Gruppentheorie
Vorlesung im Sommersemester 2002

Ulrich Brosa, brosa-gmbh@t-online.de

13. Januar 2011

1 Grundgedanke

Anliegen der Gruppentheorie ist die Lösung jedes Problems durch Funktionen, deren Symmetrie schrittweise abnimmt.

Beispiel: Die Fourier-Entwicklung ist ein typisches Ergebnis der Gruppentheorie

$$f(\varphi) = \sum_{n=-\infty}^{+\infty} f_n e^{in\varphi}$$

mit

$$f_n = \frac{1}{2\pi} \int_0^{2\pi} f(\varphi) e^{-in\varphi} d\varphi$$

In nullter Näherung wird die Funktion $f(\varphi)$ durch ihren Durchschnitt genähert

$$f(\varphi) \approx f_0, \quad f_0 = \frac{1}{2\pi} \int_0^{2\pi} f(\varphi) d\varphi$$

In erster Näherung kommen die gröbsten Abweichungen hinzu:

$$f(\varphi) \approx f_0 + f_{+1} e^{+i\varphi} + f_{-1} e^{-i\varphi}$$

usw. In der Ausdrucksweise der Gruppentheorie sind die Funktionen

$$e^{in\varphi}, n = 0, \pm 1, \pm 2, ...$$

die *irreduziblen Darstellungen* der *speziellen orthogonalen Gruppe* im Zweidimensionalen SO_2. Es handelt sich um ein Funktionensystem, dessen Mitglieder schrittweise an Symmetrie verlieren. $e^{i0\varphi}$, eine Konstante, ist die symmetrischste Funktion, die man sich vorstellen kann.

Die Gruppentheorie hat sich aus zwei Wurzeln entwickelt:

1) Lösung algebraischer Gleichungen (Galois),
2) Klassifizierung von Kristallen (Schönflies, Fjodoroff).

Galoisens Ideen wurden auf die

3) Lösung von Differenzialgleichungen (Lie)

übertragen. Aus der Synthese der beiden Ursprünge entstand die

4) Darstellungstheorie (Frobenius).

Verständnis dieser vier Gebiete ist das Ziel der Vorlesung.

Allerdings sollen die Inhalte mit anti-akademischen Methoden vermittelt werden: An die Spitze jedes Kapitels wird ein Lehrsatz gestellt. Direkt danach wird der Satz durch Beispiele zunehmender Schwierigkeit erläutert. Definitionen ergeben sich aus den Beispielen. Beweise werden in den Hintergrund geschoben, zumal sie nichts Anderes sind als Zusammenfassungen der zuvor gebrachten Beispiele. Die StudentInnen haben Erfolg gehabt, wenn sie den Satz vom Anfang des Kapitels am Ende so verstanden haben, dass sie ihn anwenden können.

Der akademische Weg, mit abstrakten Definitionen zu beginnen, daraus irgendwelche Lemmata abzuleiten, schließlich den Hauptsatz zu beweisen und vielleicht ganz am Ende irgendein triviales Beispielchen zu präsentieren, ist widernatürlich. Kein Lebewesen kann so lernen.

2 Lösung algebraischer Gleichungen

Satz von Galois: *Eine algebraische Gleichung kann dann und nur dann algebraisch gelöst werden, wenn die Gruppe der Gleichung derart aus Normalteilern aufgebaut ist, dass deren Indices sämtlich Primzahlen sind.*

Für eine algebraische Lösung werden transzendente Funktionen nicht benötigt. $+, -, *, /, \sqrt[n]{.}$ reichen.

1. Beispiel: quadratische Gleichung. Aus

$$0 = x^2 + a_1 x + a_0 = (x - x_1)(x - x_2)$$

mit gegebenen Koeffizienten a_1 und a_0 sind sofort die Vietáschen Relationen ablesbar:

$$-a_1 = x_1 + x_2, \quad a_0 = x_1 \cdot x_2$$

Ziel sind die Lösungen (*Wurzeln)* x_1 und x_2.

Die Vieta-Relationen sind der quadratischen Gleichung gleichwertig, werden aber meist verworfen, weil sie komplizierter erscheinen. Nichtsdestoweniger geht die Gruppentheorie von den Vieta-Relationen aus.

Auffälligste Eigenschaft ist ihre Symmetrie:

$$x_1 + x_2 = x_2 + x_1, \quad x_1 \cdot x_2 = x_2 \cdot x_1,$$

was auch so geschrieben werden kann:

$$x_1 + x_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} (x_1 + x_2), \quad x_1 \cdot x_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} (x_1 \cdot x_2)$$

Die *Permutation* $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ vertauscht in der auf sie folgenden Funktion das erste mit dem zweiten Argument. Per definitionem ist also

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} f(a,b) = f(b,a).$$

Die Vieta-Relationen bleiben selbstverständlich auch invariant, wenn man die Einheitspermutation $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ auf sie anwendet, d.h. nichts ändert.

Unter der Gruppe einer Gleichung versteht man diejenigen Permutationen, welche die zugehörigen Vieta-Relationen invariant lassen. Bei der der quadratischen Gleichung ist es die *symmetrische Gruppe* S_2, also die Gruppe aller Permutationen von zwei Elementen:

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Die Gruppentheorie löst die Vieta-Relationen, indem sie nicht gleich nach den Lösungen x_1 und x_2 sucht, sondern erst Funktionen berechnet, in denen die Symmetrie in möglichst kleinen Schritten abnimmt. Im vorliegenden Fall ist dies der Unterschied $b = x_1 - x_2$, auch *Diskriminante* genannt. Witzigerweise ist

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} b = -b, \text{ aber } \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} b^2 = b^2$$

b^2 ist somit eine *symmetrische* Funktion, die aus den *symmetrischen Grundfunktionen* $x_1 + x_2$ und $x_1 \cdot x_2$ berechnet werden kann:

$$b^2 - a_1^2 = (x_1 - x_2)^2 - (x_1 + x_2)^2 = -4x_1 \cdot x_2$$

Daraus folgt:

$$b^2 - a_1^2 + 4a_0 = 0 \text{ oder } b = \pm\sqrt{a_1^2 - 4a_0}$$

Sobald b bekannt ist, lassen sich x_1 und x_2 leicht berechnen, z.B.:

$$x_1 - \frac{b}{2} = \frac{x_1 + x_2}{2} \text{ oder } x_1 - \frac{b}{2} + \frac{a_1}{2} = 0 \text{ somit } x_1 = \frac{-a_1 + b}{2}$$

Natürlich ist das die bekannte Lösung der quadratischen Gleichung.

Es sei dringend empfohlen, die letzen drei Formelzeilen trotz ihrer Einfachheit genau nachzuvollziehen. Dahinter steckt das *Waring-Verfahren*, welches bei der Lösung algebraischer Gleichungen unentbehrlich ist.

2. Beispiel: kubische Gleichung.

$$0 = x^3 + a_2x^2 + a_1x + a_0 = (x - x_1)(x - x_2)(x - x_3)$$

sind die Vieta-Relationen

$$-a_2 = x_1 + x_2 + x_3, \quad a_1 = x_1x_2 + x_1x_3 + x_2x_3, \quad -a_0 = x_1x_2x_3$$

gleichwertig. Dazu gehört als Gruppe

$$S_3 = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix} \right\}$$

mit immerhin 3!=6 Elementen.

Eine Menge von Elementen $a, b, c, d, e, ..$ heißt Gruppe G, wenn eine „Multiplikation“ zwischen den Elementen so definiert ist, dass

1) aus $a \in G$ und $b \in G$ auch $ab \in G$ folgt (Vollständigkeit),

2) $(ab)c = a(bc)$ (Assoziativität),

3) ein Element e mit $ea = ae = e$ vorhanden ist (Einselement),

4) es zu jedem a ein a^{-1} mit aa^{-1}=$a^{-1}a$=e gibt (Inverses).

Die „Multiplikation“ von Permutationen wird so definiert, dass die sukzessive Anwendung zweier Permutationen dasselbe ergibt, wie das Resultat der Multiplikation:

$$\begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} f(a, b, c) = f(b, a, c) \quad \text{und} \quad \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} f(b, a, c) = f(c, a, b)$$

also

$$\begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} f(a, b, c) = f(c, a, b) \quad \text{mit} \quad \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}$$

Man muss von rechts nach links rechnen:

auf 1 folgt 2, auf 2 folgt 2. Insgesamt: auf 1 folgt 2.

auf 2 folgt 1, auf 1 folgt 3. Insgesamt: auf 2 folgt 3.

auf 3 folgt 3, auf 3 folgt 1. Insgesamt: auf 3 folgt 1.

Noch ein Beispiel:

$$\begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}$$

Durch Ausführung aller $6 \cdot 6 = 36$ Multiplikationen wird die Vollständigkeit von S_3 bewiesen. Die Assoziativität ergibt sich aus der Konstruktion:

auf i folgt j, auf j folgt k, auf k folgt l usw.

Es ist egal, an welcher Stelle die Kette in zwei Teile zerlegt wird, ob also:

auf i folgt k, auf k folgt l

oder:

auf i folgt j, auf j folgt l.

Das Einselement ist durch $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ gegeben.

Das Inverse wird gefunden, indem man die Permutation auf den Kopf stellt:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Das letzte Gleichheitszeichen gilt, weil es bei der zweizeiligen Darstellung der Permutationen auf die Reihenfolge der Spalten nicht ankommt. Vergleichen Sie das hiesige Resultat mit dem zweiten Beispiel zur Multiplikation.

Die symmetrische Gruppe S_3, obschon sie nur aus 6 Elementen besteht, enthält 5 Untergruppen, von denen jede für sich die 4 Gruppenaxiome erfüllt:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$T_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

$$T_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

$$T_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Unter der *Ordnung* $|G|$ einer Gruppe G ist ihre *Mächtigkeit* zu verstehen. Hier ist $|e| = 1$, $|T_1| = |T_2| = |T_3| = 2$, $|A_3| = 3$, $|S_3| = 6$.

Die drei Transpositionsgruppen T_1, T_2, T_3, in denen außer der Einheit nur eine selbst-inverse Transposition steht, sind von geringerer Bedeutung. Wichtig für die Lösung der kubischen Gleichung sind nur die Einheit und die *alternierende Gruppe* A_3. A_3 ist ein *Normalteiler* der symmetrischen Gruppe S_3, die Einheit ist ein Normalteiler der alternierenden Gruppe.

Damit der Begriff *Normalteiler* erklärt werden kann, müssen die *Ähnlichkeitstransformationen* $\ddot{a} = bab^{-1}$ und die *Ähnlichkeitsklassen* verstanden werden.

Eine *Ähnlichkeitstransformation* wird wie in der linearen Algebra als Wechsel des Koordinatensystems gedeutet. Erfreulicherweise lassen sich die Ähnlichkeitstransformationen von Permutationen besonders einfach berechnen. Natürlich kann man $\ddot{a} = bab^{-1}$ als Inversion und doppelte Multiplikation ausrechnen. Es geht aber viel einfacher. Z.B. mit

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{und} \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

muss man in a alle Zahlen so ersetzen, wie es b vorschreibt:

$$\ddot{a} = bab^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Sprich:
ersetze 1 durch 2,
ersetze 2 durch 1,
ersetze 3 durch 3.
Da dies wie Zauberei erscheinen dürfte, hier der allgemein gültige Beweis des Algorithmus:

$$a = \begin{pmatrix} 1 & \dots & n \\ a_1 & \dots & a_n \end{pmatrix} \text{ und } b = \begin{pmatrix} 1 & \dots & n \\ b_1 & \dots & b_n \end{pmatrix}$$

In b lassen sich die Spalten nach Maßgabe von a permutieren, ohne b zu ändern. Das Ergebnis sei

$$b = \begin{pmatrix} a_1 & \dots & a_n \\ a_{b_1} & \dots & a_{b_n} \end{pmatrix}$$

Und selbstverständlich ist

$$b^{-1} = \begin{pmatrix} b_1 & \dots & b_n \\ 1 & \dots & n \end{pmatrix}$$

Dann müssen wir nur noch hinschreiben

$$\ddot{a} = bab^{-1} = \begin{pmatrix} a_1 & \dots & a_n \\ a_{b_1} & \dots & a_{b_n} \end{pmatrix} \begin{pmatrix} 1 & \dots & n \\ a_1 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 & \dots & b_n \\ 1 & \dots & n \end{pmatrix}$$

und finden

$$\ddot{a} = \begin{pmatrix} b_1 & \dots & b_n \\ a_{b_1} & \dots & a_{b_n} \end{pmatrix},$$

was die Behauptung ist.