Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Anhang 3

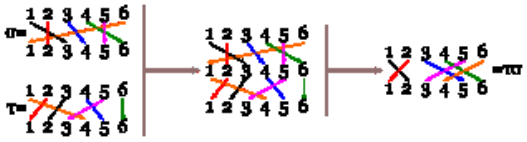
Permutationsgruppen

DEFINITION 3.1. Zu einer Menge M nennt man die Menge

$$\operatorname{Aut}(M) = \operatorname{Perm}(M) = \{\varphi : M \longrightarrow M | \, \varphi \text{ bijektiv}\}$$

der bijektiven Selbstabbildungen die *Automorphismengruppe* oder die *Permutationsgruppe* zu M.

Eine bijektive Selbstabbildung $\varphi : M \to M$ nennt man auch eine *Permutation*. Für eine endliche Menge $I = \{1, \ldots, n\}$ schreibt man $S_n = \operatorname{Perm}(I)$. Eine endliche Permutation kann man bspw. mit einer (vollständigen) Wertetabelle oder mit einem Pfeildiagramm beschreiben.



LEMMA 3.2. *Sei M eine endliche Menge mit n Elementen. Dann besitzt die Permutationsgruppe* $\operatorname{Perm}(M) \cong S_n$ *genau $n!$ Elemente.*

Beweis. Es sei $M = \{1, \ldots, n\}$. Für die 1 gibt es n mögliche Bilder, für 2 gibt es noch $n-1$ mögliche Bilder, für 3 gibt es noch $n-2$ mögliche Bilder, usw. Daher gibt es insgesamt

$$n(n-1)(n-2)\cdots 2 \cdot 1 = n!$$

mögliche Permutationen. □

LEMMA 3.3. *Sei M eine Menge und $N \subseteq M$ eine Teilmenge. Dann gibt es eine natürliche injektive Abbildung*

$$\operatorname{Perm}(N) \longrightarrow \operatorname{Perm}(M), \, \sigma \longmapsto \tilde{\sigma},$$

wobei $\tilde{\sigma}$ auf N gleich σ und auf $M \setminus N$ die Identität ist. Mittels dieser Abbildung ist $\operatorname{Perm}(N)$ *eine Untergruppe von* $\operatorname{Perm}(M)$.

Beweis. Offenbar ist die Abbildung wohldefiniert. Sie ist injektiv, da aus $\tilde{\sigma} = \tilde{\tau}$ sofort folgt, dass $\sigma = \tau$ ist. Die Abbildung liefert eine Bijektion zwischen $\operatorname{Perm}(N)$ und der Menge der Permutationen auf M, die $M \setminus N$ fest lassen. Diese Permutationen bilden eine Untergruppe. □

Zykeldarstellung für Permutationen

Sei M eine endliche Menge, $\sigma \in \mathrm{Perm}\,(M)$ eine Permutation und $x \in M$. Dann kann man die Folge

$$\sigma^0(x) = \mathrm{id}\,(x) = x,\ \sigma^1(x) = \sigma(x),\ \sigma^2(x),\ \sigma^3(x) \ldots,$$

betrachten. Da M endlich ist, gibt es eine Wiederholung $\sigma^i(x) = \sigma^j(x)$ mit $i < j$. Durch Multiplikation mit σ^{-i} sieht man, dass es ein minimales $k \in \mathbb{N}_+$ gibt mit $\sigma^k(x) = \sigma^0(x) = x$, und dass alle $\sigma^j(x)$ für j, $1 \leq j < k$, verschieden sind. Ist $y = \sigma^j(x)$, so durchläuft auch $\sigma^i(y)$ dieselbe Teilmenge aus M.

Definition 3.4. Sei M eine endliche Menge und σ eine Permutation auf M. Man nennt σ einen *Zykel der Ordnung* r, wenn es eine r-elementige Teilmenge $Z \subseteq M$ gibt derart, dass σ auf $M \setminus Z$ die Identität ist und σ die Elemente aus Z zyklisch vertauscht. Wenn $Z = \{z, \sigma(z),\ \sigma^2(z), \ldots, \sigma^{r-1}(z)\}$ ist, so schreibt man einfach

$$\sigma = \langle z, \sigma(z),\ \sigma^2(z), \ldots, \sigma^{r-1}(z) \rangle\,.$$

Dabei kann man statt z jedes andere Element aus Z als Anfangsglied nehmen. Die Menge Z heißt auch der *Wirkungsbereich* des Zykels, und die (geordnete) Auflistung heißt die *Wirkungsfolge* des Zykels.

Definition 3.5. Eine *Transposition* auf einer endlichen Menge M ist eine Permutation auf M, die genau zwei Elemente miteinander vertauscht und alle anderen Elemente unverändert lässt.

Eine Transposition ist also ein besonders einfacher Zykel mit der Zyklendarstellung $\langle x, y \rangle$, wenn die Transposition die Punkte x und y vertauscht.

Lemma 3.6. *Jede Permutation auf einer endlichen Menge M kann man als Produkt von Transpositionen schreiben.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl der Menge M. Für $\#(M) = 1$ ist nichts zu zeigen, sei also $\#(M) \geq 2$. Die Identität ist das leere Produkt aus Transpositionen. Sei also σ nicht die Identität, und sei $\sigma(x) = y \neq x$. Es sei τ die Transposition, die x und y vertauscht. Dann ist y ein Fixpunkt von $\sigma\tau$, und man kann $\sigma\tau$ auffassen als eine Permutation auf $M' = M \setminus \{y\}$. Nach Induktionsvoraussetzung gibt es dann Transpositionen τ_j auf M' mit $\sigma\tau = \prod_j \tau_j$ auf M'. Dies gilt dann auch auf M, und daher ist $\sigma = \prod_j \tau_j \tau$. □

Satz 3.7. *Sei M eine endliche Menge und σ eine Permutation auf M. Dann gibt es eine Darstellung*

$$\sigma = \sigma_1 \cdots \sigma_k\,,$$

wobei die σ_i Zykel der Ordnung ≥ 2 sind mit disjunkten Wirkungsbereichen. Dabei ist die Darstellung bis auf die Reihenfolge eindeutig.

Beweis. Es sei F die Fixpunktmenge von σ und es seien $Z_1, \ldots, Z_k$ diejenigen Teilmengen von M mit mindestens zwei Elementen derart, dass σ die Elemente aus jedem Z_i zyklisch vertauscht. Dann ist M die disjunkte Vereinigung aus F und den Z_i. Zu i, $1 \leq i \leq k$ sei σ_i der Zykel auf M, der auf $M \setminus Z_i$ die Identität ist und auf Z_i mit σ übereinstimmt. Wir behaupten

$$\sigma = \sigma_1 \cdots \sigma_k \, .$$

Um dies einzusehen, sei $x \in M$ beliebig. Bei $x \in F$ ist x ein Fixpunkt für alle σ_i und daher kommt links und rechts wieder x raus. Sei also x kein Fixpunkt der Permutation. Dann gehört $x \in Z_i$ für genau ein i. Für alle $j \neq i$ ist x ein Fixpunkt von σ_j. Da $y = \sigma(x)$ ebenfalls zu Z_i gehört, ist auch y ein Fixpunkt von σ_j für alle $j \neq i$. Wendet man daher die rechte Seite auf x an, so wird x auf x abgebildet bis man zu σ_i kommt. Dieses bildet x auf y ab und die folgenden σ_j bilden y auf y ab, so dass die rechte Seite insgesamt x auf y schickt und daher mit σ übereinstimmt. □

Aufgrund von diesem Satz können wir allgemein eine Zyklendarstellung für eine beliebige Permutation definieren.

Definition 3.8. Sei M eine endliche Menge und σ eine Permutation auf M. Es seien $Z_1, \ldots, Z_k$ die Wirkungsbereiche der Zyklen von σ mit $n_i = \#(Z_i)$. Es sei $x_i \in Z_i$ und $Z_i = \{x_i, \sigma(x_i), \ldots, \sigma^{n_i-1}(x_i)\}$. Dann nennt man

$$\langle x_1, \sigma(x_1), \ldots, \sigma^{n_1-1}(x_1)\rangle\langle x_2, \sigma(x_2), \ldots, \sigma^{n_2-1}(x_2)\rangle \cdots \langle x_k, \sigma(x_k), \ldots, \sigma^{n_k-1}(x_k)\rangle$$

die *Zyklendarstellung* von σ.

Das Signum einer Permutation

Definition 3.9. 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 3.10. 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 3.11. *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*

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

Beweis. 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 3.12. Wir betrachten die Permutation

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

mit der Zyklendarstellung

$$\langle 124536\rangle\,.$$

Die Fehlstände sind

$$(1,6),\ (2,5),\ (2,6),\ (3,4),\ (3,5),\ (3,6),\ (4,5),\ (4,6),\ (5,6)\,,$$

also 9 Stück. Das Signum ist also $(-1)^9 = -1$ und die Permutation ist ungerade.

Satz 3.13. *Sei $M = \{1,\ldots,n\}$. Dann ist die Zuordnung*

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

ein Gruppenhomomorphismus.

Beweis. Zunächst ist das Signum wirklich gleich 1 oder -1. Dies beruht dadrauf, 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

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

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

□

LEMMA 3.14. *Sei $M=\{1,\dots,n\}$ 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

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

Beweis. 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. □

Abbildungsverzeichnis