Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 9

Das Signum einer Permutation

DEFINITION 9.1. Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Dann heißt die Zahl

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

das *Signum* (oder das *Vorzeichen*) der Permutation σ.

Das Signum ist 1 oder -1, da im Zähler und im Nenner die positive oder die negative Differenz $\pm(i - j)$ steht. Es gibt für das Signum also nur zwei mögliche Werte. Bei $\operatorname{sgn}(\sigma) = 1$ spricht man von einer *geraden Permutation* und bei $\operatorname{sgn}(\sigma) = -1$ von einer *ungeraden Permutation*.

DEFINITION 9.2. Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Dann heißt ein Indexpaar $i < j$ ein *Fehlstand*, wenn $\sigma(i) > \sigma(j)$ ist.

LEMMA 9.3. *Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Es sei $k = \#(F)$ die Anzahl der Fehlstände von σ. Dann ist das Signum von σ gleich*

$$\operatorname{sgn}(\sigma) = (-1)^k .$$

Proof. Wir schreiben

$$\begin{aligned}
\operatorname{sgn}(\sigma) &= \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \prod_{(i,j)\in F} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{(i,j)\notin F} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= (-1)^k \prod_{(i,j)\in F} \frac{\sigma(i) - \sigma(j)}{j - i} \prod_{(i,j)\notin F} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= (-1)^k,
\end{aligned}$$

da nach dieser Umordnung sowohl im Zähler als auch im Nenner das Produkt aller positiven Differenzen steht. □

BEISPIEL 9.4. Wir betrachten die Permutation

x	1	2	3	4	5	6
$\sigma(x)$	2	4	6	5	3	1

SATZ 9.5. *Sei $M = \{1, \ldots, n\}$. Dann ist die Zuordnung*

$$S_n \longrightarrow \{1, -1\},\ \sigma \longmapsto \operatorname{sgn}(\sigma),$$

ein Gruppenhomomorphismus.

Proof. Zunächst ist das Signum wirklich gleich 1 oder -1. Dies beruht darauf, dass sowohl im Zähler als auch im Nenner der Definition des Signums zu jedem Indexpaar $i \leq j$ die positive oder die negative Differenz $\pm(i-j)$ vorkommt.

Das Signum der Identität ist natürlich 1. Seien zwei Permutationen σ und τ gegeben. Dann ist

$$\begin{aligned}
\operatorname{sgn}(\sigma \circ \tau) &= \prod_{i<j} \frac{(\sigma\circ\tau)(j) - (\sigma\circ\tau)(i)}{j-i} \\
&= (\prod_{i<j} \frac{(\sigma\circ\tau)(j) - (\sigma\circ\tau)(i)}{\tau(j)-\tau(i)}) \prod_{i<j} \frac{\tau(j)-\tau(i)}{j-i} \\
&= (\prod_{i<j,\,\tau(i)<\tau(j)} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)})(\prod_{i<j,\,\tau(i)>\tau(j)} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)})\ \operatorname{sgn}(\tau) \\
&= (\prod_{i<j,\,\tau(i)<\tau(j)} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)})(\prod_{i<j,\,\tau(i)>\tau(j)} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)})\ \operatorname{sgn}(\tau) \\
&= \prod_{k<\ell} \frac{\sigma(\ell)-\sigma(k)}{\ell-k} \operatorname{sgn}(\tau) \\
&= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).
\end{aligned}$$

□

LEMMA 9.6. *Sei $M = \{1, \ldots, n\}$ und sei σ eine Permutation auf M. Es sei*

$$\sigma = \tau_1 \cdots \tau_r$$

geschrieben als ein Produkt von r Transpositionen. Dann gilt für das Signum die Darstellung

$$\operatorname{sgn}(\sigma) = (-1)^r.$$

Proof. Die Transposition τ vertausche die beiden Zahlen $k < \ell$. Dann ist

$$\begin{aligned}
\operatorname{sgn}(\tau) &= \prod_{i<j} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{i,j\neq k,\ell} \frac{\tau(j)-\tau(i)}{j-i} \cdot \prod_{i=k, j\neq\ell} \frac{\tau(j)-\tau(i)}{j-i} \cdot \prod_{i\neq k, j=\ell} \frac{\tau(j)-\tau(i)}{j-i} \cdot \prod_{i=k,j=\ell} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{j>k,\,j\neq\ell} \frac{j-\ell}{j-k} \cdot \prod_{i\neq k,\,i<\ell} \frac{k-i}{\ell-i} \cdot \frac{k-\ell}{\ell-k} \\
&= \prod_{j>\ell} \frac{j-\ell}{j-k} \cdot \prod_{i<k} \frac{k-i}{\ell-i} \cdot \prod_{k<j<\ell} \frac{j-\ell}{j-k} \cdot \prod_{k<i<\ell} \frac{k-i}{\ell-i} \cdot (-1) \\
&= -1.
\end{aligned}$$

Die letzte Gleichung ergibt sich daraus, dass im ersten und im zweiten Produkt alle Zähler und Nenner positiv sind und dass im dritten und im vierten Produkt die Zähler negativ und die Nenner positiv sind, so dass sich diese (wegen der gleichen Indexmenge) Minuszeichen wegkürzen.

Die Aussage folgt dann aus der Gruppeneigenschaft. □

Bemerkung 9.7. Es sei I eine beliebige Menge mit n Elementen, die nicht geordnet sein muss. Dann kann man nicht von Fehlständen sprechen und die Definition des Signums ist nicht direkt anwendbar. Man kann sich jedoch an Lemma 9.12 orientieren, um das Signum auch in dieser leicht allgemeineren Situation zu erklären. Dazu schreibt man eine Permutation σ auf I als Produkt von r Transpositionen und definiert

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 \text{ falls } r \text{ gerade ist} \\ -1 \text{ falls } r \text{ ungerade ist.} \end{cases}$$

Um einzusehen, dass dies wohldefiniert ist, betrachtet man eine Bijektion

$$\varphi : I \longrightarrow \{1, \ldots, n\}.$$

Die Permutation σ auf I definiert auf $\{1, \ldots, n\}$ die Permutation $\sigma' = \varphi\sigma\varphi^{-1}$. Sei $\sigma = \tau_1 \cdots \tau_r$ eine Darstellung als Produkt von r Transpositionen auf I. Dann gilt

$$\sigma' = \varphi\sigma\varphi^{-1} = \varphi\tau_1 \cdots \tau_r\varphi^{-1} = \varphi\tau_1\varphi^{-1}\varphi\tau_2\varphi^{-1}\varphi \cdots \varphi^{-1}\varphi\tau_r\varphi^{-1} = \tau_1'\tau_2' \cdots \tau_r'$$

mit $\tau_j' = \varphi\tau_j\varphi^{-1}$. Dies sind ebenfalls Transpositionen, sodass die Parität von r durch das Signum von σ' festgelegt ist.

Die alternierende Gruppe

Für $n \geq 2$ ist die Signumsabbildung $\operatorname{sgn} : S_n \to \{1, -1\}$ ein surjektiver Gruppenhomomorphismus, da ja Transpositionen auf -1 abgebildet werden. Der Kern dieses Homomorphismus besteht aus allen geraden Permutationen und ist ein Normalteiler in der Permutationsgruppe S_n. Diese Untergruppe bekommt einen eigenen Namen.

Definition 9.8. Zu $n \in \mathbb{N}$ heißt die Untergruppe

$$A_n = \{\sigma \in S_n | \operatorname{sgn}(\sigma) = 1\} \subseteq S_n$$

der geraden Permutationen die *alternierende Gruppe*.

Die alternierende Gruppe besitzt ($n \geq 2$) den Index zwei, die beiden Nebenklassen sind die geraden Permutationen und die ungeraden Permutationen.

Für $n = 1, 2$ ist die alternierende Gruppe die triviale Gruppe. Für $n = 3$ ist $A_3 = \mathbb{Z}/(3)$. Die Gruppe A_4 ist isomorph zur Tetraedergruppe.

Beispiel 9.9. Wir betrachten die alternierende Gruppe A_4. Die vier Permutationen (in Zykeldarstellung)

$$\mathrm{id},\ \langle 1,2\rangle\langle 3,4\rangle,\ \langle 1,3\rangle\langle 2,4\rangle,\ \langle 1,4\rangle\langle 2,3\rangle$$

bilden darin eine kommutative Untergruppe V, in der jedes Element $\neq \mathrm{id}$ die Ordnung 2 besitzt. Sie ist isomorph zur Kleinschen Vierergruppe. Es handelt sich sogar um einen Normalteiler vom Index drei. Um dies einzusehen verwenden wir Lemma 7.8 und betrachten exemplarisch $\sigma = \langle 1,2\rangle\langle 3,4\rangle$ und $\tau = \langle 1,2,3\rangle$ mit dem Inversen $\tau^{-1} = \langle 1,3,2\rangle$. Wir erhalten

$$\langle 1,2,3\rangle\langle 1,2\rangle\langle 3,4\rangle\langle 1,3,2\rangle = \langle 1,4\rangle\langle 2,3\rangle\,,$$

was wieder zu V gehört. Die Restklassengruppe A_4/V muss isomorph zu $\mathbb{Z}/(3)$ sein, die beiden anderen (neben V) Nebenklassen sind einerseits die Dreierzykel

$$N = \langle 2,3,4\rangle,\ \langle 1,4,3\rangle,\ \langle 1,2,4\rangle,\ \langle 1,3,2\rangle$$

und andererseits die dazu inversen Dreierzykel

$$\langle 2,4,3\rangle,\ \langle 1,3,4\rangle,\ \langle 1,4,2\rangle,\ \langle 1,2,3\rangle\,.$$

Wenn man einen Tetraeder mit nummerierten Ecken anschaut, so entsprechen diese beiden Nebenklassen den Dritteldrehungen im Uhrzeigersinn oder entgegen dem Uhrzeigersinn um die Seiteneckachsen, wobei die Drehrichtung dadurch festgelegt ist, dass man auf den Eckpunkt schaut (welche Orientierung zu welcher Nebenklasse gehört, hängt dabei von der Nummerierung der Ecken ab).

Die Gruppe A_4 besitzt also einen nicht-trivialen Normalteiler. Sie ist damit unter den alternierenden Gruppen eine Ausnahme. Es gilt nämlich, und das werden wir hier nicht beweisen, dass die alternierenden Gruppen A_n, $n \geq 5$ einfach sind im Sinne der folgenden Definition.

Definition 9.10. Eine Gruppe heißt *einfach*, wenn sie genau zwei Normalteiler enthält (nämlich sich selbst und die triviale Gruppe).

Für eine Primzahl p sind die zyklischen Gruppen $\mathbb{Z}/(p)$ der Ordnung p einfach, da es in diesen Gruppen aufgrund des Satzes von Lagrange überhaupt nur die triviale und die ganze Gruppe als Untergruppe gibt. In einer nicht kommutativen einfachen Gruppe gibt es im Allgemeinen sehr viele Untergruppen, aber eben keine nicht-trivialen Normalteiler. Die einfachen Gruppen sind in gewissem Sinne die einfachsten Bausteine für alle endlichen Gruppen. Die nicht einfachen Gruppen sind in einem gewissen Sinn „zusammengesetzt“, da es dort dann einen echten Normalteiler $N \subset G$, $N \neq 0, \neq G$ gibt und damit auch eine Restklassengruppe $G/N = Q$. Die Gruppe G ist dann aus den kleineren Gruppen N und Q irgendwie „zusammengebastelt“, wobei allerdings N und Q nicht die Struktur von G festlegen. Die Klassifikation aller einfachen endlichen Gruppen war ein schwieriges Problem der Gruppentheorie und ist inzwischen (seit ca. 1980) gelöst.

Die Determinante

Wir erinnern noch kurz an die Determinante, die aus der Anfängervorlesung bekannt ist. Mittels Permutationen und deren Signa kann man eine geschlossene Definition für die Determinante geben. Zur Berechnung sind aber rekursive Verfahren sinnvoller.

DEFINITION 9.11. Zu einer $n \times n$-Matrix

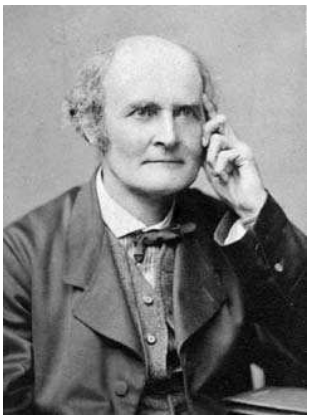
$$M = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ . & \dots & . \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

heißt

$$\det M = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

die *Determinante* von M.

Der Satz von Cayley



Arthur Cayley (1821-1895)

Zu einer Gruppe G und einem Element $g \in G$ nennt man die Abbildung

$$L_g : G \longrightarrow G,\ x \longmapsto gx$$

die *Linksmultiplikation* mit g. Das ist in aller Regel *kein* Gruppenhomomorphismus, allerdings ist es eine bijektive Abbildung der Menge G in sich. Dieser Zusammenhang wird nun kurz thematisiert.

LEMMA 9.12. *Sei G eine Gruppe und $\operatorname{Perm}(G)$ die Gruppe der Bijektionen auf G. Dann ist die Abbildung, die einem Gruppenelement die Linksmultiplikation zuordnet, also*

$$G \longrightarrow \operatorname{Perm}(G),\ g \longmapsto L_g,$$

ein injektiver Gruppenhomomorphismus.

Proof. Die Linksmultiplikation ist eine Bijektion auf G, da aus $gx = gy$ durch Multiplikation von links mit g^{-1} sofort $x = y$ folgt. Wegen $ex = x$ geht das neutrale Element auf die Identität. Ferner ist für jedes $x \in G$

$$L_{g\tilde{g}}(x) = (g\tilde{g})x = g(\tilde{g}x) = g(L_{\tilde{g}}(x)) = L_g(L_{\tilde{g}}(x)) = (L_g L_{\tilde{g}})(x),$$

was $L_{g\tilde{g}} = L_g L_{\tilde{g}}$ bedeutet. Daher ist die Zuordnung ein Gruppenhomomorphismus. Zur Injektivität verwenden wir Lemma 5.12. Es sei also $L_g = \mathrm{id}\,$. Dann ist aber sofort

$$g = ge = L_g(e) = \mathrm{id}\,(e) = e.$$

□

Satz 9.13. *(Satz von Cayley)*

Jede Gruppe lässt sich als Untergruppe einer Permutationsgruppe realisieren. Jede endliche Gruppe lässt sich als Untergruppe einer endlichen Permutationsgruppe realisieren.

Proof. Dies folgt sofort aus Lemma 5.12. □

Bemerkung 9.14. Es gilt sogar, dass mit Ausnahme der Identität jede Linksmultiplikation fixpunktfrei ist. D.h. die Untergruppe der Permutationen, die isomorph zur vorgegebenen Gruppe ist, besitzt außer der Identität nur fixpunktfreie Abbildungen. Dies folgt aus $gx = L_g(x) = x$ durch Multiplikation mit x^{-1} von rechts.

Beispiel 9.15. Sei $G = \mathbb{Z}/(n)$ eine zyklische Gruppe, repräsentiert durch die Elemente $\{0, 1, \ldots, n-1\}$. Das Einselement 1 erzeugt die Gruppe, das muss dann auch für die zu G isomorphe Untergruppe von S_n gelten. Die Linksaddition mit 1 ist die Zuordnung

$$0 \mapsto 1,\ 1 \mapsto 2,\ 2 \mapsto 3, \ldots, n-2 \mapsto n-1,\ n-1 \mapsto 0\,.$$

Das ist also ein Zykel der Ordnung n. Das Element k geht auf die k-fache Hintereinanderausführung dieses Zykels.

Abbildungsverzeichnis