Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften
TECHNISCHE UNIVERSITÄT
ILMENAU

11. Studienbrief zur Diskreten Mathematik

In dieser Woche beginnt ein neuer Abschnitt, der in einen ganz anderen Zweig der Diskreten Mathematik führt, nämlich in die „abzählende Kombinatorik". Während es in den ersten Abschnitten vielfach darum ging, die Existenz oder Nichtexistenz gewisser Objekte nachzuweisen und Anzahlbetrachtungen gar keine Rolle spielten (oder, wie im Fall der orthogonalen lateinischen Quadrate, nur eine untergeordnete), wird es hier um konkrete Anzahlbestimmungen gehen. Auf eher elementarer Stufe sind uns schon begegnet: $|A|^n$, die Anzahl der n-Tupel aus Elementen der endlichen Menge A; $n!$, die Anzahl der Permutationen einer n-elementigen Menge; und $\binom{n}{k}$, die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge.

Im folgenden wird es zunächst darum gehen, die „Wirkungen" von Gruppen in endliche Mengen zu studieren; numeriert man beispielsweise die acht Ecken eines Würfels im $\mathbb{R}^3$ mit Schwerpunkt im Ursprung mit Zahlen 1 bis 8, so bewirkt jede Drehung, die den Würfel in sich selbst überführt, eine Permutation von $\{1,\dots,8\}$; in diesem Sinne „wirkt" die „Drehgruppe des Würfels" in der Menge $\{1,\dots,8\}$. Eine Eigenschaft dieser Wirkung ist beispielsweise, daß jede Ecke des Würfels durch eine einzige Drehung in jede andere Ecke überführt werden kann.

Oftmals wird es so sein, daß eine „Bewegungsgruppe" auf „Positionen" wirkt. Versieht man jede einzelne Position mit einem „Attribut", zum Beispiel mit einer Farbe oder einem Wert $0,1$, so möchte man zwei „Positionenfärbungen" als gleich ansehen, wenn sie durch die entsprechende Bewegung ineinander überführt werden können. Denkt man sich also Zahlen $0,1$ an die Ecken des Würfels geschrieben, so gibt es nur eine wesentliche Weise der Beschriftung, die mit einer Eins und sieben Nullen auskommt (bzw. nur eine Weise „bis auf Drehung im Raum"); für eine Belegung mit zwei Einsen und sechs Nullen gibt es schon wenigstens drei wesentlich verschiedene Weisen, weil die beiden Einsen entweder auf derselben Kante, gegenüberliegend auf derselben Seite oder räumlich gegenüberliegend auftreten können und sich daran durch eine Drehung nichts ändert.

Wir werden in der kommenden Woche die Anzahl der „zyklischen $0,1$-Folgen" bestimmen; dabei werden zwei gewöhnliche $0,1$-Folgen als gleich angesehen, wenn sie durch „Rotation" auseinander hervorgehen, so daß zum Beispiel

$$1010011, 1110100$$

gleich sind: Verschiebt man 1010011 um zwei Stellen nach rechts und „schiebt" in jedem Schritt die „rechts herausgeschobene Ziffer (beide Male 1) „links wieder herein", so entsteht 1110100. Die „Positionen" der Ziffern kann man sich auch als die Ecken eines regelmäßigen n-Ecks im $\mathbb{R}^2$ um den Ursprung denken; die Drehung um $\frac{2\pi}{n}$ überführt das n-Eck in sich selbst und wirkt somit auf die Positionen. (Abstrakt wirkt die zyklische Gruppe $\mathbb{Z}_n$.) In diesem Sinne kann das zyklisch mit 1010011 an den Ecken beschriftete 7-Eck durch eine Drehung um $2 \cdot \frac{2\pi}{7}$ in das zyklisch mit 1110100 beschriftete 7-Eck überführt werden.

Bei der Analyse der Wirkung von $\mathbb{Z}_n$ kommt ein wenig Zahlentheorie ins Spiel, in Gestalt der EULERschen φ-Funktion; an der Stelle n ist sie gleich der Anzahl der zu n teilerfremden Zahlen zwischen 1 und n, also die Anzahl Zahlen zwischen 1 und n, deren größter gemeinsamer Teiler mit n gleich 1 ist. (Zum Beispiel ist $\phi(7) = 6$, $\phi(1) = 1$, $\phi(4) = 2$.) Das ist Thema der zweiten Hälfte des Stoffs dieser Woche; einstweilen uns das erlauben, den Zyklenindex unter der Wirkung von $\mathbb{Z}_n$ „in sich selbst" anzugeben. Dabei wirkt $\mathbb{Z}_n$ „in sich selbst" in dem Sinne, daß jedes $a \in \mathbb{Z}_n$ eine natürliche Permutation der Elemente von $\mathbb{Z}_n$ bewirkt (die Linkstranslation um a). Das gilt ganz allgemein für jede Gruppe, und so läßt sich auch ein Klassiker der Gruppentheorie beweisen, daß jede Gruppe G isomorph zu einer Gruppe von Permutationen (der Elemente von G) ist.

Zählen unter Gruppenwirkung ist Bestandteil der nach ihrem Erfinder benannten PÓLYA-Theorie, die wir in den kommenden Wochen darstellen möchten.

Ilmenau, den 30. Juni 2020 · Matthias Kriesell

Kapitel 3
Pólya-Theorie

Sei X eine endliche Menge. Mit S_X wird wie üblich die *Gruppe der Permutationen von X* bezeichnet, wobei die Gruppenoperation die *Hintereinanderschaltung* bzw. *Konkatenation* $\circ$ ist. Wir schreiben S_n anstelle von $S_{\mathbb{N}_n}$. Sind $a_1, \ldots, a_\ell$ paarweise verschiedene Elemente aus X, so wird durch

$$\alpha(x) := \begin{cases} a_{i+1} & \text{falls } x = a_i \text{ für ein } i \in \{1, \ldots, \ell - 1\}, \\ a_1 & \text{falls } x = a_\ell \text{ und} \\ x & \text{sonst} \end{cases}$$

eine Permutation α von X definiert, ein sogenannter *Zyklus der Länge ℓ mit den Elementen $a_1, \ldots, a_\ell$*. Schreibweise für dieses α ist

$$(a_1\, a_2\, \ldots\, a_\ell),$$

die sogenannte *Zyklenschreibweise* (mit Klammern, ohne Kommata). Ein Zyklus der Länge höchstens 1 ist stets die Identität. Zyklen ohne gemeinsame Elemente heißen *elementfremd* oder *disjunkt*, und in der Algebra zeigt man, daß sich jede Permutation τ auf eine bis auf die Reihenfolge der Faktoren eindeutige Weise als Produkt disjunkter Zyklen der Länge wenigstens 2 schreiben läßt (die Identität ist dabei gleich dem leeren Produkt). Dazu äquivalent ist, daß sich τ auf eine bis auf die Reihenfolge der Faktoren eindeutige Weise als Produkt von Zyklen schreiben läßt, deren Elementmengen eine Partition von X bilden. Eine solche Faktorisierung heißt *volle Zerlegung* von τ. Dort kommen die Fixpunkte von τ als Zyklen der Länge 1 vor, die Identität ist dann das Produkt der $|X|$ vielen Zyklen der Länge 1. Für uns spielt die Anzahl der Zyklen einer gewissen Länge eine Rolle: Für $\tau \in S_X$ und $j \in \mathbb{N}$ sei

$$c_j(\tau)$$

die Anzahl der Zyklen der Länge j in einer vollen Zerlegung von τ (das ist wohldefiniert, hängt also nicht von der konkreten vollen Zerlegung ab, weil diese ja bis auf die Reihenfolge der Faktoren eindeutig bestimmt ist). Immer gilt $c_j(\tau) = 0$ für $j > |X|$ und weiterhin

$$|X| = \sum_{j=1}^{|X|} j c_j(\tau).$$

Entsprechend heißt die Folge

$$c(\tau) = (c_1(\tau), c_2(\tau), \ldots, c_{|X|}(\tau))$$

das *Zyklenspektrum* bzw. schlicht: der *Typ* von τ. Die Menge S_X zerfällt daher in Klassen gleichen Typs. Im Fall der S_3 kann man wie folgt tabellieren:

τ	$c(\tau)$
$()$	$(3,0,0)$
$(1\,2)$	$(1,1,0)$
$(1\,3)$	$(1,1,0)$
$(2\,3)$	$(1,1,0)$
$(1\,2\,3)$	$(0,0,1)$
$(1\,3\,2)$	$(0,0,1)$

Ist H eine Gruppe von Permutationen von X (also eine Untergruppe von S_X), so heißt das Polynom

$$p_H \in \mathbb{Q}[x_1,\ldots,x_{|X|}],\ p_H(x_1,\ldots,x_{|X|}) := \frac{1}{|H|}\sum_{\tau\in H} x_1^{c_1(\tau)}\cdot\ldots\cdot x_{|X|}^{c_{|X|}(\tau)}$$

der *Zyklenindex* oder *Zyklenindikator* von H. Beispielsweise hat die Untergruppe $\{(),(1\,2)\}$ von S_3 den Zyklenindex

$$p_{\{(),(1\,2)\}}(x_1,x_2,x_3) = \frac{1}{2}(x_1^3 + x_1x_2),$$

der Zyklenindex von S_3 selbst (als Untergruppe von S_3) ist

$$p_{S_3}(x_1,x_2,x_3) = \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3).$$

Als weiteres Beispiel mag die Permutation $(2\,3\,4)$ aus S_5 dienen; sie hat den Typ $(2,0,1,0,0)$ und erzeugt in S_5 die (zyklische) Untergruppe

$$H = \{(),(2\,3\,4),(2\,4\,3)\}$$

mit dem Zyklenindex

$$p_H(x_1,\ldots,x_5) = \frac{1}{3}(x_1^5 + 2x_1^2x_3).$$

Hier kommt ein etwas wirklichkeitsnäheres Beispiel. Sei X die Menge der acht Ecken eines Würfels und H die Menge aller Permutation von X, die sich durch eine (starre) Drehung des Würfels um eine Drehachse durch seinen Mittelpunkt bewirken lassen. Dies ist eine Untergruppe von S_X. Abhängig von der Lage der Drehachse ergeben sich die möglichen Drehwinkel (der gedrehte Würfel muß ja deckungsgleich zum ursprünglichen sein). Der Typ der durch die Drehung bewirkten Permutation hängt zudem vom Drehwinkel ab. Wir tabellieren wie folgt.

Die Drehachse verbindet...	Winkel	Anzahl	Typ
...Mitten gegenüberliegender Seiten	0π	1	$(8,0,0,0,0,0,0,0)$
	π	3	$(0,4,0,0,0,0,0,0)$
	$\frac{1}{2}\pi, \frac{3}{2}\pi$	$2\cdot 3$	$(0,0,0,2,0,0,0,0)$
...Mitten gegenüberliegender Kanten	π	6	$(0,4,0,0,0,0,0,0)$
...zwei gegenüberliegende Ecken	$\frac{2}{3}\pi, \frac{4}{3}\pi$	$2\cdot 4$	$(2,0,2,0,0,0,0,0)$

Insgesamt erhält man $|H| = 24$ Permutationen und kann anhand der Typenhäufigkeiten den Zyklenindex ablesen:

$$p_H(x_1, \ldots, x_8) = \frac{1}{24}(x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2x_3^2).$$

Für das nächste Beispiel beötigen wir „EULERs φ": Für $n \in \mathbb{N}_n$ sei

$$\varphi(n) := |\{k \in \mathbb{N}_n : \, n, k \text{ teilerfremd}\}|.$$

Dabei sind n, k *teilerfremd*, falls ihr größter gemeinsamer Teiler, ggT(n, k), gleich 1 ist. In diesem Sinne ist 1 teilerfremd zu allen Zahlen, auch zu sich selbst. (Daher ist $\varphi(1) = 1$.) Mit Hilfe des Prinzips von Inklusion und Exklusion, Satz 1.8, können wir $\varphi(n)$ in Kenntnis der Primteiler von n bestimmen. Sei

$$n = p_1^{\alpha} \cdot \cdots \cdot p_\ell^{\alpha_\ell}$$

die Primfaktorzerlegung, $p_i \neq p_j$ für $i \neq j$. Für $j \in \mathbb{N}_\ell$ sei

$$A_j := \{x \in \mathbb{N}_n : \, p_j | x\}.$$

Wir bemerken zunächst, daß für einen Teiler d von n es genau n/d Vielfache von d in $\mathbb{N}_n$ gibt, nämlich $d, 2d, 3d, \ldots, (n/d)d$. Wir erhalten mit der Konvention $\bigcap_{j \in \emptyset} A_j = \mathbb{N}_n$ und mit $\prod_{j \in \emptyset} p_j = 1$:

$$\begin{aligned}
\varphi(n) &= n - |\bigcup_{j=1}^{\ell} A_j| \\
&= n - \sum_{s=1}^{\ell} (-1)^{s+1} \sum_{J \in \mathfrak{P}_s(\mathbb{N}_\ell)} |\bigcap_{j \in J} A_j| \\
&= n - \sum_{\substack{J \subseteq \mathbb{N}_\ell \\ J \neq \emptyset}} (-1)^{|J|+1} \, |\bigcap_{j \in J} A_j| \\
&= \sum_{J \subseteq \mathbb{N}_\ell} (-1)^{|J|} \, |\bigcap_{j \in J} A_j| \\
&= \sum_{J \subseteq \mathbb{N}_\ell} (-1)^{|J|} \cdot \frac{n}{\prod_{j \in J} p_j} \\
&= n \cdot \prod_{j=1}^{\ell} (1 - \frac{1}{p_j}).
\end{aligned}$$

Die letzte Identität ergibt sich durch Ausmultiplizieren der rechten Seite. Man erhält zum Beispiel

$$\varphi(6) = 6 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 2 = |\{1, 5\}|.$$

Als weitere vertrauensbildende Maßnahme stellt man für eine Primzahl p fest

$$\varphi(p) = p \cdot (1 - \frac{1}{p}) = p - 1.$$

Für einen Teiler d von n erhält man als Folgerung

$$\begin{aligned} & |\{m \in \mathbb{N}_n : \text{ggT}(m,n) = d\}| \\ = \; & |\{m \in \mathbb{N}_n : m/d, n/d \text{ teilerfremde ganze Zahlen}\}| \\ = \; & \varphi(n/d), \end{aligned}$$

und daraus

$$n = \sum_{m \in \mathbb{N}_n} 1 = \sum_{d|n} \sum_{\substack{m \in \mathbb{N}_n \\ \text{ggT}(m,n)=d}} 1 = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d),$$

wobei sich die letzte Gleichung schlicht daraus ergibt, daß mit d auch n/d alle Teiler von n durchläuft. Zum Beispiel kommt für $n = 6$

$$\sum_{d|6} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6.$$

EULERs φ hat eine wichtige Interpretation in der Theorie der zyklischen Gruppen. Zunächst gilt für $n \geq m \geq 1$: m erzeugt $\mathbb{Z}_n$ genau dann, wenn $\text{ggT}(m,n) = 1$ ist. Besitzen nämlich einerseits m und n einen gemeinsamen Teiler $k > 1$, so ist $(n/k) \cdot m = (m/k) \cdot n$ und damit $(n/k) \cdot m = 0$ in $\mathbb{Z}_n$. Die Ordnung von m in $\mathbb{Z}_n$ ist darum höchstens $n/k < n$, und folglich ist m kein Erzeuger von $\mathbb{Z}_n$. Ist umgekehrt $\text{ggT}(m,n) = 1$ und $k \leq n$ die Ordnung von m, so gilt $k \cdot m = 0$ in $\mathbb{Z}_n$, also $km = \ell n$ für ein $\ell > 0$. Weil m ein Teiler von km und damit von ℓn ist, jedoch teilerfremd zu n, ist m ein Teiler von ℓ. Insbesondere ist $m \leq \ell$, also $k \geq n$ und folglich $k = n$. Daher ist m Erzeuger von $\mathbb{Z}_n$. Die Anzahl der Erzeuger von $\mathbb{Z}_n$, also die Anzahl der Elemente der Ordnung n in $\mathbb{Z}_n$, ist also gleich $\varphi(n)$.

In der Algebra zeigt man, daß eine Untergruppe $H \neq \{0\}$ von $\mathbb{Z}_n$ von demjenigen a aus H mit kleinstem positiven Repräsentanten erzeugt wird, insbesondere selbst wieder zyklisch ist. Hieraus folgt, daß es zu jedem Teiler d von n nur eine Untergruppe der Ordnung d von $\mathbb{Z}_n$ gibt, und zwar die von n/d erzeugte. Diese Untergruppe enthält dann *alle* Elemente der Ordnung d, und sie wird von jedem einzelnen dieser Elemente erzeugt, aber von keinen anderen. Daher gilt auch allgemein:

Lemma 3.1.

Ist d ein Teiler von n so gibt es genau $\varphi(d)$ viele Elemente der Ordnung d in $\mathbb{Z}_n$.

□

Wir betrachten nun die Gruppe $X := \mathbb{Z}_n$ und für $a \in X$ die *Linkstranslation*

$$\lambda_a : X \to X,\ \lambda_a(x) = a + x.$$

Jedes λ_a ist bijektiv, also aus S_X. Tatsächlich ist

$$h : X \to S_X, h(a) := \lambda_a$$

ein Gruppenhomomorphis, denn es gilt

$$\lambda_{a+b}(x) = (a + b) + x = a + (b + x) = \lambda_a(\lambda_b(x)) = (\lambda_a \circ \lambda_b)(x)$$

für alle $x \in X$ und darum

$$h(a + b) = \lambda_{a+b} = \lambda_a \circ \lambda b = h(a) \circ h(b)$$

für alle $a, b \in A$. Aus $h(a) = h(b)$ folgt $\lambda_a = \lambda_b$ und insbesondere $a = a + 0 = \lambda_a(0) = \lambda_b(0) = b + 0 = b$, so daß h injektiv ist. Daher h sogar ein Gruppenisomorphismus von X in die Bildgruppe

$$h(X) = \{\lambda_a : a \in X\}$$

aller Linkstranslationen.[1] Weil Linkstranslationen Permutationen sind, können wir über ihr Zyklenspektrum reden. Ist etwa a ein Element der Ordnung d in X (davon gibt es genau $\varphi(d)$ viele), so bildet λ_a die von a in X erzeugte zyklische Untergruppe H in sich selber ab. Weil a die Ordnung d hat, ist λ_a als Permutation von H ein Zyklus der Länge d. Ist $b + H$ eine Linksnebenklasse von H und $y \in b + H$, also $y = b + qa$ für ein $q \in \mathbb{Z}$, so ist $\lambda_a(y) = \lambda_a(b + qa) = b + (a + qa) = b + \lambda_a(qa)$, so daß die Elemente $b + a, b + 2a, \ldots, b + da$ einen Zyklus der Länge d mit Elementmenge $b + H$ bilden. Folglich besitzt λ_a genau $|G/H| = n/d$ viele Zyklen der Länge d und keine weiteren, also:

$$c_d(\lambda_a) = n/d \text{ und } c_j(\lambda_a) = 0 \text{ für } j \neq d.$$

Somit ist der Zyklenindex von $h(X)$ vollständig bestimmt:

$$p_{h(X)}(x_1, \ldots, x_n) = \frac{1}{n} \sum_{d|n} \varphi(d) x_d^{n/d}.$$

Wir werden diese Feststellungen später benutzen, um zum Beispiel die „zyklischen $\{0, 1\}$-Folgen" zu zählen, wobei zwei $\{0, 1\}$-Folgen als gleich gelten, wenn sie durch „Rotation auseinander hervorgehen".

[1] Dieselbe Idee zeigt, daß *jede* Gruppe isomorph zu einer Gruppe von Permutationen ist.

Übungen (6)

Abgabe bis Freitag den 10. Juli 2020.

Die Aufgaben 4,5,6 können erst mit dem Stoff des 12. Studienbriefes bearbeitet werden.

1. Im 11. Studienbrief wurden die Drehungen des Würfels auf sich selbst betrachtet und die Permutationen der acht Ecken typisiert, die jene bewirken. Behandeln Sie die analoge Fragestellung für die zwölf Kanten des Würfels und bestimmen Sie den Zyklenindex.

2. Eine *zahlentheoretische Funktion* ist eine Abbildung $f : \mathbb{N} \setminus \{0\} \to \mathbb{C}$. Sie heißt *multiplikativ*, wenn $f(a \cdot b) = f(a) \cdot f(b)$ für teilerfremde Zahlen a, b gilt und $f(1) \neq 0$ ist. Man zeige, daß die *Euler*sche φ-Funktion multiplikativ ist.

3. Ein Element a des Rings R mit $1 \neq 0$ heißt *Einheit*, falls es ein $b \in R$ mit $a \cdot b = b \cdot a = 1$ gibt, falls also a ein multiplikativ Inverses besitzt. Die Einheiten bilden eine Gruppe mit $\cdot$, die mit R^* bezeichnet wird. Man zeige, daß
$$|\mathbb{Z}_n^*| = \varphi(n)$$
für den Restklassenring $\mathbb{Z}_n$, $n \geq 2$, gilt, und folgere daraus, daß $\mathbb{Z}_n$ genau dann ein Körper ist, wenn n eine Primzahl ist.

4. Man zeige, daß die im 12. Studienbrief definierte Relation $\sim$ (siehe Orbit) eine Äquivalenzrelation ist.

5. Wieviele Perlenketten (im Sinne des 12. Studienbriefes) der Länge 13 können aus Perlen dreier Farben hergestellt werden? In wievielen davon treten alle drei Farben auf?

6. Wieviele Möglichkeiten gibt es, die sechs Kanten eines regelmäßigen Tetraeders mit zwei Farben zu färben, wobei Färbungen, die sich durch Drehung des Tetraeders auf sich selbst auseinander ergeben, als gleich betrachtet werden?

   Hinweis. Die „Tetraedergruppe" besteht aus 12 Drehungen.