Automorphismen und Untergruppen von S_n und A_n

Vortrag zum Seminar zur Gruppentheorie, 05.10.2015

Annika Sachtje

Wie der Titel bereits vermuten lässt ist der Vortrag zweigeteilt. Erst befassen wir uns mit den äußeren Automorphismen der A_n, dann mit dem äußeren Automorphismus der S_6. Im zweiten Abschnitt werden dann die Untergruppen von S_n (bzw. A_n) erläutert, wobei wir hier von intransitiven zu transitiven und von imprimitiven zu primitiven Untergruppen übergehen, bevor wir uns den affinen Untergruppen und den Untergruppen des diagonalen Typs widmen werden. All dies dient letztlich als Vorarbeit für den Satz von O'Nan-Scott, welcher im nächsten Vortrag besprochen werden wird.

§1 Äußere Automorphismen

Wir beginnen mit den äußeren Automorphismen der alternierenden Gruppen. Nach einer kurzen Wiederholung arbeiten wir uns anhand einiger Lemmata zu dem Hauptsatz des Abschnittes vor, der die Automorphismen der alternierenden Gruppen in Zusammenhang zu den Symmetrischen Gruppen setzt.

— *Automorphismen der alternierenden Gruppen* —

Zunächst rufen wir uns einige Aussagen aus der Computeralgebra ins Gedächtnis. Für die Beweise dazu sei jedoch auf die Computeralgebra-Vorlesung von Prof. Nebe im Sommersemester 2015 verwiesen.

(1.1) Lemma
Die alternierende Gruppe A_n (mit $n > 2$) wird von ihren 3-Zykeln erzeugt.

(1.2) Lemma
Für $n \geq 4$ hat die alternierende Gruppe A_n triviales Zentrum, also $Z(A_n) = \{1\}$

(1.3) Lemma
Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.

(1.4) Satz
Sei G Gruppe, dann gilt: $G/Z(G) \cong Inn(G)$

(1.5) Bemerkung
$Inn(G) \trianglelefteq Aut(G)$

(1.6) Lemma
Für $n \geq 5$ besitzt A_n keine Untergruppe, deren Index kleiner ist als n.

Beweis
Annahme: Es existiert eine Untergruppe $G < A_\mathrm{n}$ mit Index $k < n$.

Dann operiert A_n auf A_n/G durch Linksmultiplikation, weshalb ein Homomorphismus $\phi : A_\mathrm{n} \to S_\mathrm{k}$ existiert, wobei $S_\mathrm{k} \cong Sym(A_\mathrm{n}/G)$ gilt. Da A_n mit $n \geq 5$ eine einfache Gruppe ist, muss ϕ entweder trivial oder injektiv sein. Injektivität kann in unserem Fall nicht gelten, da die S_k kleinere Ordnung hat als die A_n. Somit bliebe noch der triviale Homomorphismus $\phi = 1$. Dann würde allerdings folgendes gelten:

$$gG = G \qquad \text{für alle } g \in A_n,$$

was wiederum bedeuten würde, dass $G = A_n$ gilt.
Dies jedoch steht im Widerspruch zu der Tatsache, dass wir G als echte Untergruppe von A_n gewählt haben.
Die obige Annahme war folglich falsch und eine solche Untergruppe existiert nicht. □

(1.7) Folgerung
Sei M eine Menge, $n \geq 5$. Operiert A_n auf M treu (nicht trivial), so gilt $|M| \geq n$

Beweis
A_n operiere auf der Menge M, dann gilt nach dem Bahnensatz und mit Lemma (1.6), da der Stabilisator eine Untergruppe bildet:

$$|M| = \frac{|A_n|}{|Stab_{A_n}(m)|} \geq n \qquad \text{mit } m \in M$$

□

Um den Hauptsatz dieses Abschnittes beweisen zu können, müssen wir uns noch von der Richtigkeit des folgenden Lemmas überzeugen:

(1.8) Lemma
Sei $n \in \{4, 5\}$ oder $n \geq 7$ und $A_{n\text{-}1} \cong G \leq A_n$. Dann gilt:

G ist der Stabilisator einer der n Punkte, in der natürlichen A_n-Menge.

Beweis
Im Fall $n \in \{4,5\}$ lässt sich dies leicht durch die Bestimmung der Untergruppen verifizieren, bzw. aus dem Untergruppenverband ablesen.

Annahme: $G \neq Stab_{A_n}(i)$ für alle $i \in \{1,...,n\}$
Nehmen wir weiter an, dass G nicht transitiv auf den n Punkten operiert. Daraus folgt, dass es mehr als eine Bahn geben muss und für eine Bahn $B_1 \subset \{1,...,n\}$ gilt:

$$\{1,...,n\} = B_1 \cup \{1,...,n\} \setminus B_1$$

Da G auf $\{1,...,n\}$ operiert, operiert G auf eben jenen Bahnen und nach Lemma (1.6) gilt: $|B_1| \geq n-1$, sodass nach obiger Gleichung $1 \leq |\{1,...,n\} \setminus B_1| \leq 1$ gelten muss. Dies ist jedoch durch unsere Annahme, G sei kein Stabilisator eines Punktes aus $\{1,...,n\}$, bereits ausgeschlossen.
Wir stoßen somit auf einen Widerspruch, woraus folgt, dass unter unserer Annahme G transitiv auf $\{1,...,n\}$ operieren muss. Um zu zeigen, dass auch die Annahme der transitiven Operation falsch ist und G doch Stabilisator einer der n Punkte sein muss, machen wir folgende Fallunterscheidung:
Fall $n = 7$:
Nach dem Bahnensatz gilt:

$$|G| = |G \cdot i| \cdot |Stab_G(i)| \qquad \text{mit } i \in \{1,...,n\}$$

Da G transitiv auf {1,...,n} operiert, gilt $|G \cdot i| = 7$, aber $7 \nmid |A_6| = 360$.
Die ist ein Widerspruch zu unserer allerersten Annahme, also kann G nicht transitiv auf {1,...,n} operieren und muss ein Stabilisator sein.

Für $n \geq 8$ betrachten wir nun ein anderes Argument:

Fall $n > 8$:
Laut Voraussetzung gilt $G \cong A_{n-1}$, dieser Isomorphismus sei fortan mit ϕ bezeichnet.
Behauptung: Der Isomorphismus $\phi : A_{n-1} \to G$ schickt 3-Zykel auf 3-Zykel.

Sei $g = \phi((a,b,c))$, das Bild eines 3-Zykels aus A_{n-1}, mit $a,b,c \in \{1,...,n-1\}$ verschieden. Es gilt $C_G(g) \leq G \leq A_n$ und $C_G(g) \cong C_{A_{n-1}}((a,b,c))$.Sodass unter Anwendung von ϕ gilt:

$$C \cong C_G(g)/\langle g \rangle \cong C_{A_{n-1}}((a,b,c))/\langle (a,b,c) \rangle \cong A_{n-4}$$

Wir betrachten nun die Bahnen der Operation von C auf $\{1,...,n\}$. Seien $E_1,...,E_l$ diese Bahnen, welche der Größe nach absteigend geordnet seien. Da $C \cong A_{n-4}$ und $n-4 \geq 5$ ist, gilt mit Lemma (1.6) erneut:

$$|E_1| \geq n-4 \qquad \text{oder} \qquad |E_1| = 1$$

Da $C \neq \{id\}$ gilt, kann nicht $|E_1| = 1$ und somit $|E_i| = 1$ für alle $i \in \{1, ..., n\}$ gelten, sodass $|E_1| \geq n - 4$ gelten muss.
Aus $g = \phi((a, b, c))$ wissen wir, dass g Ordnung drei haben muss und somit Produkt disjunkter 3-Zykel ist, sei also $g = (g_1, g_2, g_3)(g_4, g_5, g_6)$....
Angenommen es gelte $g_1 \in E_1$, dann folgt:

$$\text{Für alle } \epsilon \in E_1 \text{ existiert ein } \gamma \in C \text{ mit } \gamma(g_1) = \epsilon$$

Und weiter gilt:

$$^{\gamma}g = (\epsilon, \gamma(g_2), \gamma(g_3)) \text{ etc.}$$

Demnach müssen alle Elemente von E_1 in 3-Zykeln von g vorkommen. Dies bedeutet insbesondere, dass 3 die Bahnenlänge von E_1 teilen muss und dass es ein den Zykeln entsprechendes Blocksystem $\mathcal{B} = \{\{g_1, g_2, g_3\}, ...\}$ für $C \cong A_{n-4}$ geben muss. Dies wiederum induziert einen Homomorphismus

$$\varphi : A_{n-4} \to S_{\frac{|E_1|}{3}}$$

Da wir uns im Fall $n > 8$ befinden, ist A_{n-4} einfach, sodass φ nur injektiv oder trivial sein kann. Für die Injektivität müsste gelten:

$$(n-4)! \leq (\frac{|E_1|}{3})! \leq (\frac{n}{3})!$$

Dies stellt jedoch einen eindeutigen Widerspruch dar, denn es gilt $n > 8$.
Auch die Trivialität kann ausgeschlossen werden, da gilt: $\frac{|E_1|}{3} \geq \frac{n-4}{3} > \frac{7-4}{3} = 1$. Demzufolge, kann g kein Element aus E_1 enthalten und muss somit auf den restlichen 4 Punkten operieren, also einen 3-Zykel darstellen.

Wir betrachten diese Elemente von G nun etwas genauer:
Die Elemente, die $(1, 2, 3)$ bzw. $(1, 2, 4)$ in $A_{\text{n-1}}$ entsprechen, erzeugen eine zu A_4 isomorphe Untergruppe. Die beiden Elemente haben folglich (a, b, c) bzw. (a, b, d) als Abbild unter ϕ in A_{n}. Auf gleiche Weise müssen die Elemente, die $(1, 2, j)$ entsprechen auf Elemente (a, b, x) aus A_{n} abgebildet werden. Daraus folgt, dass die Bilder der $n - 3$ Erzeuger genau $n - 1$ Punkte permutieren.
Somit ist bewiesen, dass G einer der, zu $A_{\text{n-1}}$ isomorphen, Stabilisatoren eines Punktes sein muss.

<u>Fall $n = 8$</u>:
Angenommen $\phi((a, b, c)) = (1, 2, 3)(4, 5, 6) = g$.
Dann gilt $C = C_G(g)/\langle g \rangle \cong C_{A_7}((a, b, c))/\langle (a, b, c) \rangle \cong A_4$ und
$C_{A_8}(g) = \langle (1, 4)(2, 5)(3, 6)(7, 8), (1, 2, 3), (4, 5, 6) \rangle$.

Es gilt aber $|C| = 12 \nmid 18 = |C_{A_8}(g)|$. Dieser Widerspruch zwingt uns erneut dazu 3-Zykel auf 3-Zykel zu schicken. Dies führt dann bei genauerer Betrachtung wie im Fall $n > 8$ dazu, dass G nur Stabilisator eines der n Punkte seien kann. □

Mit diesen Erkenntnissen können wir uns nun der eigentlichen Aussage dieses Abschnittes widmen:

(1.9) Satz
Für $n \in \{4, 5\}$ und $n \geq 7$ gilt stets $Aut(A_n) \cong S_n$

Beweis
Jedes $\phi \in Aut(A_\mathrm{n})$ operiert auf der Menge aller Untergruppen von A_n isomorph zu A_{n-1}. Nach Lemma (1.8) genügt es also die Operation von $Aut(A_n)$ auf den Stabilisatoren von $\{1, ..., n\}$ zu betrachten. Die Stabilisatoren stehen in natürlicher Bijektion zu den n Punkten, sodass oben genannte Operation folgenden Homomorphismus induziert:

$$\psi : Aut(A_n) \to S_n, \phi \mapsto (i \mapsto j \quad \text{mit } \phi(Stab_{A_n}(i)) = Stab_{A_n}(j))$$

Es bleibt zu zeigen, dass ψ ein Isomorphismus ist.
Surjektivität:
Jede Permutation $\pi \in S_n$ induziert einen Automorphismus $\kappa_\pi \in Aut(A_n)$, wobei gilt:

$$\kappa_\pi(\sigma) = \pi\sigma\pi^{-1} \qquad , \sigma \in A_n$$

Und es gilt stets $\psi(\kappa_\pi) = \pi$.
Injektivität:
Sei $\phi \in Aut(A_n)$ mit $\psi(\phi) = id$, dann folgt $\phi(Stab_{A_n}(i)) = Stab_{A_n}(i)$ für alle $i \in \{1, ..., n\}$. Es besteht also die Möglichkeit, dass ϕ einen Zykel $(a, b, c, d, ...)$ auf einen Zykel $(b, a, c, d, ...)$ schickt (wir beschränken uns hier auf die Vertauschung von zwei Punkten, es gilt aber analog für alle Möglichen Zykelpermuationen innerhalb eines Stabilisators. Dann würde ϕ den Zykel $(a, c, d, ...)$ aus dem Stabilisator von b auf den Zykel $(b, c, d, ...)$ schicken, welcher offensichtlich nicht in $Stab_{A_n}(b)$ enthalten ist. Da dies für alle Stabilisatoren und somit für alle Punkte gelten muss, muss auch ϕ die Identität gewesen sein. □

Als einfaches Beispiel betrachten wir dazu den Fall $n = 4$.
Der Fall $n = 5$ ist analog zu behandeln.

(1.10) Beispiel
Sei $n = 4$, A_4 die alternierende Gruppe vom Grad 4. Dann gilt

$$Aut(A_4) \cong S_4$$

Um uns dies zu verdeutlichen betrachten wir den Untergruppenverband von A_4:

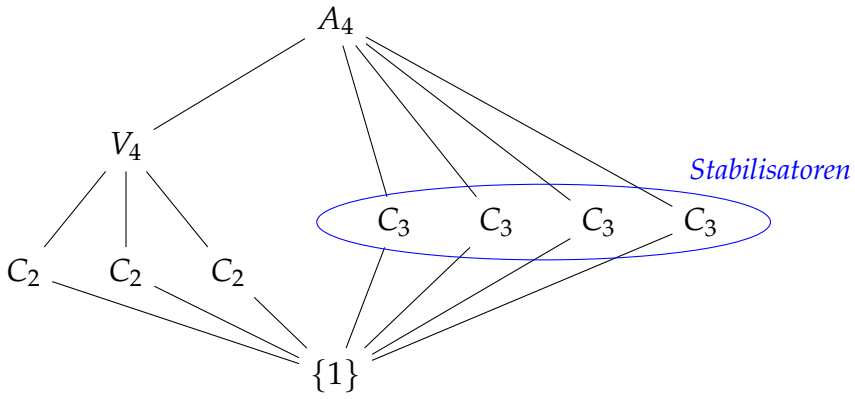

Abbildung 1: Untergruppenverband

Wir wissen bereits, dass es genügt die 4 Stabilisatoren zu betrachten. Diese nummerieren wir nun derart, dass gilt:

$$i := Stab_{A_n}(i) \quad \text{für alle } i \in \{1, ..., 4\}$$

Kombinatorisch ist bereits klar, dass es $4! = 4 \cdot 3 \cdot 2 \cdot 1$ Möglichkeiten gibt, die Stabilisatoren miteinander zu vertauschen und mit der genannten Bezeichnung entspricht jede dieser Permutationen einem Element aus S_4.

Nach den Automorphismen der alternierenden Gruppen wollen wir uns nun mit den äußeren Automorphismen der symmetrischen Gruppen befassen.

— *Der äußere Automorphismus der S_6* —

In diesem Unterabschnitt betrachten wir die S_6 etwas genauer, da diese durch äußere Automorphismen aus den anderen symmetrischen Gruppen hervorsticht.

(1.11) Lemma
Es existiert eine Untergruppe $G \leq S_6$ mit $|G| = 5!$, welche kein Stabilisator von einem Punkt aus $\{1, ..., 6\}$ ist.

Beweis
Wir werden dieses Lemma konstruktiv beweisen.
Da die Untergruppe $G \cong S_5$ kein Stabilisator sein soll, also keinen der 6 Punkte fix lassen darf, muss sie transitiv auf der Menge $\{1, ..., 6\}$ operieren. Betrachten wir hierzu die S_5, so stellen wir fest, dass diese sechs 5-Sylowgruppen hat, hier mit $P_1, ..., P_6$ bezeichnet. Diese 5-Sylowgruppen stehen in Bijektion zu der Menge $\{1, ..., 6\}$. Die Konjugation der S_5 auf ihren 5-Sylowgruppen ist dann die gesuchte transitive Operation und induziert einen Homomorphismus

$$\psi : S_5 \to S_6, \pi \mapsto (i \mapsto j \quad \text{mit} \quad {}^{\pi}(P_i) = P_j)$$

Damit haben wir also nun eine transitive Untergruppe $G = \psi(S_5)$ konstruiert, welche offensichtlich Index 6 hat. Demzufolge operiert die S_6, durch die natürliche Rechtsmultiplikation, transitiv auf den 6 Rechtsrestklassen der Untergruppe G.
D.h.:

$$\phi : S_6 \to S_M \cong S_6 \qquad mit \;\; M = \{Gm | m \in S_6\}$$

ist ein Gruppenhomomorphismus.
Der Kern von ϕ ist trivial, umfasst also nur die Identität, da die S_6 nur triviale Normalteiler von Index größer oder gleich 6 besitzt.

Damit ist ϕ folglich sogar ein Isomorphismus und insbesondere ein Automorphismus.
Um zu zeigen, dass ϕ eben jener besonder äußere Automorphismus ist, bleibt nun noch sicherzustellen, dass gilt:

$$\phi \notin Inn(S_6)$$

Innere Automorphismen erhalten die Transitivität, ϕ jedoch bildet die transitive Untergruppe G auf den Stabilisator der trivialen Rechtsrestklasse G ab. □

(1.12) Satz
Es gilt $Aut(S_6) \cong Aut(A_6) \cong S_6 \rtimes C_2$.
[1]

Der Beweis dazu sei im folgenden nur skizziert.

Beweis
Betrachten wir ein $\phi \in Out(S_6)$, so schickt ϕ 3-Zykel auf doppel-3-Zykel und doppel-3-Zykel auf 3-Zykel. Wenn wir dann untersuchen, wie ϕ^2 abbildet, so stellen wir fest, dass es ein innerer Automorphismus ist, wonach sich die obige Struktur ergibt:

$$Aut(S_6) = Inn(S_6) \rtimes P \cong S_6 \rtimes C_2$$

mit $P = \langle \phi \rangle$, wobei ϕ ein äußerer Automorphismus von Ordnung 2 ist. □

§2 Untergruppen der S_n

In diesem Abschnitt befassen wir uns nun mit den Untergruppen der S_n, als Vorarbeit für den Satz von O'Nan-Scott.

(2.1) Satz
Sei $A_n \neq H < S_n$, dann ist H eine Untergruppe einer oder mehrerer der folgenden Untergruppen:

(i) einer intransitiven Gruppe $S_k \times S_m$, mit $n = k + m$

(ii) einer imprimitiven Gruppe $S_k \wr S_m$, mit $n = km$

(iii) eines primitiven Kranzproduktes $S_k \wr S_m$, mit $n = k^m$

(iv) einer affinen Gruppe $AGL_k(p) \cong C_p^k \rtimes GL_k(p)$, mit $n = p^k$

(v) einer Gruppe der Form $T^k.(Out(T) \times S_k)$,
mit T nicht-abelscher, einfacher Gruppe, die auf den Restklassen einer Untergruppe $Aut(T) \times S_k$ operiert, wobei $n = |T|^{k-1}$ gilt

(vi) einer fast einfachen Gruppe,
welche auf den Restklassen einer maximalen Untergruppe von Index n operiert.

Als sinnvolle Strategie bietet es sich an zunächst die maximalen Untergruppen von S_n zu bestimmen und dann beliebige Untergruppen als Untergruppen der maximalen Untergruppen von S_n zu behandeln. Daher werden wir uns in diesem Abschnitt mit einigen wichtigen Klassen von Untergruppen beschäftigen, die häufig auch maximal sind. Die Maximalität werden wir jedoch nicht in allen Fällen nachweisen.

— *Intransitive Untergruppen* —

Intransitive Untergruppen von S_n besitzen mindestens zwei Bahnen auf der Menge $\{1, .., n\}$. Sei G eine solche Untergruppe, dann gilt $G \leq Sym(B_1) \times ... \times Sym(B_r) \cong S_{n_1} \times ... \times S_{n_r}$, wobei n_i die Längen der r Bahnen B_i von G sind und die S_{n_i} diejenigen Permutationen enthalten, die die Punkte der i-ten Bahn ausschließlich innerhalb dieser Bahn vertauschen und alle anderen Punkte festlassen.
In diesem Unterabschnitt gelte als globale Notation: B_i sind die Bahnen von G auf $\{1, ..., n\}$ und n_i seien jeweils die Länge der Bahn.
Je nach Anzahl der Bahnen gilt folgendes:

(2.2) Lemma
Sei $G \leq S_n$ und besitze mehr als zwei Bahnen auf $\{1,..,n\}$, dann kann G nicht maximal sein.

Beweis
Definiere

$$H := S_{n_1} \times S_{n_2+ \ldots + n_r}$$

dann gilt $G < H < S_n$.
Also ist G keine maximale Untergruppe. □

(2.3) Lemma
Sei $G \leq S_n$ und besitze genau zwei Bahnen auf $\{1,..,n\}$, sodass gilt: $G \cong S_k \times S_{n-k}$ mit $k = n_1$.
Dann ist G eine maximale Untergruppe von S_n, falls $k \neq n - k$

Beweis
Sei ohne Einschränkung $k < n - k$. Die Untergruppe S_k operiere auf $B_1 := \{1,..,k\}$ und S_{n-k} operiere auf $B_2 := \{k+1,..,n\}$. Sei außerdem $\sigma \in S_n \setminus G$ und $K := \langle G, \sigma \rangle \leq S_n$.
Um zu beweisen, dass G maximal ist, müssen wir zeigen, dass K alle Transpositionen von S_n enthält und somit schon die gesamte S_n bildet.
Da $\sigma \notin G$, muss es einen Punkt aus B_2 mit einem aus B_1 vertauschen. Gleichzeitig gilt $|B_2| > |B_1|$, sodass σ nicht mit allen Punkten aus B_2 so verfahren kann. Es existieren also $i, j \in B_2$, sodass $\sigma(i) \in B_1$ und $\sigma(j) \in B_2$ gilt. Für diese Punkte gilt weiterhin:

$$(i,j) \in G \qquad \textit{und} \qquad (\sigma(i), \sigma(j)) \in {}^{\sigma}G \leq K$$

Konjugieren wir nun letztere Transposition mit Elementen aus G, so erhalten wir alle Transpositionen aus S_n, die nicht sowieso bereits in G enthalten sind.
Daher folgt $K = S_n$, womit bewiesen ist, dass G eine maximale Untergruppe von S_n ist. □

(2.4) Beispiel
Maximale Untergruppen der S_6 sind unter anderen

$$S_5 \qquad \text{und} \qquad S_4 \times S_2$$

Da G aus Lemma (2.2) eine beliebige intransitive Untergruppe von S_n war, haben wir somit alle intransitiven, und dementsprechend auch alle maximalen intransitiven Untergruppen der S_n klassifiziert.

(2.5) Folgerung
Sei $G \leq S_n$ eine intransitive Untergruppe, dann gilt $G \leq S_{n_1} \times ... \times S_{n_r}$.
Gilt sogar $G = S_{n_1} \times S_{n-n_1}$ und $n_1 \neq n - n_1$, so ist G maximale Untergruppe von S_n.

Sei also von nun an die Untergruppe $G \leq S_n$ stets transitiv.

— Transitive imprimitive Untergruppen —

Im Bereich der transitiven maximalen Untergruppen befassen wir uns vorerst mit jenen Untergruppen, die zudem imprimitiv sind.

Betrachten wir dazu zunächst noch einmal die Situation aus Lemma (2.3), jedoch nun für $k = n - k$. Der Beweis zu diesem Lemma wird in diesem Fall hinfällig, da eine Permutation aus S_{2k} existiert, welches die beiden Bahnen vermischt und im Normalisator von $S_k \times S_k$ enthalten ist.
Die Untergruppe $S_k \times S_k$ ist tatsächlich nicht maximal.
Ein Beispiel für ein solches Element wäre die Permutation $(1, k+1)(2, k+2)...(k, 2k)$.
Genau betrachtet haben wir es hier also mit dem Kranzprodukt $S_k \wr S_2$ zu tun.

(2.6) Lemma
Das Kranzprodukt $S_k \wr S_2$ ist eine maximale Untergruppe von S_{2k}.

Allgemeiner betrachtet bedeutet dies:

(2.7) Lemma
Für $k > 1, m > 1$ und $n = km$ gilt:

Das Kranzprodukt $S_k \wr S_m$ ist maximale Untergruppe der S_n

Beweis
S_k operiert auf $\{1, .., k\}$ und S_m operiert auf $\{1, ..., m\}$. Dadurch lässt sich folgende Operation von $S_k \wr S_m$ auf $\{1, ..., k\} \times \{1, ..., m\}$ definieren:

$$\phi : S_k \wr S_m \times (\{1, ..., k\} \times \{1, ..., m\}) \to \{1, ..., k\} \times \{1, ..., m\}, (\pi, \varphi)(a, i) \mapsto (\pi_{\varphi(i)}(a), \varphi(i))$$

Wir weisen nach, dass dies eine wohldefinierte Operation ist. Seien $(\pi, \varphi), (\sigma, \psi) \in S_k \wr S_m$ mit $\pi = (\pi_1, ..., \pi_m), \sigma = (\sigma_1, ..., \sigma_m), a \in \{1, ..., k\}$ und $i \in \{1, ..., m\}$.

$$(\pi, \varphi)((\sigma, \psi)(a, i)) = (\pi, \varphi)(\sigma_{\psi(i)}(a), \psi(i)) = (\pi_{\varphi(\psi(i))}(\sigma_{\psi(i)}(a)), \varphi(\psi(i))$$

$$= (\pi_{\varphi\psi(i)}\sigma_{\varphi^{-1}(\varphi(\psi(i)))}(a), \varphi(\psi(i)))$$

$$= ((\pi_1\sigma_{\varphi^{-1}(1)}, ..., \pi_m\sigma_{\varphi^{-1}(m)}), \varphi\psi)(a,i)$$
$$= ((\pi,\varphi)(\sigma,\psi))(a,i)$$

Wenn wir nun $(a,i) \in \{1,...,k\} \times \{1,...,m\}$ mit $k \cdot (i-1) + a$ identifiizeren, so ist dies eine Operation auf km Punkten, sodass $S_k \wr S_m$ eine Untergruppe der S_n mit $n = km$ ist. Wir bekommen außerdem ein Blocksystem $\mathcal{B} = \{B_1, ..., B_m\}$ mit $B_i = \{k \cdot (i-1) + 1, ..., k \cdot (i-1) + k\}$ und $S_k \wr S_m$ enthält nur die Permutationen aus S_{km}, die diese Blöcke stabilisieren. Es gilt also:

$$S_k \wr S_m = Stab_{S_{km}}(\{B_1, ..., B_m\}) \qquad \square$$

Nun zeigen wir noch, dass $S_k \wr S_m$ tatsächlich maximale Untergruppe von S_{km} ist. Angenommen es gäbe eine Untergruppe $H \leq S_{km}$ mit $S_k \wr S_m < H \leq S_{km}$.
Dann kann H nur triviale Blöcke haben und ist somit primitiv. Da $S_k \wr S_m$ 2-Zykel enthält, muss auch H diese 2-Zykel enthalten. Nach Huppert [[2], Seite 171, Satz 4.5] gilt somit bereits $H = S_{km}$.

(2.8) Beispiel
Betrachten wir die Gruppe S_6, so sind die einzigen beiden transitiven imprimitiven maximalen Untergruppen gegeben durch:

$$S_2 \wr S_3 = (S_2 \times S_2 \times S_2) \rtimes S_3 = \langle (1,2), (3,4), (5,6), (1,3,5)(2,4,6), (1,3)(2,4) \rangle$$

und

$$S_3 \wr S_2 = \langle (1,2,3), (1,2), (4,5,6), (4,5), (1,4)(2,5)(3,6) \rangle$$

(2.9) Folgerung
Ist $G < S_n$ eine transitive imprimitive Untergruppe der symmetrischen Gruppe vom Grad n, so hat G die Form:

$$G = S_k \wr S_m \qquad \text{mit } k > 1, m > 1 \in \mathbb{N} \text{ passend und } n = km$$

Gelte also von nun an: G primitiv.

— *Primitive Kranzprodukte* —

Diesen wollen wir uns mit einem Beispiel nähern.
Dazu betrachten wir die S_n mit $n = k^2$ und ordnen die n Punkte der Grundmenge in einer $k \times k$-Matrix an. Wenn wir nun eine Kopie von S_k die Spalten vertauschen lassen, ohne die Menge der Zeilen zu beeinflussen und eine zweite Kopie die Zeilen auf gleiche Weise vertauschen lassen, so erhalten wir aufgrund der Kommutativität dieser beiden Kopien von S_k, eine Gruppe

$$G \cong S_k \times S_k.$$

Da sowohl die Zeilen als auch die Spalten jeweils ein imprimitives System bilden, ist diese Gruppe imprimitiv, also nicht wonach wir suchen. Nehmen wir allerdings die Spiegelung an der Hauptdiagonalen hinzu, die Spalten auf Zeilen abbildet und umgekehrt, erhalten wir das Kranzprodukt $S_k \wr S_2$, welches wiederum sehr wohl primitiv ist.

(2.10) Beispiel
Das Kranzprodukt $S_3 \wr S_2$ beispielsweise ist eine primitive Untergruppe der S_9. Sie ist jedoch nicht maximal.
Es gilt:

$$S_3 \wr S_2 = \langle (1,4)(2,5)(3,6), (1,7)(2,8)(3,9), (4,7)(5,8)(6,9), (1,2)(4,5)(7,8),$$
$$(1,3)(4,6)(7,9), (2,3)(5,6)(8,9), (2,4)(3,7)(6,8) \rangle$$

(2.11) Bemerkung
Der kleinste maximale Fall ist das Kranzprodukt $S_5 \wr S_2$ als primitive Untergruppe der S_{25}.

(Zur Veranschaulichung der Einbettung siehe Abbildung 2 am Ende des Dokuments)

Wenn wir diese Konstruktion für m Dimensionen verallgemeinern, also für $n = k^m$ mit $k > 2, m > 1$ ebenso verfahren, erhalten wir eine primitive Operation des Kranzproduktes $S_k \wr S_m$ auf k^m Punkten.

$$\omega : S_k \wr S_m \times \{1, ..., k\}^m \to \{1, ..., k\}^m \overset{1:1}{\longleftrightarrow} \{1, ..., n\}$$
$$(((\pi_1, ..., \pi_m), \phi), (a_1, ..., a_m)) \mapsto (\pi_{\phi^{-1}(1)}(a_{\phi^{-1}(1)}), ..., \pi_{\phi^{-1}(m)}(a_{\phi^{-1}(m)}))$$

(2.12) Definition
Oben genannte Operation ω des Kranzproduktes wird oft auch „**Produktoperation**“ genannt, um sie von der imprimitiven Operation auf km Punkten aus dem vorherigen Abschnitt unterscheiden zu können.

Die Maximalität dieser Untergruppen von S_n bzw. A_n werden wir hier nicht beweisen. Es sei aber erwähnt, dass folgendes gilt:

(2.13) Satz
Primitive Kranzprodukte sind maximal

- *in* A_n, *falls* $k \geq 5$ *und* $4 \mid k^{m-1}$
- *in* S_n, *falls* $k \geq 5$ *und* $4 \nmid k^{m-1}$

— Affine Untergruppen —

Wie der Titel bereits sagt, befassen wir uns nun mit den affinen Untergruppen der S_n bzw. A_n, mit $n = p^k$.
Affine Gruppen sind im Wesentlichen die Symmetriegruppen von Vektorräumen.

Sei $\mathcal{V}$ der Vektorraum von k-Tupeln in $\mathbb{F}_p$ mit p prim. Dann hat dieser Vektorraum p^k Elemente und hat die Symmetriegruppe

$$AGL_k(p) \cong T \rtimes GL_k(p)$$

genannt die affine generelle lineare Gruppe. Hierbei ist $T \cong C_p^k$ die Gruppe der Translationen $t_a : v \mapsto v + a$. Diese ist ein Normalteiler von $AGL_k(p)$ und isomorph zur additiven Gruppe des Vektorraumes, welche wiederum isomorph zum k-fachen direkten Produkt der zyklischen Gruppe C_p ist.
Die affine generelle lineare Gruppe operiert treu auf $\mathcal{V}$ als Vertauschung der Vektoren und kann somit als Untergruppe der S_n mit $n = p^k$ interpretiert werden.

(2.14) Beispiele

1. $AGL_3(2) \cong C_2^3 \rtimes GL_3(2)$ ist affine Gruppe und permutiert die Vektoren des Vektorraumes ${\mathbb{F}_2}^3$ kann also in S_8 eingebettet werden.

   In diesem Fall gilt sogar, dass alle Permutationen von $AGL_3(2)$ gerade sind, diese Gruppe also tatsächlich bereits in A_8 eingebettet werden kann.

2. Die $AGL_1(7) \cong C_7 \rtimes C_6$ ist sogar maximale Untergruppe der S_7

   $AGL_1(7) \cap A_7 \cong C_7 \rtimes C_3$ ist jedoch nicht maximal in A_7

— Untergruppen des diagonalen Typs —

Diese Gruppen sind nicht so einfach zu beschreiben. Ich werde daher zunächst einige Definitionen anbringen um das nötige Vorwissen zu gewährleisten.

(2.15) Definition
Gegeben seien Gruppen G und K. Eine ***Erweiterung*** *von K mit G ist ein Tripel (H, ϵ, ν), das aus einer Gruppe H, einem Monomorphismus $\epsilon : G \to H$*
und einem Epimorphismus $\nu : H \to K$ mit

$$Kern(\nu) = \epsilon(G)$$

besteht.

Bezeichnung: $H = G.K$
[3]

(2.16) Beispiel
Jeder Normalteiler N einer Gruppe H liefert eine Erweiterung $N.(H/N)$,
wobei ϵ die Inklusionsabbildung und ν der kanonische Epimorphismus ist.
[3]

Mit diesem Wissen können wir uns nun den Untergruppen der S_n des diagonalen Typs widmen.

Diese werden aus einer nicht abelschen einfachen Gruppe T gebildet und haben folgende Form:

$$G = T^k.(Out(T) \times S_k) \cong (T \wr S_k).Out(T)$$

Diese Untergruppen bestehen also aus einem Normalteiler $T \wr S_k$ von G, der durch die Gruppe der äußeren Automorphismen, welche auf die selbe Weise auf allen k Kopien von T operiert, erweitert wird.
Die Gruppe G besitzt eine diagonale Untergruppe $D = \{(t, ..., t) | t \in T\}$, sowie eine Untergruppe H, für die gilt:

$$D < H = D.(Out(D) \times S_k) \leq G$$

Die Untergruppe H hat Index $|T|^{k-1}$, daher ergibt die Permutationsoperation der Gruppe G auf den Restklassen der Untergruppe H eine Einbettung in die S_n mit $n = |T|^{k-1}$.

(2.17) Beispiel
Die kleinste solche Gruppe ist die $(A_5 \times A_5) \rtimes (C_2 \times C_2)$, welche auf den Restklassen einer Untergruppe $S_5 \times C_2$ operiert.

— *Fast einfache Gruppen* —

Zuletzt kommen wir schließlich zu den fast einfachen primitiven Gruppen.

(2.18) Definition
Eine Gruppe G heißt ***fast einfach****, wenn gilt:*

$$T \leq G \leq Aut(T)$$

für eine einfache Gruppe T.

Eine fast einfache Gruppe besteht also aus einer einfachen Gruppe, die möglicherweise durch einige Elemente oder sogar die gesamte Automorphismengruppe erweitert wurde.

(2.19) Lemma
Sei G eine fast einfache Gruppe und M eine beliebige maximale Untergruppe von G, dann gilt:
G lässt sich als primitive Untergruppe von S_n mit $n = [G : M]$ einbetten.

Dies gilt da die Permutationsoperation von G auf den Restklassen von M primitiv ist.

Beweis
Als Beweis sei hier lediglich die Einbettung angegeben, die Verifikation per Nachrechnen sei dem geneigten Leser überlassen.

Sei M maximale Untergruppe von G, sodass gilt: $T \leq M \leq G \leq Aut(M) \leq Aut(T)$. Dann operiert G auf den Restklassen $G/M = \{g_1M, ..., g_nM\}$ und es ergibt sich die Einbettung:

$$\omega : G \to S_n, \;\; \pi \mapsto (i \mapsto j \;\; \text{mit } \pi g_i M = g_j M) \qquad \square$$

Die Klasse der fast einfachen maximalen Untergruppen von S_n gänzlich zu bestimmen ist für uns allerdings zu schwierig, da dieses Problem vollständiges Wissen über die maximalen Untergruppen von allen fast einfachen Gruppen erfordern, was ein in sich noch schwierigeres Problem darstellt.

Es sei daher dabei belassen, dass Liebeck, Praeger und Saxl festgestellt haben, dass - unter bestimmten technischen Bedingungen - jede Einbettung wie in Lemma 2.19 maximal ist, sofern sie nicht in deren Liste von Ausnahmen angeführt ist.
Zudem ist bekannt, dass für n gegen unendlich für fast alle Werte von n keine fast einfachen Untergruppen von S_n bzw. A_n existiert.

Literatur

[1] http://www.mathematik.tu-dortmund.de/~swagner/alg13/alg1-8.pdf, Zugriff 24.09.2015

[2] Huppert,B.:Endliche Gruppen I (Band 134), Springer-Verlag 1967

[3] https://www.minet.uni-jena.de/algebra/skripten/gt/gt-2010/gt.pdf, Zugriff 07.09.2015

Von diesen Quellen abgesehen basiert die Ausarbeitung auf dem Buch „The finite simple groups“ von R.Wilson.

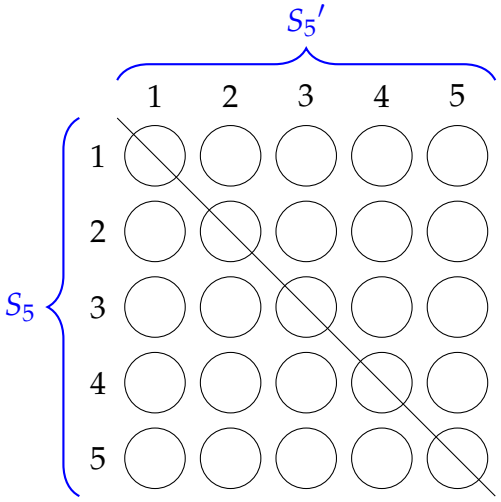

Abbildung 2: Einbettung von $S_5 \wr S_2$ in S_{25}