, 9, 11, 13, 16$ usf.

Wir wollen uns nun überlegen, daß eine Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung $n \geq 2$ höchstens $n - 1$ Elemente haben

kann. Seien dazu $Q_i : X \times Y \to K_i$, $i \in \{1, \ldots, k\}$ paarweise orthogonal lateinische Quadrate der Ordnung n. Durch Umbenennung erhalten wir solche mit $X = Y = K_i = N := \{1, \ldots, n\}$ und durch Umbenennung der Symbole in den einzelnen Quadraten solche mit $Q_i(1, y) = y$ für alle $y \in N$ und $i \in \{1, \ldots, k\}$. Wegen $Q_i(1, 1) = 1$ ist dann $Q_i(2, 1) \neq 1$, und wäre $Q_j(2, 1) = Q_i(2, 1) =: c$ für $j \neq i$, so würde das Symbolpaar (c, c) in der Superposition (Q_j, Q_i) doppelt auftreten: Einmal an der Stelle $(2, 1)$ und einmal bei $(1, c)$.

Daher ist für jede Zahl $n \geq 2$ die Maximalzahl paarweise orthogonaler lateinischer Quadrate

$$N(n) := \max\{k : \begin{Bmatrix}\text{es gibt eine Menge von } k \text{ paarweise} \\ \text{orthogonalen lateinischen Quadraten}\end{Bmatrix}\}$$

definiert und es gilt

$$1 \leq N(n) \leq n-1 \text{ für alle } n \geq 2.$$

Die obere Schranke wird zumindest dann angenommen, wenn es einen Körper der Ordnung n gibt, was genau dann der Fall ist, wenn n eine Primzahlpotenz ist. Die untere Schranke wird für $n = 2$ angenommen. Desweiteren gilt

$$N(n) \geq 2 \text{ für alle ungeraden } n \geq 3.$$

Die kleinste Zahl $n \geq 2$, für die $N(n)$ durch diese Betrachtungen nicht festgelegt ist, ist $n = 6$. EULER mußte 1782 die Frage, ob es überhaupt zwei orthogonale lateinische Quadrate der Ordnung 6 gibt, unbeantwortet lassen und hat sie als das berühmte EULERsche Offiziersproblem umformuliert:

> „Kann man 36 Offiziere aus 6 Regimentern und darin von 6 unterschiedlichen Rängen so auf ein 6×6-Feld stellen, daß jedes Regiment und jeder Rang genau einmal in jeder Zeile und in jeder Spalte auftritt?"

Auf den allerersten Blick scheint hier nur formuliert zu sein, daß die Regimenter und Ränge für sich besehen lateinische Quadrate bilden; die Orthogonalität ergibt sich jedoch aus der Eingangsvoraussetzung, daß alle 36 Attributpaare aus Regiment und Rang (wenigstens einmal) vorkommen sollen.[2] In unserer Terminologie besagt die Frage gerade: „Ist $N(6) \geq 2$?". Die Frage konnte erst 1900 von TARRY verneint werden; es ist also $N(6) = 1$.

EULER hat vermutet, daß $N(n) = 1$ für *jedes* $n \equiv 2 \bmod 4$ gilt. Das ist auf jeden Fall richtig für $n = 2$ und (wie er nicht wußte) für $n = 6$ — und wer einmal versucht hat, zwei orthogonale lateinische Quadrate der Ordnung 10 zu konstruieren, wird nicht umhinkommen, die Vermutung für nicht allzu abwegig zu halten. Tatsächlich konnten aber 1959 BOSE, SHRIKHANDE und PARKER zeigen, daß $N(n) \geq 2$ für alle $n \geq 2$ außer für $n = 2$ und $n = 6$ gilt; die drei führen seither den Titel „EULER spoiler".

[2] Genau genommen geht auch das nicht ganz zweifelsfrei aus der Formulierung hervor...

Übungen (4)

Abgabe bis Freitag den 12. Juni 2020.

1. Sei $(P, \mathfrak{B})$ ein 2-$(n^2, n, 1)$-Design, eine sogenannte *affine Ebene* der *Ordnung* n. Man überlege sich, daß für jeden Block $B \in \mathfrak{B}$

$$\mathfrak{C}_B := \{C \in \mathfrak{B} : C = B \vee C \cap B = \emptyset\}$$

   eine Partition von P ist und schließe daraus, daß seinerseits $\mathfrak{B}$ eine Partition in genau $n+1$ solcher „Parallelenscharen" besitzt, etwa $\mathfrak{C}_1, \ldots, \mathfrak{C}_{n+1}$. Entstehe nun P^+ aus P durch Hinzufügen von $n+1$ neuen Punkten $\infty_1, \ldots, \infty_{n+1}$. Jedes $B \in \mathfrak{B}$ ist in genau einem $\mathfrak{C}_i$ enthalten, und wir definieren $B^+ := B \cup \{\infty_i\}$. Sei

$$\mathfrak{B}^+ := \{B^+ : B \in \mathfrak{B}\} \cup \{\{\infty_1, \ldots, \infty_{n+1}\}\}.$$

   Man zeige, daß $(P^+, \mathfrak{B}^+)$ eine projektive Ebene der Ordnung n ist.

2. Sei $(P, \mathfrak{B})$ eine projektive Ebene der Ordnung n und $X \in \mathfrak{B}$. Sei $P^- := P \setminus X$ und $B^- := B \setminus X$ für jedes $B \in \mathfrak{B}$. Sei

$$\mathfrak{B}^- := \{B^- : B \in \mathfrak{B} \setminus \{X\}\}.$$

   Man zeige, daß $(P^-, \mathfrak{B}^-)$ eine affine Ebene der Ordnung n ist.

3. Seien $Q : X \times Y \to K$ und $R : X \times Y \to L$ zwei orthogonale lateinische Quadrate. S entstehe aus Q durch Umbenennung der Symbole: Dazu sei M eine Menge („neuer Symbole"), $f : K \to M$ eine Bijektion (welche die „Umbenennung" regelt) und $S : X \times Y \to M$ definiert durch $S(x, y) := f(Q(x, y))$ für alle $x \in X$, $y \in Y$. Man zeige: Auch S und R sind orthogonale lateinische Quadrate.

4. Seien $Q : X \times Y \to K$ und $R : X \times Y \to L$ zwei orthogonale lateinische Quadrate. Q' und R' entstehen aus Q, R durch simultane Vertauschung von Zeilen und Spalten: Dazu seien $\alpha : X \to X$ und $\beta : Y \to Y$ bijektiv und $Q'(x, y) := Q(\alpha(x), \beta(y))$ und $R'(x, y) := R(\alpha(x), \beta(y))$ für alle $x \in X$, $y \in Y$. Man zeige: Auch Q', R' sind orthogonale lateinische Quadrate.

5. Seien $Q, R : \mathbb{N}_n \times \mathbb{N}_n \to \mathbb{N}_n$ lateinische Quadrate der Ordnung n. Durch $M : \mathbb{N}_n \times \mathbb{N}_n \to \mathbb{N}_{n^2}$, $M(i, j) := n \cdot (Q(i, j) - 1) + R(i, j)$ wird ein neues Quadrat definiert.

   (i) Zeigen Sie, daß die Zeilen- und Spaltensummen $\sum_{k=1}^{n} M(i, k)$ bzw. $\sum_{k=1}^{n} M(k, j)$ für alle i und j aus $\mathbb{N}_n$ übereinstimmen.

(ii) Zeigen Sie: Wenn Q, R orthogonal sind, dann nimmt $M(i,j)$ jede Zahl zwischen 1 und n^2 genau einmal an; gilt auch die Umkehrung?

(iii) Sei $n \geq 1$ ungerade. Man zeige: Es gibt ein Quadrat $M : \mathbb{N}_n \times \mathbb{N}_n \to \mathbb{N}_{n^2}$ in dem alle Zeilen- und Spaltensummen sowie die Diagonalsumme $\sum_{k=1}^{n} M(k,k)$ übereinstimmen.