Norbert Klingen

Permutationsgruppen

Köln WS 2007/08

Inhalt

§1 Permutationsgruppen 1
a. Operationen auf Mengen. 1
Anwendungsbeispiel: Die Sylowsätze. 6
b. Transitive Permutationsdarstellungen. 10
c. Der Permutationscharakter. 12

§2 Mehrfache Transitivität, Primitivität 14
a. Mehrfache Transitivität. 14
b. Primitivität. 17
c. Die Sätze von Jordan. 21

§3 Bestimmung von Galoisgruppen 27
a. Die Galoisgruppe eines Polynoms. 27
b. Die Diskriminante. 29
c. Galoisgruppen über $\mathbb{Q}$ 32
d. Beispiele. 34

§1 Permutationsgruppen

a. Operationen auf Mengen. Sei Ω eine (endliche) Menge. $S_\Omega = S(\Omega)$ bezeichne die Menge aller Permutationen (= bijektiven Selbstabbildungen) von Ω. Wir schreiben für $\sigma \in S_\Omega$ und $a \in \Omega$ $\sigma a := \sigma(a)$. Für eine Permutation $\sigma \in S_\Omega$ nennen wir die von σ 'bewegten' Elemente in Ω den *Träger* von σ: 1/17.10.

$$\mathrm{Tr}\,\sigma = \{a \in \Omega \mid \sigma a \neq a\}\,.$$

Offenbar gilt $\mathrm{Tr}\,\sigma = \mathrm{Tr}\,\sigma^{-1}$ (denn $\sigma a \neq a \iff a \neq \sigma^{-1}a$) und $\sigma^{-1}\mathrm{Tr}\,\sigma = \mathrm{Tr}\,\sigma$ (denn $a \in \mathrm{Tr}\,\sigma \iff \iff \sigma a \neq a \iff \sigma a \neq \sigma(\sigma a) \iff \sigma a \in \mathrm{Tr}\,\sigma \iff a \in \sigma^{-1}\mathrm{Tr}\,\sigma$). Durch Anwendung von σ folgt auch $\mathrm{Tr}\,\sigma = \sigma\mathrm{Tr}\,\sigma$.

(1.1) Proposition: *Es sei Ω eine (endliche) Mengen und $\sigma, \rho \in S_\Omega$ elementfremde Permutationen, d. h. ihre Träger seien disjunkt: $\mathrm{Tr}\,\sigma \cap \mathrm{Tr}\,\rho = \emptyset$. Dann gilt:*

a) σ und ρ sind vertauschbar: $\sigma \circ \rho = \rho \circ \sigma$.

b) $(\sigma \circ \rho)^k = \mathrm{id}_\Omega \iff \sigma^k = \mathrm{id}_\Omega = \rho^k$.

c) Die Ordnung von $\sigma \circ \rho$ ist das kleinste gemeinsame Vielfache der einzelnen Ordnungen:

$$\mathrm{ord}\,\sigma \circ \rho = \mathrm{kgV}(\mathrm{ord}\,\sigma, \mathrm{ord}\,\rho)\,.$$

Beweis: a) Für $a \notin \mathrm{Tr}\,\sigma \cup \mathrm{Tr}\,\rho$ gilt $\sigma a = a = \rho a$, also $\sigma \circ \rho(a) = \rho \circ \sigma(a)$.
Ist $a \in \mathrm{Tr}\,\sigma$, so auch $\sigma a \in \mathrm{Tr}\,\sigma$ und wegen der Elementfremdheit $a, \sigma a \notin \mathrm{Tr}\,\rho$, also $\rho a = a$ und $\rho(\sigma a) = \sigma a$ und daher $\sigma \circ \rho(a) = \sigma a = \rho \circ \sigma(a)$.
Genauso schließt man für $a \in \mathrm{Tr}\,\rho$. Insgesamt gilt $\rho \circ \sigma = \sigma \circ \rho$.
b) Wegen der Vertauschbarkeit $\sigma \circ \rho = \rho \circ \sigma$ gilt $(\sigma \circ \rho)^k = \sigma^k \circ \rho^k$ und damit folgt $\Longleftarrow$ von b).
$\Longrightarrow$: Ist $a \in \mathrm{Tr}\,\sigma$, so folgt $\sigma^\nu a \in \mathrm{Tr}\,\sigma$ und daher $\sigma^\nu a \notin \mathrm{Tr}\,\rho$, also $\rho(\sigma^\nu a) = \sigma^\nu a$. Daraus ergibt sich dann induktiv $(\sigma \circ \rho)^k a = \sigma^k a$, also $\sigma^k a = a$. Für $a \notin \mathrm{Tr}\,\sigma$ gilt diese Gleichung erst recht, also folgt $\sigma^k = \mathrm{id}_\Omega$. Für ρ argumentiert man genauso. □

Sind $l \geq 2$ und $a_1, \ldots, a_l \in \Omega$ verschieden, so versteht man unter dem *Zyklus* $(a_1, \ldots, a_l)$ die Permutation σ, die diese Elemente zyklisch vertauscht, d. h.

$$\sigma(a_i) = a_{i+1}\ (1 \leq i < l)\,, \quad \sigma(a_l) = a_1\,, \quad \sigma(b) = b \text{ sonst}\,.$$

Man nennt l die *Länge* des Zyklus $(a_1, \ldots, a_l)$. *Transpositionen* sind Zyklen der Länge 2.

(1.2) Proposition: *Seien Ω und S_Ω wie oben.*
a) Jede Permutation $\sigma \in S_\Omega$ besitzt eine (bis auf die Reihenfolge) eindeutige Darstellung als Produkt elementfremder Zyklen (die sog. Zyklenzerlegung von σ).
b) Ist $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ ein Produkt elementfremder Zyklen σ_i der Längen $l_1 \geq l_2 \geq \ldots \geq l_r \geq 2$, so nennen wir $(l_1, \ldots, l_r)$ den Zyklentyp von σ. Der Zyklentyp $(l_1, \ldots, l_r)$ eines $\sigma \in S_\Omega$ bestimmt die folgenden Invarianten von σ:

- *das Signum* $\mathrm{sign}(\sigma) = (-1)^{\sum_{i=1}^{r}(l_i - 1)}$,
- *die Ordnung* $\mathrm{ord}(\sigma) = \mathrm{kgV}(l_1, \ldots, l_r)$,
- *die Konjugationsklasse $C(\sigma)$ in S_Ω:*

$$C(\sigma) := \{\tau^{-1}\sigma\tau \mid \tau \in S_\Omega\} = \{\rho \in S_\Omega \mid \rho \text{ hat Zyklentyp } (l_1, \ldots, l_r) \text{ von } \sigma\}\,.$$

Beweis: a) Existenz: Die Identität ist das *leere* Produkt von Zyklen. Sei also σ nicht die Identität. Dann wählt man $a_1 \in \mathrm{Tr}\,\sigma \neq \emptyset$ beliebig, definiert dann rekursiv $a_{i+1} = \sigma a_i$ sowie $l \geq 2$ minimal mit der Eigenschaft $a_{l+1} = a_1$. Dann operiert σ auf der Menge $\{a_1, \ldots, a_l\}$ genauso wie der Zyklus $\sigma_1 = (a_1, \ldots, a_l)$. Also bleiben diese Elemente unter $\sigma' = \sigma_1^{-1} \circ \sigma$ fest, so dass $\mathrm{Tr}\,\sigma' \subsetneq \mathrm{Tr}\,\sigma$. Induktiv (über die Mächtigkeit des Trägers) erhält man die Existenzaussage von a).

Eindeutigkeit: Ist nun $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_s$ *irgendeine* Zerlegung in elementfremde Zyklen, so muss einer der Zyklen den Punkt a_1 bewegen. Da die Zyklen wegen der Elementfremdheit vertauschbar

sind, kann o. E. angenommen werden, dass dies σ_1 ist. Dann folgt, dass σ_1 mit σ auf $\{a_1, \ldots, a_l\}$ übereinstimmt, der oben zuerst konstruierte Zyklus sein muss. Man schließt nun induktiv weiter.

b) Jeder Zyklus der Länge l ist Produkt von $l-1$ Transpositionen, genauer: $(a_1, \ldots, a_l) = (a_1, a_l)(a_1, a_{l-1}) \ldots (a_1, a_2)$. Also ist das Signum eines Zyklus der Länge l gerade $(-1)^{l-1}$. Da das Signum multiplikativ ist, folgt die erste Behauptung von b).
Wegen (1.1) c) genügt es zu zeigen, dass die Ordnung eines Zyklus gleich seiner Länge ist. Sei also $\sigma = (a_1, \ldots, a_l)$. Dann gilt $\sigma^k a_i = a_{i+k \bmod l}$, also

$$\sigma^k a_i = a_i \text{ (nur) für ein } i \implies l \mid k \iff \sigma^k = \mathrm{id}\,.$$

Damit ist $l = \operatorname{ord}(a_1, \ldots, a_l)$.
Für die dritte Behauptung rechnet man zunächst nach, dass das Konjugierte eines Zyklus wieder ein Zyklus ist, genauer

$$\tau \circ (a_1, \ldots, a_l) \circ \tau^{-1} = (\tau a_1, \ldots, \tau a_l)\,.$$

Dies überträgt sich sofort auf Produkte von Zyklen gleichen Typs:

$$\tau \circ (a_{11}, \ldots, a_{1l_1}) \circ (a_{21}, \ldots, a_{2l_2}) \circ \ldots \circ \tau^{-1} = (b_{11}, \ldots, b_{1l_1}) \circ (b_{21}, \ldots, b_{2l_2}) \circ \ldots$$

mit $b_{ij} = \tau a_{ij}$. Damit ist die Inklusion $\subseteq$ gezeigt: Konjugierte Elemente haben denselben Zyklentyp.
Aber auch die Umkehrung folgt damit, denn wenn zwei Zyklenzerlegungen gleichen Typs gegeben sind, definiert man $\tau \in S_\Omega$ einfach wie oben gefordert: $\tau a_{ij} := b_{ij}$. Diese Definition ist möglich und injektiv, da die a_{ij} und b_{ij} jeweils untereinander verschieden sind, ihre Anzahlen aber einander entsprechen (da die Zyklentypen identisch sind). □

Nachtrag 7/26.11.

Korollar: a) Die symmetrische Gruppe S_n wird erzeugt von allen Transpositionen (= Zyklen der Länge 2): $S_n = \langle (ab) \mid a \neq b \rangle$.
b) Die alternierende Gruppe A_n wird erzeugt von allen 3-Zyklen: $A_n = \langle (abc) \mid a, b, c \text{ verschieden} \rangle$, bzw. von allen Produkten von zwei Transpositionen $A_n = \langle (ab)(cd) \mid a \neq b, c \neq d \rangle$.

Beweis: a) Wie im Beweis von (1.2) gezeigt ist jede Permutation Produkt von Transpositionen, letztere erzeugen also S_n.
b) A_n besteht aus allen geraden Permutationen und diese sind genau die Produkte einer geraden Anzahl von Transpositionen. Damit erzeugen alle Produkte von 2 Transpositionen (sie gehören zu A_n) ganz A_n.
Hieraus folgt auch, dass A_n von allen 3-Zyklen erzeugt wird, denn alle 3-Zyklen sind gerade und jedes Produkt aus 2 Transpositionen ist als Produkt von 3-Zyklen darstellbar:

$$(ab) \circ (cd) = \begin{cases} \mathrm{id} & \text{falls } \{a,b\} = \{c,d\}, \\ (abd) & \text{falls } \#\{a,b,c,d\} = 3, \text{ o.E. } b = c, \\ (acb) \circ (acd) & \text{falls } \#\{a,b,c,d\} = 4. \end{cases}$$

Satz: Für $n \geq 5$ ist die alternierende Gruppe A_n eine einfache Gruppe.

Beweis: Es sei $N \neq \langle 1 \rangle$ ein nichttrivialer Normalteiler von A_n: $N \triangleleft A_n$. Wir wollen zeigen, dass dieser für $n \geq 5$ bereits ganz A_n sein muss. Dazu genügt es zu zeigen, dass N einen 3-Zyklus enthält:

$$(\alpha\beta\gamma) \in N \triangleleft A_n \implies N = A_n\,.$$

Beweis: Sei (abc) ein beliebiger 3-Zyklus. Dann existiert ein $\sigma \in S_n$ mit $\sigma\alpha = a$, $\sigma\beta = b$ und $\sigma\gamma = c$. Da $n \geq 5$ ist, existieren $d \neq e$ verschieden von a, b, c und die Permutation $\sigma' = (de) \circ \sigma$ hat ebenfalls die Eigenschaften $\sigma'\alpha = a$, $\sigma'\beta = b$, $\sigma'\gamma = c$. Nun haben σ und σ' unterschiedliches Vorzeichen, so dass eine der beiden zu A_n gehört; o.E. sei dies σ. Dann gilt wegen der Normalteilereigenschaft von N

$$(abc) = \sigma \circ (\alpha\beta\gamma) \circ \sigma^{-1} \in N\,.$$

N enthält also *jeden* 3-Zyklus und ist damit gleich A_n.

Zum Beweis des Satzes konstruieren wir nun wenigstens einen 3-Zyklus in N. Dazu wählen wir zunächst ein $\sigma \in N$, $\sigma \neq 1$, dessen Träger $\mathrm{Tr}\,\sigma$ minimale Mächtigkeit k hat: 8/5.12.

$$k = \#\mathrm{Tr}\,\sigma \leq \#\mathrm{Tr}\,\rho \text{ für alle } \rho \in N\,,\ \rho \neq 1\,.$$

k ist der sog. Minimalgrad von N. σ ist Produkt von Zyklen der Längen l_i und es gilt

$$k = \#\mathrm{Tr}\,\sigma = \sum_{i=1}^{r} l_i \quad \text{mit } l_1 \geq l_2 \geq \ldots \geq l_r \geq 2\,.$$

Da N keine Transposition enthalten kann, ist $k \geq 3$, und wir wollen zeigen $k = 3$.
1. Fall $k = 4$: Dann folgt $l_1 = 4$, $r = 1$ und σ ist ein (ungerader) 4-Zyklus (Widerspruch) oder $l_1 = l_2 = 2$, $r = 2$ und σ ist ein Produkt von 2 elementfremden Transpositionen: $\sigma = (ab) \circ (cd) \in N$. Da $n \geq 5$ ist, gibt es ein $1 \leq e \leq n$ mit $e \neq a, b, c, d$. Da N Normalteiler in A_n ist, folgt

$$N \ni (cde) \circ (ab) \circ (cd) \circ (cde)^{-1} = (ab) \circ (de) \implies (ab) \circ (cd) \circ (ab) \circ (de) = (cde) \in N\,,$$

im Widerspruch zur Minimalität von $k = 4$.
2. Fall: $k \geq 5$: Dann gilt

$$l_1 \geq 4 \ \vee\ l_1 = 3, l_2 \geq 2 \ \vee\ l_1 = 2, l_2 = 2, l_3 = 2\,.$$

Also

$$N \ni \sigma = \begin{cases} (abcd\ldots) \circ \ldots & \text{Fall (I)}, \\ (abc) \circ (de\ldots) \circ \ldots & \text{Fall (II)}, \\ (ab) \circ (cd) \circ (ef) \circ \ldots & \text{Fall (III)}, \end{cases}$$

wobei die genannten Zahlen a, b, c, d, e, f untereinander verschieden sind. Für die Mächtigkeit des Trägers von σ bedeutet dies in den entsprechenden Fällen

$$k = \#\mathrm{Tr}\,(\sigma) \begin{cases} > 4\,, & \text{Fall (I), da } k \geq 5 \text{ vorausgesetzt}, \\ > 5\,, & \text{Fall (II), da } k = 5 \implies \sigma = (abc)(de) \notin A_n, \\ \geq 6\,, & \text{Fall (III)}. \end{cases}$$

Aufgrund der Konjugationsformel für Zyklen $\mu \circ (\alpha\beta\gamma\ldots) \circ \mu^{-1} = (\mu(\alpha), \mu(\beta), \mu(\gamma), \ldots)$ erhalten wir für $\mu = (bcd) \in A_n$:

$$N \ni \sigma_1 := \mu \circ \sigma \circ \mu^{-1} = \begin{cases} (acdb\ldots) \circ \ldots & \text{Fall (I)}, \\ (acd) \circ (be\ldots) \circ \ldots & \text{Fall (II)}, \\ (ac) \circ (db) \circ (ef) \circ \ldots & \text{Fall (III)}. \end{cases}$$

Damit unterscheiden sich σ und σ_1 nur an wenigen Stellen:

$$\sigma(x) = \sigma_1(x) \quad \text{für } x \notin T := \begin{cases} \{a, b, d\} & \text{Fall (I)}\ , \\ \{a, b, c, d, \sigma^{-1}(d)\} & \text{Fall (II)}, \\ \{a, b, c, d\} & \text{Fall (III)}, \end{cases}$$

Also gilt für $\sigma_0 = \sigma^{-1} \circ \sigma_1 \in N$:

$$\mathrm{Tr}\,\sigma_0 \subset T \quad \text{und} \quad \#T = \begin{cases} 3 < k & \text{(I)}, \\ 5 < k & \text{(II)}, \\ 4 < k & \text{(III)}. \end{cases}$$

Man beachte, dass im Falle (II) $k = 5$ nicht möglich ist, da sonst $\sigma = (abc)(de)$ ungerade wäre im Widerspruch zu $\sigma \in A_n$. In jedem Falle ergibt sich ein Widerspruch zur Minimalität von k.

Korollar: Für $n \geq 5$ ist A_n der einzige nicht-triviale Normalteiler von S_n.

Beweis: Sei $N \lhd S_n$ ein Normalteiler in S_n, also $N \cap A_n \lhd A_n$ und folglich wegen der Einfachheit von A_n für $n \geq 5$:

$$N \cap A_n = \langle 1 \rangle \ \vee \ N \cap A_n = A_n \, .$$

Im Fall $N \cap A_n = A_n$ gilt $N \supset A_n$ und daher (wegen $(S_n : A_n) = 2$) $N = S_n$ oder $N = A_n$. Bleibt der Fall $N \cap A_n = \langle 1 \rangle$. Damit sind alle geraden Permutationen von N trivial. Da Produkte ungerader Permutationen gerade sind, kann N dann höchstens ein Element $\neq 1$ enthalten, denn

$$\tau_1, \tau_2 \in N \setminus \{1\} \implies \tau_1^2, \tau_1\tau_2 \in N \text{ gerade} \implies \tau_1^2 = 1 = \tau_1\tau_2 \implies \tau_1 = \tau_2 \, .$$

Also $N = \{1\}$ oder $N = \{1, \tau\}$ mit $\tau^2 = 1$. Da N Normalteiler in S_n ist, liegen auch alle Konjugierten von τ in N, stimmen also mit τ überein bzw. $\tau \in \mathrm{Zentr}(S_n)$. Für $n \geq 3$ ist aber das Zentrum von S_n trivial:

$$\mathrm{id} \neq \tau \in S_n \implies \bigvee_a \tau(a) \neq a \, , \ n \geq 3 \implies \bigvee_c c \neq a, \tau(a) \implies [(ac) \circ \tau \circ (ac)](c) = \tau(a) \neq \tau(c) \, .$$

Folglich ist τ nicht mit (ac) vertauschbar. Wid.
Wir erhalten somit $N = \{1\}$ ist trivial. Insgesamt gibt es für N nur die 3 Fälle $N = \{1\}$, $N = A_n$, $N = S_n$. □

Ende des Nachtrags

Wir definieren nun die Objekte, die wir untersuchen wollen:

(1.3) Definition: a) Eine *Permutationsgruppe* G auf einer endlichen Menge Ω ist eine Untergruppe der vollen symmetrischen Gruppe S_Ω über Ω.
b) Eine *Operation* einer Gruppe G auf einer Menge Ω ist eine Abbildung $G \times \Omega \to \Omega$, $(\sigma, a) \mapsto \sigma a$ mit den Eigenschaften

$$1_G a = a \ (a \in \Omega) \, , \quad \sigma(\tau a) = (\sigma\tau)a \ (a \in \Omega \, , \ \sigma, \tau \in G) \, .$$

c) Eine *Permutationsdarstellung* einer Gruppe G ist ein Homomorphismus $P : G \to S_\Omega$ von G in die volle symmetrische Gruppe über einer Menge Ω.
d) Zwei Operationen heißen *äquivalent,* wenn existieren
ein Gruppenisomorphismus $\varphi : G \xrightarrow{\sim} G'$ und
eine Bijektion $\psi : \Omega \xrightarrow{\sim} \Omega'$
so dass das folgende Diagramm kommutativ ist:

$$\begin{array}{ccccc} G & \times & \Omega & \longrightarrow & \Omega \\ \varphi \downarrow & & \downarrow \psi & /\!/\!/ & \downarrow \psi \\ G' & \times & \Omega' & \longrightarrow & \Omega' \end{array}$$

Es sei angemerkt, dass b) und c) zwei völlig äquivalente Begriffsbildungen beschreiben, während a) im wesentlichen die *treuen* (=injektiven) Permutationsdarstellungen erfasst. In a) bzw. c) nennt man $\#\Omega$ den *Grad* der Permutationsgruppe bzw. -darstellung.

(1.4) Beispiele: Sei G eine Gruppe.
a) Die Gruppe G operiert auf sich selbst durch Linksmultiplikation: $(\sigma, a) \mapsto \sigma \cdot a$ (Multiplikation in G).
b) Die Gruppe G operiert auf sich selbst (von rechts) durch Konjugation: $(a, \sigma) \mapsto a^\sigma = \sigma^{-1} a \sigma$.
c) Sei U eine Untergruppe von G und $G/U = \{\sigma U \mid \sigma \in G\}$ die *Menge* der Rechtsnebenklassen von U. G operiert durch Multiplikation von links auf $\Omega = G/U$: $(\sigma, \rho U) \mapsto \sigma\rho U$.
d) Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ operiert durch Matrixmultiplikation von links (und auch von rechts) auf dem Vektorraum $V = K^n$. Da $0 \in V$ dabei festbleibt, operiert $\mathrm{GL}_n(K)$ auch auf $V^\# := V \setminus \{0\}$.

Dies gilt insbesondere für *endliche* Körper $K = \mathbb{F}_{p^l}$ und die (endliche) allgemeine lineare Gruppe $\mathrm{GL}_n(p^l) := \mathrm{GL}_n(\mathbb{F}_{p^l})$. Man erhält so eine Operation auf der endlichen Menge $V = \mathbb{F}_{p^l}^n$ bzw. $V^\#$ vom Grad p^{ln} bzw. $p^{ln} - 1$.
e) Noch spezieller: $\mathrm{GL}_n(2)$ hat eine (natürliche) Permutationsdarstellung vom Grade $2^n - 1$. Die einfachsten Spezialfälle sind die Gruppe $\mathrm{GL}_2(2) \simeq S_3$ und $\mathrm{GL}_3(2) \subset S_7$. $\mathrm{GL}_3(2)$ erweist sich als *die* einfache Gruppe der Ordnung 168.

(1.5) Definition: Die Gruppe G operiere auf der endlichen Menge Ω und es sei $a \in \Omega$. Dann definieren wir:
a) die *Bahn* (oder auch *Orbit*) von a unter G:

$$G.a = \{\sigma a \mid \sigma \in G\}\,.$$

b) die *Fixgruppe* von a in G:

$$G_a = \{\sigma \in G \mid \sigma a = a\}\,,$$

c) die *Fixmenge* von G in Ω:

$$\Omega^G = \{a \in \Omega \mid \sigma a = a \text{ für alle } \sigma \in G\}\,.$$

(1.6) Beispiele: A) Bahnen können tatsächlich wie Bahnkurven aussehen, etwa im folgenden Beispiel: Lässt man die multiplikative Gruppe $\mathbb{C}^\times$ auf $\mathbb{C}$ durch Multiplikation operieren und betrachtet die Untergruppen $G = \mathbb{R}_+$, $\mathbb{R}^\times$, $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ sowie ganz $\mathbb{C}^\times$, so erhält man für $a = 0 \in \mathbb{C}$ immer die Bahn $\{0\}$ (0 ist Fixpunkt). Für $a \neq 0$ erhält man die Bahnen 2/23.10.

$$Ga = \begin{cases} \text{Strahl von 0 durch } a \text{ (ohne 0)} & G = \mathbb{R}_+, \\ \text{Gerade durch 0 und } a \text{ (ohne 0)} & G = \mathbb{R}^\times, \\ \text{Kreis um 0 durch } a & G = S^1, \\ \mathbb{C}^\times & G = \mathbb{C}^\times. \end{cases}$$

Die Fixgruppe ist die gesamte Gruppe ($G_a = G$ für $a = 0$) oder trivial ($G_a = \{1_G\}$ für $a \neq 0$).
B) Für die in (1.4) gegebenen Beispiele erhält man:
a) Linksmultiplikation: Diese Operation hat nur eine Bahn, ganz G. Die Fixgruppe G_a eines jeden $a \in G$ ist trivial: $G_a = \{1\}$. Die Fixmenge bestimmt sich wie folgt:

$$\Omega^G = \{a \in G \mid \sigma a = a \text{ für alle } \sigma \in G\} = \begin{cases} \Omega & \text{falls } G \text{ trivial}\,, \\ \emptyset & \text{sonst.} \end{cases}$$

b) Konjugation: Die Bahnen dieser Operation sind die *Konjugationsklassen* von Elementen:

$$C(a) = \{a^\sigma \mid \sigma \in G\}\,.$$

Die Fixgruppen G_a bzgl. dieser Operation sind die *Zentralisatoren*

$$\mathrm{Zentr}_G(a) = \{\sigma \in G \mid \sigma a = a\sigma\}\,.$$

Die Fixmenge unter der Konjugation ist das Zentrum von G: $\{a \in G \mid \sigma a = a\sigma \text{ für alle } \sigma \in G\}$.
c) Nebenklassenmengen: Ganz $\Omega = G/U$ bildet eine Bahn unter der Operation von G. Die Fixgruppen sind die Konjugierten von U; genauer: Ist $a = \rho U \in \Omega$, so ist $G_a = G_{\rho U} = \rho U \rho^{-1}$, denn $\sigma \cdot \rho U = \rho U \iff \rho^{-1}\sigma\rho \in U$. Insbesondere ist U die Fixgruppe von $a = 1 \cdot U \in \Omega$.
d) Matrixmultiplikation: Die Operation von $\mathrm{GL}_n(K)$ auf K^n hat zwei Bahnen: $\{0\}$ und $K^n \setminus \{0\}$. 0 ist der einzige Fixpunkt der Operation. Die Fixgruppe eines $v \in K^n$, $v \neq 0$, ist die Menge der Matrizen A, die den Eigenwert 1 haben und v als einen Eigenvektor zu diesem Eigenwert.

(1.7) Proposition: *Eine endliche Gruppe G operiere auf einer endlichen Menge Ω und es sei $a \in \Omega$.*
a) Die Fixgruppen sind tatsächlich Untergruppen und es gilt

$$\sigma G_a \sigma^{-1} = G_{\sigma a}\,.$$

Damit sind die Fixgruppen zu Punkten a, b in derselben Bahn (also $b = \sigma a$ für ein $\sigma \in G$) in G konjugiert, insbesondere von gleicher Ordnung.
b) Es gilt die elementare, aber wichtige Beziehung:

$$(G : G_a) = \#G.a\,.$$

Bahnlängen sind also Gruppenindizes und damit Teiler der Ordnung $\#G$ von G.
c) Man hat die Bahnzerlegung

$$\Omega = \Omega^G \,\dot\cup\, \dot{\bigcup_{a\in\mathcal{R}}}\, G.a$$

mit einem geeigneten Repräsentantensystem $\mathcal{R} \subset \Omega$ der nicht-einelementigen Bahnen.

Beweis: Bei a) überprüft man leicht die Inklusion $\sigma G_a \sigma^{-1} \subset G_{\sigma a}$. Genauso gilt $\sigma^{-1} G_{\sigma a} \sigma \subset G_a$, woraus die umgekehrte Inklusion $G_{\sigma a} \subset \sigma G_a \sigma^{-1}$ folgt.
b) ergibt sich aus der Bijektion

$$G/G_a \xrightarrow{\sim} Ga\,,\ \sigma G_a \mapsto \sigma a\,.$$

Dabei ist die Surjektivität durch die Definition der Bahn Ga gegeben, während sich die Injektivität aus der Definition der Fixgruppe G_a ergibt:

$$\sigma.a = \tau.a \iff \tau^{-1}\sigma.a = a \iff \tau^{-1}\sigma \in G_a \iff \sigma G_a = \tau G_a\,.$$

Also ist die Bahnlänge von Ga gleich der Zahl der Nebenklassen von G_a in G.
c) ist klar, denn die Bahnen sind die Äquivalenzklassen bzgl. der Äquivalenzrelation $a \sim b \iff b = \sigma a$ für ein $\sigma \in G$. Die Fixmenge Ω^G ist die Vereinigung der einelementigen Bahnen. □

Als Beispiel für eine gruppentheoretische Anwendung zeigen wir

(1.8) Satz: *Operiert eine p-Gruppe G (eine Gruppe von Primzahlpotenzordnung p^n) auf einer Menge Ω, so gilt:*

$$\#\Omega \equiv \#\Omega^G \bmod p\,.$$

Beweis: In einer p-Gruppe sind alle Gruppenindizes $(G : G_a)$, die ≥ 2 sind, notwendig durch p teilbar, also ist in der obigen Bahnengleichung die gesamte Summe durch p teilbar, also $\#\Omega - \#\Omega^G$ ein Vielfaches von p, wie behauptet.
Hieraus ergibt sich die folgende für die Theorie der p-Gruppen fundamentale Tatsache.

(1.9) Korollar: *a) Eine nicht-triviale p-Gruppe G hat ein nicht-triviales Zentrum.*
b) p-Gruppen sind auflösbar.

Zum *Beweis* betrachten wir die Operation von G auf sich selbst ($\Omega = G$) durch Konjugation. Dann ist $\Omega^G = \mathrm{Zentr}(G)$ und gemäß (1.8) gilt

$$\#G \equiv \#\mathrm{Zentr}(G) \bmod p\,.$$

Mit $\#G$ ist also auch $\#\mathrm{Zentr}(G)$ durch p teilbar, also $\#\mathrm{Zentr}(G) \geq p$. Damit ist a) bewiesen.
b) Sei G eine nicht-triviale p-Gruppe. Gemäß a) existiert in G ein Normalteiler $Z(G) \lhd G$ mit einer Faktorgruppe $G/Z(G)$, die von kleinerer Prinzahlpotenzordnung ist. Da $Z(G)$ abelsch, insbesondere also auflösbar ist, muss man nur die Auflösbarkeit von $G/Z(G)$ zeigen; diese folgt per Induktion.

Nachtrag

Anwendungsbeispiel: Die Sylowsätze. Wir untersuchen die Umkehrung des Satzes von Lagrange: Gibt es zu einem Teiler d der Ordnung einer endlichen Gruppe G eine Untergruppe H von G mit $\#H = d$? Betrachtet man *spezielle* Gruppen, so kann man positive Antworten finden; z. B. 7/28.11.

Proposition: *In endlichen zyklischen Gruppen gibt es zu jedem Teiler d der Gruppenordnung genau eine Untergruppe der Ordnung d. Genauer: Ist $G = \langle a\rangle$ zyklisch von der Ordnung n und d ein Teiler von n, so ist $\langle a^{n/d}\rangle$ die einzige Untergruppe von G mit der Ordnung d.*

Beweis: Sei $k = n/d$. Es ist $\mathrm{ord}(a) = n$, also $a^i = 1 \iff n \mid i$. Daraus folgt

$$(a^k)^i = 1 \iff n \mid k \cdot i \iff k \cdot d \mid k \cdot i \iff d \mid i\,.$$

Damit ist $d = \mathrm{ord}(a^k)$, also $\langle a^k \rangle$ eine (zyklische) Untergruppe der Ordnung d.

Nun zur Eindeutigkeit. Sei H eine Untergruppe von G mit der Ordnung d. Da G zyklisch, insbesondere also abelsch ist, ist H ein Normalteiler und wir können die Faktor*gruppe* G/H betrachten. Diese hat die Ordnung $(G : H) = \#G/\#H = n/d = k$. Also gilt nach dem Satz von Lagrange $\bar{a}^k = \bar{1}$ für $\bar{a} = aH \in G/H$. Dies bedeutet

$$\bar{a}^k = a^k H = H\,,\ \text{bzw. } a^k \in H\,.$$

Damit liegt a^k in H, also $\langle a^k \rangle \subset H$. Wegen gleicher Ordnung stimmen die beiden Gruppen überein, womit die Eindeutigkeit gezeigt ist.

Diese Proposition gibt für *spezielle Gruppen* eine positive Antwort auf die Frage nach der Umkehrung des Satzes von Lagrange. Die Sylowsätze hingegen geben eine positive Antwort für spezielle Teiler d, nämlich für *Primzahlpotenzen* $d = p^s$. Die fundamentale Bedeutung der Sylowsätze liegt nun darin, dass sie für *beliebige* Gruppen gelten. Sie spielen daher eine nicht zu überschätzende Rolle bei der Strukturaufklärung beliebiger Gruppen.

Sei nun G eine Gruppe der Ordnung n, p eine Primzahl und es gelte $p^s \mid n$. Dann ist $\#G = n = p^r \cdot m$ mit $p \nmid m$ und $r \geq s$. Um eine Untergruppe H von G mit der gewünschten Ordnung p^s zu finden, betrachten wir zunächst sämtliche Teilmengen von G mit der Mächtigkeit p^s:

$$\Omega = \binom{G}{p^s} = \{T \subset G \mid \#T = p^s\}\,.$$

Darauf operiert G durch Linksmultiplikation. Für ein $T \in \Omega$ ist dann die Fixgruppe $G_T = \{\sigma \in G \mid \sigma T = T\}$ eine Untergruppe von G. Diese operiert nun ihrerseits auf den *Elementen* von T durch Linksmultiplikation und man erhält so (bei Wahl eines beliebigen $a \in T$) eine injektive Abbildung

$$\varphi_a : G_T \hookrightarrow T\,,\ \sigma \mapsto \sigma a\,.$$

Insbesondere folgt also für jedes $T \in \Omega$: $\#G_T \leq \#T = p^s$.

Wir suchen nun unter diesen Fixgruppen $H = G_T$ eine mit der maximalen Ordnung p^s. Nun gilt für $H = G_T$:

$$\#H = p^s \iff \varphi_a : H \xrightarrow{\sim} T \iff T = Ha\,.$$

Andererseits gilt wegen $\#H \leq p^s$

$$\begin{aligned}\#H = p^s &\iff p^s \mid \#H = \frac{\#G}{(G:H)} = \frac{p^r m}{(G:H)} \iff (G:H) \mid p^{r-s}m \\ &\iff p^{r-s+1} \nmid (G:H) = (G:G_T) = \#GT\,.\end{aligned}$$

Dabei ist $GT = \{\sigma T \mid \sigma \in G\} \subset \Omega$ die Bahn von $T \in \Omega$. Fasst man beide Aussagen zusammen, so erhält man für $T \subset G$

$$T \in \Omega \wedge p^{r-s+1} \nmid \#(GT) \iff T \in \Omega \wedge \bigvee_{a \in G} T = G_T a \iff \bigvee_{a \in G} \bigvee_{\substack{H \leq G \\ \#H = p^s}} T = Ha\,. \qquad (1)$$

Bei der zweiten Äquivalenz gilt '$\Leftarrow$', weil aus $T = Ha$ folgt: $\#T = \#H = p^s$ und $G_T = H$. Insbesondere erhalten wir aus (1)

$$\bigvee_{H \leq G} \#H = p^s \iff \bigvee_{T \in \Omega} p^{r-s+1} \nmid \#(GT)\,. \qquad (2)$$

Wir wollen nun zeigen, dass es derartige $T \in \Omega$ und folglich Untergruppen der gesuchten Art gibt. Dazu betrachten wir die Menge

$$\Omega' = \{T \in \Omega \mid p^{r-s+1} \not| \#(GT)\} \underset{(1)}{=} \{Ha \mid H \leq G\,,\ \#H = p^s\,,\ a \in G\}$$

und müssen zeigen, dass sie nicht leer ist. Ω' besteht aus allen Nebenklassen aller Untergruppen der Ordnung p^s. Nun sind Nebenklassen von verschiedenen Untergruppen notwendig verschieden (siehe oben: $T = Ha \Rightarrow H = G_T$), also gilt

$$\Omega' = \dot{\bigcup_{\substack{H \leq G \\ \#H = p^s}}} \{Ha \mid a \in G\} = \dot{\bigcup_{\substack{H \leq G \\ \#H = p^s}}} H\backslash G\,.$$

Da alle $H\backslash G$ dieselbe Mächtigkeit

$$(G : H) = \frac{\#G}{\#H} = \frac{n}{p^s} = p^{r-s}m$$

haben, folgt

$$\#\Omega' = p^{r-s}m \cdot \#\{H \leq G \mid \#H = p^s\} =: p^{r-s}m \cdot h_G(p^s)\,. \tag{3}$$

($h_G(p^s)$ bezeichnet also die Anzahl der Untergruppen H von G mit $\#H = p^s$, die wir ja studieren wollen.) Weiter gilt bekanntlich

$$\#\Omega = \binom{n}{p^s} = \frac{n}{p^s} \cdot \binom{n-1}{p^s - 1} = p^{r-s}m \cdot \binom{n-1}{p^s-1}\,. \tag{4}$$

Andererseits besteht $\Omega \setminus \Omega'$ nach Definition von Ω' gerade aus allen $T \in \Omega$ mit $p^{r-s+1} \mid \#GT$, also zerfällt $\Omega \setminus \Omega'$ in lauter Bahnen, deren Mächtigkeit durch p^{r-s+1} teilbar ist. Das bedeutet

$$p^{r-s+1} \mid \#(\Omega \setminus \Omega') = \#\Omega - \#\Omega'\,, \quad \text{bzw.} \quad \#\Omega \equiv \Omega' \mod p^{r-s+1}\,. \tag{5}$$

Aus (3) – (5) folgt

$$\begin{aligned} p^{r-s}m \cdot \binom{n-1}{p^s-1} &\equiv p^{r-s}m \cdot h_G(p^s) \mod p^{r-s+1}\,, \quad \text{bzw.} \\ m \cdot \binom{n-1}{p^s-1} &\equiv m \cdot h_G(p^s) \mod p\,. \end{aligned}$$

Da p kein Teiler von m ist, gilt nun

$$p \mid m \cdot \left(\binom{n-1}{p^s-1} - h_G(p^s)\right) \implies p \mid \binom{n-1}{p^s-1} - h_G(p^s)\,,$$

und daher

$$h_G(p^s) \equiv \binom{n-1}{p^s-1} \mod p\,. \tag{6}$$

Wir zeigen nun

$$\binom{n-1}{p^s-1} \equiv 1 \bmod p\,. \tag{7}$$

Dies kann man rein zahlentheoretisch für $p^s \mid n$ beweisen. Man kann es aber auch gruppentheoretisch aus (6) folgern. Dazu benutzt man, dass in (6) die rechte Seite nicht von G, sondern nur

von $\#G = n$ abhängig ist! Und für $G = C_n$ zyklisch von der Ordnung n ist die linke Seite von (6) gemäß (2.8) gleich 1. Also

$$1 = h_{C_n}(p^s) \equiv \binom{n-1}{p^s-1} \bmod p\,,$$

womit (7) bewiesen ist. (6) und (7) zusammen ergeben für jede Gruppe G der Ordnung n und Primzahlpotenzen $p^s \mid n$:

$$h_G(p^s) \equiv 1 \bmod p\,. \tag{8}$$

Insbesondere kann die Zahl der Untergruppen der Ordnung p^s nicht 0 sein! Damit ist der folgende Satz bewiesen:

Erster Sylowsatz: *Sei G eine endliche Gruppe.*
a) Dann gibt es zu jeder Primzahlpotenz p^s, die die Gruppenordnung $\#G$ teilt, eine Untergruppe H von G mit $\#H = p^s$.
b) Für die Anzahl $h_G(p^s)$ solcher Untergruppen gilt genauer:

$$h_G(p^s) \equiv 1 \bmod p\,.$$

Unter den p-Untergruppen von G spielen die von größtmöglicher Ordnung eine besondere Rolle. Dies sind die sog. p-Sylow(unter)gruppen von G. Ist $\#G = p^r m$ mit einer Primzahl p, $p \nmid m$, so definiert man:

$$\begin{aligned} P \text{ } p\text{-Sylowuntergruppe von } G \;&:\Longleftrightarrow\; P \le G \text{ und } \#P = p^r \\ &\Longleftrightarrow\; P \text{ } p\text{-Gruppe und } p \nmid (G:P)\,. \end{aligned}$$

Nach dem vorangehenden Satz besitzt *jede* Gruppe für *jede* Primzahl eine p-Sylowuntergruppe. Eine Übersicht über alle p-Sylowuntergruppen gibt unter anderem der folgende Satz.

Zweiter Sylowsatz: *Sei G eine endliche Gruppe, p eine Primzahl, P eine p-Sylowuntergruppe und H eine beliebige p-Untergruppe von G. Dann existiert ein $\sigma \in G$ mit*

$$H \subset \sigma^{-1} P \sigma = P^\sigma\,.$$

Folglich:
a) Jede p-Untergruppe von G ist in einer p-Sylowuntergruppe von G enthalten.
b) p-Sylowuntergruppen von G sind genau die (bzgl. Inklusion) maximalen p-Untergruppen von G.
c) Sämtliche p-Sylowuntergruppen von G sind in G untereinander konjugiert:

$$P, P' \text{ } p\text{-Sylowuntergruppen von } G \Longrightarrow \bigvee_{\sigma \in G} P' = P^\sigma\,.$$

d) Ist s_p die Anzahl der p-Sylowuntergruppen von G und $\#G = p^r m$ mit $p \nmid m$, so gilt:

$$s_p \mid m \quad \textit{und} \quad s_p \equiv 1 \bmod p\,.$$

Beweis: Die p-Untergruppe $H \subset G$ operiert durch Linksmultiplikation auf den Rechtsnebenklassen $\Omega = G/P = \{aP \mid a \in G\}$ von P. Dann gilt nach (2.6)

$$\#\Omega \equiv \#\Omega^H \bmod p\,.$$

Ist $G = p^r m$ mit $p \nmid m$, so ist $\#\Omega = (G:P) = m$ nicht durch p teilbar, also

$$\#\Omega^H \equiv \#\Omega \not\equiv 0 \bmod p\,.$$

Insbesondere ist $\#\Omega^H \neq 0$, also existiert in Ω ein Fixelement aP unter der Operation von H:

$$\bigwedge_{h\in H} haP = aP\,,\ \text{bzw. } a^{-1}ha \in P\,.$$

Damit gilt $a^{-1}Ha \subset P$ bzw. $H \subset aPa^{-1}$, womit die Behauptung bewiesen ist.

Nun zu den Folgerungen. a) Mit P ist auch P^σ eine p-Sylowuntergruppe.
b) p-Sylowuntergruppen sind natürlich maximale p-Untergruppen, da größere p-Potenzen nicht mehr $\#G$ teilen. Sei nun umgekehrt H eine (bzgl. Inklusion) maximale p-Untergruppe. Wie gezeigt, liegt H in einer p-Sylowuntergruppe, muss also wegen der Maximalität mit dieser übereinstimmen. Also ist H selbst p-Sylowuntergruppe.
c) Sind P, P' p-Sylowuntergruppen, so existiert ein $\sigma \in G$ mit $P' \subset P^\sigma$. Da P' und P^σ als p-Sylowuntergruppen gleichmächtig sind, folgt $P' = P^\sigma$.
d) Die Gruppe G operiert durch Konjugation auf den Untergruppen. Ist P eine p-Sylowuntergruppe, so ist die Bahn von P unter dieser Operation (nach c)) gerade die Menge aller p-Sylowuntergruppen. Nun sind Bahnlängen aber Indizes von Fixgruppen. In diesem Falle ist diese Fixgruppe gerade

$$\mathrm{Fix}_G(P) = \{\sigma \in G \mid P^\sigma = P\} =: \mathcal{N}_G(P)\,,$$

der sog. Normalisator von P in G. Also gilt nach (2.5) c)

$$s_p = \#\{P \mid P \text{ } p\text{-Sylowuntergruppe von } G\} = \#\{P^\sigma \mid \sigma \in G\} = (G : \mathcal{N}_G(P))\,.$$

Diese Überlegungen zeigen allgemein: *Die Anzahl der Konjugierten einer Untergruppe ist der Index des Normalisators in der Gruppe.*

Nun ist der Normalisator nach Definition die größte Untergruppe von G, in der P ein Normalteiler ist:

$$\mathcal{N}_G(P) = \{\sigma \in G \mid \sigma^{-1}P\sigma = P\}\,,$$

also $\mathcal{N}_G(P) \supset P$ und daher gilt $s_p = (G : \mathcal{N}_G(P)) \mid (G : P) = m$. Damit ist auch d) bewiesen, denn die Kongruenz modulo p wurde bereits im ersten Sylowsatz gezeigt.

Ende des Nachtrags

b. Transitive Permutationsdarstellungen. 3/31.10.

(1.10) Definition: Eine Gruppenoperation heißt *transitiv,* wenn sie nur *eine* Bahn hat, wenn also jedes Element überall hin abgebildet wird:

$$G \text{ operiert transitiv auf } \Omega \iff \bigwedge_{a,b\in\Omega} \bigvee_{\sigma\in G} \sigma a = b\,.$$

Gemäß (1.7) b) ist der Grad einer transitiven Permutationsdarstellung (dies ist $\#\Omega$) ein Teiler der Gruppenordnung.

Beispiele: a) $\mathrm{GL}_n(p^l)$ operiert transitiv auf $V^\#$ ($V = \mathbb{F}_{p^l}^n$); $p^{ln} - 1$ teilt $\#\mathrm{GL}_n(p^l)$.
b) Zerlegt man $\sigma \in S_n$ in elementfremde Zyklen, so bilden die in den jeweiligen Zyklen auftretenden Elemente die mehrelementigen Bahnen der zyklischen Gruppe $\langle\sigma\rangle$; die übrigen Bahnen sind einelementig, ihre Elemente sind genau die Fixpunkte von $\langle\sigma\rangle$.

Die nachfolgende Proposition gibt eine gruppentheoretische Übersicht über alle transitiven Permutationsdarstellungen einer Gruppe G.

(1.11) Proposition: *Sei G eine Gruppe.*
a) Jede Untergruppe U von G bestimmt eine transitive Permutationsdarstellung von G durch Linksmultiplikation auf den Nebenklassen von U:

$$G \times G/U \longrightarrow G/U\,,\quad (\sigma, \tau U) \mapsto \sigma\tau U\,.$$

Der Grad dieser Darstellung ist der Gruppenindex $(G : U)$ und U ist die Fixgruppe der Nebenklasse $1_G U$.
b) Umgekehrt: Jede transitive Permutationsdarstellung von G auf einer Menge Ω ist äquivalent zu einer der in a) konstruierten. Dabei ist U wählbar als Fixgruppe G_a eines Punktes $a \in \Omega$ und es gilt $(G : U) = \#\Omega$.
c) Zwei Darstellungen gemäß a) zu Untergruppen U und U' sind genau dann äquivalent zueinander, wenn U und U' in G konjugiert sind: $U' = U^\rho = \rho^{-1} U \rho$.
d) Die Zuordnungen von a) und b) liefern also eine Bijektion zwischen

- *den Klassen äquivalenter transitiver Permutationsdarstellungen von G vom Grade n*

und

- *den Konjugationsklassen von Untergruppen $U \subset G$ vom Index n.*

Beweis: a) ergibt sich unmittelbar aus den Gruppenaxiomen.

b) Wir wählen $a \in \Omega$. Wegen der Transitivität gilt $\Omega = Ga$ und der Beweis von (1.7) b) liefert die Bijektion $\psi : G/G_a \xrightarrow{\sim} Ga = \Omega$, $\sigma G_a \mapsto \sigma a$. Zusammen mit $\varphi = \mathrm{id}_G$ ergibt sich nun das in Definition (1.3) d) geforderte kommutative Diagramm

$$\begin{array}{ccccc} G & \times & G/G_a & \longrightarrow & G/G_a \\ \| & & \downarrow \psi & /\!/\!/ & \downarrow \psi \\ G & \times & \Omega & \longrightarrow & \Omega \end{array}$$

Damit ist die gegebene transitive Permutationsdarstellung äquivalent zu der gemäß a) durch die Untergruppe $U = G_a$ gegebenen.

c) Ist $U' = U^\rho$, so liefern die Konjugation mit ρ einen Gruppenautomorphismus von G (dies sei φ) und die Multiplikation mit ρ^{-1} eine Bijektion $G/U \xrightarrow{\sim} G/U'$ (dies sei die Bijektion ψ), die zusammen eine Äquivalenz zwischen den beiden Permutationsdarstellungen zu U und U' herstellen.
Sind umgekehrt diese beiden Darstellungen äquivalent, so ist U (die Fixgruppe von $1_G U$) zugleich Fixgruppe einer Nebenklasse $\rho U' = \psi(1_G U)$ bzgl. der zweiten Darstellung. Letztere ist aber gerade die Untergruppe $\rho U' \rho^{-1}$ konjugiert zu U'.

d) ist die Zusammenfassung der vorangehenden Teile. □

(1.12) Folgerung: *a) Ist U eine Untergruppe vom Index n in G, so ist $N = \bigcap_{\sigma \in G} U^\sigma = \bigcap_{\sigma \in G} \sigma^{-1} U \sigma$ ein Normalteiler in G vom Index $\leq n!$.*
b) Hat eine einfache Gruppe G eine Untergruppe vom Index n, so ist $\#G \leq n!$.

Beweis: U bestimmt eine transitive Permutationsdarstellung $P_U : G \to S_n$. Deren Kern ist der Durchschnitt aller Fixgruppen G_a; dies sind genau die Konjugierten von U, also

$$\mathrm{Ke}\, P_U = \bigcap_{\sigma \in G} U^\sigma = N\,.$$

Damit erhält man einen *injektiven* Homomorphismus $G/N \hookrightarrow S_n$, also $\#G/N = (G : N) \leq n!$.
b) Nach a) wissen wir: Gibt es in einer Gruppe eine Untergruppe U vom Index n, so enthält diese einen (echten) Normalteiler vom Index $\leq n!$. Daraus folgt sofort b), denn einfache Gruppen haben nur $N = \{1\}$ als echten Normalteiler, also $n! \geq (G : N) = \#G$.

Anwendungsbeispiel: Die Ordnungen echter Untergruppen der alternierenden Gruppe A_5 sind 2,3,4,5,6,10,12.

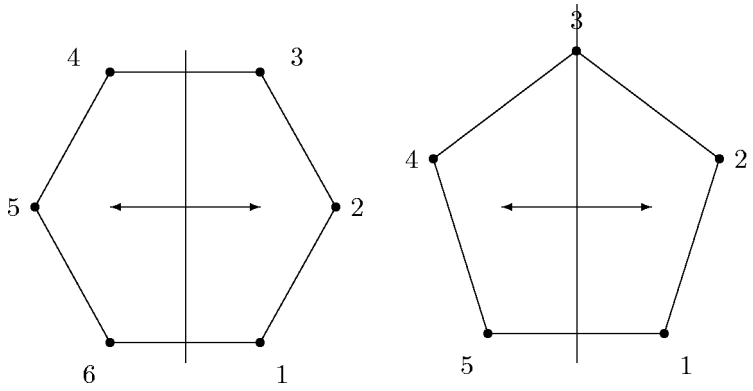
Begründung: Gemäß (1.12) enthält die einfache Gruppe A_5 keine echte Untergruppe vom Index ≤ 4. Die Index echter Untergruppen ist also ≥ 5, die Ordnung also ≤ 12. Untergruppen der kleinen Ordnungen $2, 3, 4, 5$ können explizit angegeben werden ($\langle (12)(34) \rangle$, $\langle (123) \rangle$, $V_4 = \langle (12)(34), (13)(24) \rangle$, $\langle (12345) \rangle$). Die Operation der A_5 auf $\underline{5} = \{1, 2, 3, 4, 5\}$ ist transitiv (5-er Zyklus), also ist die Fixgruppe einer Ziffer eine Untergruppe vom Index 5, von der Ordnung 12 ($\simeq A_4$).
Untergruppen der Ordnungen 6 und 10 erhält man ebenfalls durch geeignete Operationen.
Ordnung 6: A_5 operiert nicht nur auf den 5 Ziffern $\underline{5}$, sondern auch auf den 2-elementigen

Teilmengen darin $\mathcal{P}_2(\underline{5})$. Diese Operation ist transitiv: Seien $M = \{a, b\}$ und $M' = \{a', b'\}$ zwei beliebige 2-elementige Teilmengen. Dann lässt sich die Zuordnung $a \mapsto a'$, $b \mapsto b'$ zu einer Permutation $\sigma \in S_5$ erweitern. Es gilt also $\sigma M = M'$. Im Falle $\sigma \in A_5$ ist man fertig. Im Falle $\sigma \notin A_5$ wählen wir die Transposition $\tau = (a, b)$ und erhalten $\sigma_1 = \sigma \circ \tau \in A_5$ mit $\sigma_1 a = \sigma b = b'$, $\sigma_1 b = \sigma a = a'$, auf jeden Fall also $\sigma_1 M = M'$: A_5 operiert transitiv auf $\Omega = \mathcal{P}_2(\underline{5})$. Die Mächtigkeit dieser Menge ist $\binom{5}{2} = 10$, die Fixgruppen dieser Operation sind also (konjugierte) Untergruppen der A_5 vom Index 10 bzw. von der Ordnung 6. (Explizit $G_{\{1,2\}} = \langle (3,4,5), (1,2)(3,4) \rangle = \{\mathrm{id}, (12)(34), (12)(35), (12)(45), (345), (354)\}$.)
Ordnung 10: Die Diedergruppen als Symmetriegruppe der regelmäßigen n-Ecke.
Es sei E_n das regelmäßige n-Eck (mit den Ecken auf dem Einheitskreis). Dann bilden die orthogonalen Transformationen, die E_n in sich überführen eine Permutationsgruppe vom Grade n:

$$D_{2n} = \{\sigma \in O_2(\mathbb{R}) \mid \sigma E_n = E_n\}\,.$$

Sie besteht aus den Drehungen um Vielfache von $2\pi/n$ und Spiegelungen. Sie wird erzeugt von der Drehung um $2\pi/n$ (diese erzeugt einen Normalteiler der Ordnung n in ihr) und einer Spiegelung (von der Ordnung 2) und hat daher die Ordnung $2n$. (Daher die Notation, die aber nicht einheitlich ist; es wird auch D_n statt D_{2n} geschrieben.) Numeriert man die Ecken zyklisch mit den Ziffern $1, \ldots, n$, so erhält man die folgende Erzeugung $D_{2n} = \langle \sigma, \tau \rangle$ mit dem n-Zyklus $\sigma = (1, \ldots, n)$ und einer Spiegelung τ. Diese kann gewählt werden als Produkt von $[\frac{n}{2}]$ Transpositionen

$$\tau = (1, n)(2, n-1) \ldots ([\frac{n}{2}], n + 1 - [\frac{n}{2}])\,.$$



Im Falle $n = 5$ (und allgemein für $n \equiv 1 \bmod 4$) ist die Diedergruppe D_{2n} eine Untergruppe der alternierenden Gruppe A_n, denn für ungerades n ist der n-Zyklus σ eine gerade Permutation und für $n \equiv 1 \bmod 4$ ist $[\frac{n}{2}] = \frac{n-1}{2}$ gerade und damit auch $\tau \in A_n$.

c. Der Permutationscharakter. Eine wichtige Invariante von Permutationsgruppen ist ihr *Permutationscharakter.*

(1.13) Definition: Der *Permutationscharakter* einer Permutationsdarstellung $P : G \to S_\Omega$ ist die Funktion

$$\chi : G \to \mathbb{N}\,,\ \chi(\sigma) = \#\{a \in \Omega \mid \sigma a = a\} = \#\Omega^{\langle \sigma \rangle}\,,$$

die jedem Gruppenelement die Anzahl seiner Fixpunkte zuordnet.

Dieser Permutationscharakter besitzt eine matrizentheoretische Beschreibung.

(1.14) Bemerkung: a) Die symmetrische Gruppe S_n besitzt eine Einbettung in die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{C})$, indem man jede Permutation $\sigma \in S_n$ als Permutation der kanonischen Basis interpretiert und dann linear fortsetzt. In Matrizen ausgedrückt ergibt dies:

$$S_n \to \mathrm{GL}_n(\mathbb{C})\,,\ \sigma \mapsto (\delta_{i,\sigma(j)})_{i,j}\,.$$

b) Jede Permutationsdarstellung $P : G \to S_n$ induziert auf diese Weise eine *Matrixdarstellung* (d. i. ein Gruppenhomomorphismus) $M_P : G \to \mathrm{GL}_n(\mathbb{C})$ und der Permutationscharakter erweist sich als die Spur dieser Matrixdarstellung:

$$\mathrm{Spur}(M_P(\sigma)) = \sum_i \delta_{i,\sigma i} = \#\{i \mid i = \sigma i\} = \chi(\sigma)\,.$$

Die Spur einer Matrixdarstellung nennt man ihren Charakter. Er legt die Matrixdarstellung bis auf Isomorphie fest. Dies ist eines der fundamentalen Resultate der sog. Darstellungstheorie, einer Teildisziplin der Gruppentheorie. 4/7.11.

Der Permutationscharakter enthält ebenfalls sehr viel Information über die Permutationsdarstellung, legt sie jedoch nicht bis auf Isomorphie fest. (Der Isomorphiebegriff ist enger!) Wir wollen nun zwei erste Beispiele dafür geben, welche Information aus dem Permutationscharakter zu entnehmen ist.

(1.15) Satz: *Die Gruppe G operiere auf der endlichen Menge Ω und es sei χ ihr Permutationscharakter. Dann gilt:*
a) χ bestimmt den Zyklentyp aller Elemente von G.
b) Aus der Kenntnis von χ ist die Transitivität der Operation ablesbar:

$$G \text{ operiert transitiv auf } \Omega \iff \sum_{\sigma\in G} \chi(\sigma) = \#G\,.$$

Allgemein gilt: Die Anzahl der Bahnen von G auf Ω ist der Mittelwert des Permutationscharakters:

$$\frac{1}{\#G}\sum_{\sigma\in G}\chi(\sigma)\,.$$

Beweis: a) Wir betrachten die Zyklendarstellung von σ und sortieren diese nach den Längen l der auftretenden Zyklen:

$$\sigma = \prod_{l=1}^{n}\prod_{j=1}^{r_l}\sigma_{lj}$$

wobei σ_{lj} elementfremde Zyklen der Länge l sind; dabei ist $r_l \geq 0$ ist die Zahl der Zyklen der Länge l. In diese Darstellung sind auch die Zyklen der Länge 1 aufgenommen: $\sigma_{1j} = (a_j) = \mathrm{id}$ für jeden Fixpunkt a_j von σ $(j = 1, \ldots, r_1)$. Daher ist $n = \#\Omega = \sum_{l=1}^{n} r_l$ die Summe aller Zyklenlängen und $r_1 = \chi(\sigma)$ die Zahl der Fixpunkte.

Nun gilt für die Potenz eines Zyklus der Länge l $(l \geq 1)$:

$$(a_1, \ldots, a_l)^s \begin{cases} \text{fixpunktfrei} & \text{für } l \nmid s \\ = \mathrm{id} & \text{für } l \mid s \end{cases} \quad \text{auf } \{a_1, \ldots, a_l\}\,.$$

Denn wegen $(a_1, \ldots, a_l)^s(a_j) = a_{j+s \bmod l}$ gibt es einen Fixpunkt a_j nur für $j \equiv j+s \bmod l$, d. h. $l \mid s$. In dem Falle ist aber $(a_1, \ldots, a_l)^s = \mathrm{id}$. Die Fixpunktzahl von $(a_1, \ldots, a_l)^s$ *auf* $\{a_1, \ldots, a_l\}$ ist also l für $l \mid s$ und 0 sonst.

Wegen der Elementfremdheit der Zyklen kann man nun die Anzahl der Fixpunkte von $\sigma^s = \prod_l \prod_j \sigma_{lj}^s$ bestimmen als *Summe* der Fixpunktanzahlen der einzelnen Zyklenpotenzen σ_{lj}^s:

$$\chi(\sigma^s) = \sum_{\substack{l=1\\ l\mid s}}^{n}\sum_{j=1}^{r_l} l = \sum_{\substack{l=1\\ l\mid s}}^{n} r_l \cdot l\,.$$

Diese Formel ist bei Kenntnis *aller* $\chi(\sigma^s)$ eine Rekursionsformel für die r_l, womit der Zyklentyp von σ durch den Permutationscharakter $\chi\,|_{\langle\sigma\rangle}$ bestimmt ist.

b) Es sei s die Anzahl der Bahnen von G und $\Omega = \dot{\bigcup}_{j=1}^{s} \Omega_i$ die Bahnzerlegung von Ω. Wir berechnen

$$\sum_{\sigma\in G} \chi(\sigma) = \sum_{\sigma\in G} \sum_{\substack{a\in\Omega \\ \sigma a = a}} 1 = \sum_{a\in\Omega} \sum_{\substack{\sigma\in G \\ \sigma a = a}} 1 = \sum_{a\in\Omega} \#G_a = \sum_{i=1}^{s} \sum_{a\in\Omega_i} \#G_a \,.$$

Gemäß der Bahnengleichung (siehe (1.7) b) gilt für jedes i und $a \in \Omega_i$ $\#\Omega_i = \#Ga = (G : G_a) = \frac{\#G}{\#G_a}$, also ist

$$\#G_a = \frac{\#G}{\#\Omega_i}$$

unabhängig von $a \in \Omega_i$. Dies ergibt

$$\sum_{\sigma\in G} \chi(\sigma) = \sum_{i=1}^{s} \sum_{a\in\Omega_i} \frac{\#G}{\#\Omega_i} = \sum_{i=1}^{s} \#\Omega_i \cdot \frac{\#G}{\#\Omega_i} = \sum_{i=1}^{s} \#G = s \cdot \#G \,,$$

wie behauptet. □

§2 Mehrfache Transitivität, Primitivität

a. Mehrfache Transitivität. In naheliegender Verallgemeinerung der Transitivität definieren wir

(2.1) Definition: Eine Gruppe G operiert *r-transitiv* auf Ω, wenn $1 \le r \le \#\Omega$ ist und für je zwei r-Tupel $(a_1, \ldots, a_r)$, $(a'_1, \ldots, a'_r)$ von verschiedenen Elementen in Ω (d.h. $a_i \ne a_j$, $a'_i \ne a'_j$, für $i \ne j$) ein $\sigma \in G$ existiert mit $\sigma(a_i) = a'_i$ für $i = 1, \ldots, r$.
Existiert jeweils genau ein solches σ, so nennt man die Operation *scharf r-transitiv*.

Operiert eine Gruppe G auf einer Menge Ω, so operiert G in natürlicher Weise auch auf der Menge aller r-Tupel Ω^r ($r \in \mathbb{N}$) (komponentenweise) sowie auf der Potenzmenge $\mathbb{P}(\Omega)$ (elementweise). Letztere spaltet sich auf in die Mengen $\binom{\Omega}{r}$ aller r-elementigen Teilmengen von Ω, auf denen G ebenfalls operiert.

Notation: Anders als bei einzelnen Elementen $a \in \Omega$ müssen wir für Mengen $\Delta \subset \Omega$ unterscheiden zwischen der *Fixgruppe*

$$\mathrm{Fix}_G(\Delta) := \{\sigma \in G \mid \sigma|_\Delta = \mathrm{id}_\Delta\} \,,$$

die Δ *elementweise* festlässt, und dem *Stabilisator*

$$G_\Delta = \mathrm{Stab}_G(\Delta) := \{\sigma \in G \mid \sigma\Delta = \Delta\} \,,$$

der Δ als Ganzes in sich überführt. Der Stabilisator $G_\Delta = \mathrm{Stab}_G(\Delta)$ von Δ operiert nicht nur auf ganz Ω, sondern in natürlicher Weise auch auf Δ, nämlich durch Restriktion:

$$\mathrm{res}_\Delta : G_\Delta \to S(\Delta) \,,\ \sigma \mapsto \sigma|_\Delta \,.$$

(2.2) Proposition: *Die Gruppe G operiere auf Ω und es sei $2 \le r \le \#\Omega$. Dann sind äquivalent:*

(i) G operiert (scharf) r-transitiv auf Ω,

(ii) a) G operiert transitiv auf der Menge $\binom{\Omega}{r}$ aller r-elementigen Teilmengen von Ω und
b) für eine/jede r-elementige Teilmenge Δ von Ω ist die Restriktion $\mathrm{res}_\Delta : G_\Delta \to S(\Delta)$ surjektiv (bijektiv),

(iii) a) G operiert transitiv auf Ω und
b) für ein/jedes $a \in \Omega$ operiert G_a (scharf) $(r-1)$-transitiv auf $\Omega \setminus \{a\}$.

iv) Für ein/jedes $a \in \Omega$ gilt:
a) $G_a \neq G$ und
b) G_a operiert (scharf) $(r-1)$-transitiv auf $\Omega \setminus \{a\}$.
Sind die äquivalenten Bedingungen (i) – (iv) erfüllt und ist $n = \#\Omega$, so gilt:

$$n(n-1)(n-2)\cdot\ldots\cdot(n-r+1) \text{ teilt } \#G\,,$$

wobei Gleichheit genau dann gilt, wenn die Gruppe scharf r-transitiv operiert.

Beweis: i) $\Longrightarrow$ ii): Seien $\Delta, \Delta' \subseteq \Omega$ r-elementige Teilmengen von Ω. Wähle beliebige Abzählungen $\Delta = \{a_1, \ldots, a_r\}$ und $\Delta' = \{a'_1, \ldots, a'_r\}$. Dann existiert nach i) ein $\sigma \in G$ mit $\sigma a_i = a'_i$ für $i = 1, \ldots, r$. Insbesondere gilt also $\sigma\Delta = \Delta'$, womit gezeigt ist, dass G transitiv auf $\binom{\Omega}{r}$ operiert.
ad ii) b): Sei $\Delta = \{a_1, \ldots, a_r\}$ eine beliebige r-elementige Teilmenge von Ω und $\tau \in S_\Delta$ eine beliebige Permutation auf Δ. Zu $a'_i := \tau(a_i)$ existiert dann gemäß a) (genau) ein $\sigma \in G$ mit der Eigenschaft $\sigma a_i = a'_i = \tau(a_i)$ für alle i. Also $\sigma\Delta = \tau(\Delta) = \Delta$, d. h. $\sigma \in G_\Delta$ und für alle $a \in \Delta$ $\sigma a = \tau(a)$, d. h. $\sigma\,|_\Delta = \tau$. Damit ist die Restriktionsabbildung surjektiv (bzw. bijektiv bei scharfer r-Transitivität).

ii) $\Longrightarrow$ i): Sei $\Delta = \{b_1, \ldots, b_r\}$ eine r-elementige Teilmenge mit der Eigenschaft ii) b). Wir wollen die (scharfe) r-Transitivität von G nachweisen; also seien $(a_1, \ldots, a_r)$, $(a'_1, \ldots, a'_r)$ zwei r-Tupel von verschiedenen Elementen in Ω. Dann gibt es gemäß ii) a) Elemente $\sigma, \tau \in G$ mit

$$\sigma\{a_1, \ldots, a_r\} = \Delta \quad \text{und} \quad \tau\{a'_1, \ldots, a'_r\} = \Delta\,.$$

Damit ist durch $\sigma a_i \mapsto \tau a'_i$ eine Permutation in S_Δ gegeben. Gemäß ii) b) existiert dazu (genau) ein $\rho \in G$ mit $\rho\sigma a_i = \tau a'_i$ $(i = 1, \ldots, r)$. Dann hat $\alpha = \tau^{-1}\rho\sigma \in G$ die gewünschte Eigenschaft $\alpha a_i = a'_i$ $(i = 1, \ldots, r)$.

i) $\Longrightarrow$ iii): a) ist eine Abschwächung von i), da man jedes Element als erstes Glied eines r-Tupels verschiedener Elemente ansehen kann (im Falle $r \leq \#\Omega$).
Sei nun $a \in \Omega$ beliebig. Weiter seien $(a_1, \ldots, a_{r-1})$, $(a'_1, \ldots, a'_{r-1})$ zwei $r-1$-Tupel verschiedener Elemente in $\Omega \setminus \{a\}$. Dann bilden $(a_1, \ldots, a_{r-1}, a)$ und $(a'_1, \ldots, a'_{r-1}, a)$ zwei r-Tupel verschiedener Elemente in Ω. Zu diesen existiert gemäß i) (genau) ein $\sigma \in G$ mit $\sigma a_i = a'_i$ $(i = 1, \ldots, r-1)$ und $\sigma a = a$. Damit ist $\sigma \in G_a$ mit den gewünschten Eigenschaften gefunden: ii) b) ist gezeigt.

iii) $\Longrightarrow$ i): Sei a ein Element mit der Eigenschaft iii) b). Seien nun $(a_1, \ldots, a_r)$, $(a'_1, \ldots, a'_r)$ zwei r-Tupel verschiedener Elemente in Ω. Gemäß iii) a) existieren $\sigma, \tau \in G$ mit $\sigma a_r = a$ und $\tau a'_r = a$. Wegen $\sigma a_i \neq \sigma a_r = a$ $(i = 1, \ldots, r-1)$ bildet $(\sigma a_1, \ldots, \sigma a_{r-1})$ ein $r-1$-Tupel von verschiedenen Elementen in $\Omega \setminus \{a\}$. Ebenso $(\tau a'_1, \ldots, \tau a'_{r-1})$. Gemäß iii) b) existiert (genau) ein $\rho \in G_a$ mit $\rho\sigma a_i = \tau a'_i$ $(i = 1, \ldots, r-1)$. Wegen $\rho \in G_a$ folgt auch $\rho\sigma a_r = \rho a = a = \tau a'_r$. Insgesamt ergibt sich so für $\alpha = \tau^{-1}\rho\sigma \in G$ die gewünschte Eigenschaft $\alpha a_i = a'_i$ für alle $i = 1, \ldots, r$.

iii) $\Longrightarrow$ iv): Ist G transitiv auf Ω, so gibt es wegen $2 \leq \#\Omega$ ein $\sigma \in G$ mit $\sigma a \neq a$, also ist $G \neq G_a$. Gilt iii) b) für *ein* $a \in \Omega$, so folgt wegen Transitivität iii) a) die Aussage iii)b) für *jedes* $b \in \Omega$.

iv) $\Longrightarrow$ iii): Sei $a \in \Omega$ mit den Eigenschaften von iv). Wir müssen lediglich iii) a), die Transitivität von G auf Ω zeigen. Seien also $b, c \in \Omega$, o. E. verschieden.
1. Fall: b, c sind *beide* von a verschieden. Dann gibt es gemäß iv) b) ein $\sigma \in G_a \subset G$ mit $\sigma b = c$.
2. Fall: Ist $b = a$, so existiert gemäß iv) a) ein $\tau \in G$ mit $\tau b = \tau a \neq a$. Gemäß 1. Fall existiert nun ein $\sigma \in G_a \subset G$ mit $\sigma\tau a = c$. Damit ist $\rho = \sigma\tau \in G$ gefunden mit $\rho b = c$.

Beweis des Zusatzes: Seien $a_1, \ldots, a_r$ verschiedene Elemente in Ω. Wir definieren rekursiv

$$G_{a_1,\ldots,a_{k+1}} := (G_{a_1,\ldots,a_k})_{a_{k+1}}\,.$$

Es gilt dann nach dem Satz von Lagrange

$$\#G = (G : G_{a_1}) \cdot (G_{a_1} : G_{a_1,a_2}) \cdot \ldots \cdot (G_{a_1,\ldots,a_{r-1}} : G_{a_1,\ldots,a_r}) \cdot \#G_{a_1,\ldots,a_r}\,.$$

Wegen der rekursiven Beschreibung der r-Transitivität iii) sind die Gruppenindizes gleich den entsprechenden Bahnlängen und man erhält mit $n = \#\Omega$

$$\#G = n \cdot (n-1) \cdot \ldots \cdot (n-r+1) \cdot \#G_{a_1,\ldots,a_r} .$$

Im Falle scharfer r-Transitivität besteht die Gruppe $G_{a_1,\ldots,a_r} = \{\sigma \in G \mid \sigma a_i = a_i\}$ gemäß ii) b) nur aus der Identität. Damit ist der Zusatz vollständig bewiesen.

(2.3) Beispiele: a) S_n ist scharf n-transitiv und für $n \geq 3$ ist A_n scharf $(n-2)$-transitiv. 5/14.11.
b) D_{2n} ist nicht 2-transitiv für $n > 3$, denn $n(n-1) \mid \#D_{2n} = 2n \iff n \leq 3$. Alternatives Argument: Benachbarte Ecken bleiben unter der Operation von D_{2n} benachbart, und für $n > 3$ gibt es benachbarte und nicht benachbarte Eckenpaare.
c) $\mathrm{GL}_d(2)$ operiert 2-transitiv auf $\Omega = \mathbb{F}_2^d \setminus \{0\}$, denn je zwei verschiedene Vektoren $\neq 0$ sind linear unabhängig (Grundkörper $\mathbb{F}_2$!), also zu Basen ergänzbar, und auf den geordneten Basen operiert $\mathrm{GL}_d(2)$ (scharf) transitiv.
Die Operation auf Ω ist jedoch nicht 3-transitiv, denn $\binom{\Omega}{3}$ zerfällt unter der Operation von $\mathrm{GL}_d(2)$ in zwei Bahnen, nämlich die linear abhängigen Tripel einerseits und die linear unabhängigen andererseits.
d) Wir betrachten die projektive Gerade über einem Körper K:

$$\Omega = I\!P^1(K) = K \,\dot\cup\, \{\infty\} = (K^2 \setminus \{0\})/\sim$$

(Dabei bezeichnet $\sim$ die Äquivalenzrelation $(a,b) \sim (a',b') \iff (a',b') = \alpha \cdot (a,b)$ für ein $\alpha \in K^\times$ mit den Äquivalenzklassen $(a:b) = (a,b)/\sim = K^\times(a,b)$.) Darauf operiert die *projektive lineare Gruppe*

$$\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^\times E_2 .$$

Für $K = \mathbb{C}$ ist Ω die Riemannsche Zahlenkugel und $\mathrm{PGL}_2(\mathbb{C})$ die Gruppe der *gebrochen linearen* oder auch *Möbius-Transformationen*

$$\mathrm{PGL}_2(\mathbb{C}) = \{\frac{az+b}{cz+d} \mid ad - bc \neq 0\} .$$

Wir benutzen diese letzte Beschreibung von PGL_2 auch für beliebige Körper und zeigen:

(2.4) Proposition: $\mathrm{PGL}_2(K)$ *operiert scharf 3-transitiv auf* $I\!P^1(K)$. *Für endliche Körper* K *gilt*

$$\#\mathrm{PGL}_2(K) = (\#K+1)\#K(\#K-1) .$$

Beweis: Zunächst kann $\infty \in I\!P^1(K)$ durch $\frac{1}{z}$ auf 0 abgebildet werden, also gilt $G \neq G_\infty$. Die Fixgruppe G_∞ von ∞ ist gerade die Gruppe der linearen Transformationen

$$G_\infty = \{az + b \mid a \in K^\times ,\ b \in K\} .$$

Diese operiert auf $\Omega \setminus \{\infty\} = K$ transitiv, denn 0 kann durch $z + a$ auf jedes $a \in K$ abgebildet werden. Die Fixgruppe der 0 darin ist

$$G_{\infty,0} = (G_\infty)_0 = \{az \mid a \in K^\times\} ,$$

und diese operiert scharf transitiv auf $\Omega \setminus \{0,\infty\} = K^\times$. Damit ist gemäß Proposition (2.2) iv) die Behauptung bewiesen.
Der Zusatz für endliche Körper K ergibt sich ebenfalls aus (2.2) unter Beachtung von $\#\Omega = \#(K \cup \{\infty\}) = \#K + 1$.

(2.5) Proposition: *Operiert* G *transitiv auf* Ω *und ist* χ *der Permutationscharakter, so gilt:*

$$G \text{ 2-transitiv auf } \Omega \iff \sum_{\sigma \in G} \chi^2(\sigma) = 2 \cdot \#G .$$

Es gilt allgemeiner: Ist für irgendein $a \in \Omega$ s die Anzahl der Bahnen von G_a auf Ω (!) (also einschließlich der 'trivialen' Bahn $\{a\}$), *so gilt:*

$$\frac{1}{\#G} \sum_{\sigma \in G} \chi^2(\sigma) = s\,.$$

Beweis: Wegen der vorausgesetzten Transitivität ist s von a unabhängig!
Es gilt nun

$$\begin{aligned}\sum_{\sigma \in G} \chi^2(\sigma) &= \sum_{\sigma \in G} \chi(\sigma) \cdot \#\{a \in \Omega \mid \sigma a = a\} \\ &= \sum_{\sigma \in G} \sum_{\substack{a \in \Omega \\ \sigma a = a}} \chi(\sigma) = \sum_{a \in \Omega} \sum_{\substack{\sigma \in G \\ \sigma a = a}} \chi(\sigma) \\ &= \sum_{a \in \Omega} \sum_{\sigma \in G_a} \chi(\sigma) \\ &\underset{(1.13)}{=} \sum_{a \in \Omega} s \cdot \#G_a = s \cdot \#\Omega \cdot \#G_a \underset{(1.8)}{=} s \cdot \#G\,.\end{aligned}$$

In der letzten Gleichung und bei der Unabhängigkeit der Zahl s von a wurde die Transitivität von G benötigt.

b. Primitivität. Eine wichtige Begriffsbildung zwischen einfacher und mehrfacher Transitivität ist die sog. Primitivität von Permutationsdarstellungen:

(2.6) Definition: Die Gruppe G operiere auf der Menge Ω.
a) Eine Teilmenge $B \subset \Omega$ heißt *Block* unter der Operation von G auf Ω (kurz G-Block), wenn gilt:

$$\sigma B = B \ \vee \ \sigma B \cap B = \emptyset \quad \text{für alle } \sigma \in G.$$

Offenbar sind Ω, $\emptyset$ und die einpunktigen Mengen $\{a\}$ $(a \in \Omega)$ Blöcke bzgl. jeder Operation auf Ω. Dies sind die sog. trivialen Blöcke.
b) Die Operation von G heißt *primitiv* auf Ω, wenn sie transitiv ist und nur die trivialen Blöcke besitzt.

(2.7) Bemerkung: *Operiert eine Gruppe G 2-transitiv, so auch primitiv.*

Beweis: Sei $B \subset \Omega$ ein G-Block mit mindestens 2 Elementen, etwa $a, b \in B$, $a \neq b$. Da G 2-fach transitiv operiert, existiert zu jedem $c \in \Omega, c \neq a$ ein $\sigma \in G$ mit $\sigma a = a$ und $\sigma b = c$. Da B ein Block ist, und $a \in \sigma B \cap B$ gilt, muss $\sigma B = B$ sein, und folglich gilt $c \in \sigma B = B$. Dies heißt, dass ganz Ω in B liegt; G operiert damit definitionsgemäß primitiv. □

(2.8) Beispiel: Sei Ω eine endliche Menge, zerlegt in k disjunkte Mengen B_j $(j = 1, \ldots, k)$ von *gleicher* Mächtigkeit b, also $\#\Omega = k \cdot b$. Wir betrachten nun die Gruppe $S(B_1|\ldots|B_k)$ aller Permutationen der symmetrischen Gruppe S_Ω, die diese *Partition* (B_j) von Ω 'respektieren', d.h.

$$S(B_1|\ldots|B_k) := \{\sigma \in S_\Omega \mid \bigwedge_i \bigvee_j \sigma B_i = B_j\}\,.$$

Diese Permutationsgruppe $G = S(B_1|\ldots|B_k)$ ist transitiv auf Ω. Die Mengen B_j sind G-Blöcke der Länge b, so dass G für $1 < b < \#\Omega$ imprimitiv ist.
Die Elemente von G permutieren definitionsgemäß die k Blöcke B_j, also hat man eine natürliche Permutationsdarstellung $p\colon G \to S_k$ gegeben durch

$$p(\sigma)(i) = j \iff \sigma B_i = B_j\,.$$

p ist offenbar surjektiv und der Kern dieser Darstellung p

$$\operatorname{Ke} p = \{\sigma \in S_\Omega \mid \sigma B_j = B_j \text{ für alle } j\}$$

ist offensichtlich isomorph zur Gruppe

$$(S_b)^k = \underbrace{S_b \times \ldots \times S_b}_{k-\text{mal}},$$

da man auf jedem Block B_j unabhängig beliebige Permutationen $\sigma_j \in S_b \simeq S_{B_j}$ vorschreiben kann. Damit ist $S(B_1|\ldots|B_k)$ eine Gruppenerweiterung des Normalteilers $(S_b)^k$ mit S_k und hat die Ordnung

$$\#S(B_1|\ldots|B_k) = \#\mathrm{Ke}\, p \cdot \#\mathrm{Im}\, p = (b!)^k \cdot k!\,.$$

Diese Gruppe $S(B_1|\ldots|B_k)$ ist das Kranzprodukt $S_b \wr S_k$ im Sinne der nachfolgenden Definition: 6/21.11.

(2.9) Definition: Sei G eine (abstrakte) Gruppe und H eine Gruppe mit einer fixierten Permutationsdarstellung $p : H \to S_k$. Dann definiert man das *Kranzprodukt* (angelsächsisch 'wreath product', wreath = Kranz, Gewinde) als

$$G \wr H := G^k \cdot H = \{((\sigma_1, \ldots, \sigma_k), \tau) \mid \sigma_i \in G\,,\ \tau \in H\}$$

mit der Multiplikation

$$((\sigma_1, \ldots, \sigma_k), \tau) \cdot ((\sigma'_1, \ldots, \sigma'_k), \tau') = ((\sigma_1, \ldots, \sigma_k)(\sigma'_{\tau 1}, \ldots, \sigma'_{\tau k}), \tau\tau')\,.$$

Einschub: Semidirekte Produkte. Dieses Kranzprodukt ist ein *semidirektes* Produkt von G^k mit H, wobei H auf G^k durch Permutation der Faktoren gemäß p operiert.

Wir erinnern zunächst an das (äußere) direkte Produkt zweier Gruppen N und H. Dies ist das kartesische Produkt $G = N \times H$ mit komponentenweiser Multiplikation. Dieses hat folgende Eigenschaften:
1. Beide Faktoren sind (isomorph zu) Untergruppen in G:

$$N \hookrightarrow G\,, \quad \sigma \mapsto (\sigma, 1)\,, \qquad H \hookrightarrow G\,, \quad \tau \mapsto (1, \tau)\,,$$

2. $G = NH$ mit $N \lhd G$, $H \leq G$ und $N \cap H = \{1\}$, so dass die Darstellung $\rho = \sigma\tau$ mit $\sigma \in N$, $\tau \in H$ eindeutig ist.
3. Die Elemente von N und H sind vertauschbar: $\sigma\tau = \tau\sigma$.
Man nennt nun eine Gruppe G das direkte Produkt von Untergruppen N und H, wenn 2. und 3. erfüllt sind (und daher $G \simeq N \times H$ ist).

Verzichtet man auf 3. so erhält man den Begriff des *semidirekten* Produktes:

$$N \lhd G\,,\ H \leq G\,,\ G = NH \text{ mit } N \cap H = \{1\}\,.$$

Durch diese Forderungen ist das semidirekte Produkt G noch nicht eindeutig festgelegt. Zwar ist jedes Element $\rho \in G$ *eindeutig* als Produkt $\rho = \sigma\tau$ ($\sigma \in N$, $\tau \in H$) darstellbar, also ist G *mengenmäßig* gleich dem kartesischen Produkt von N und H, aber die Gruppenstruktur liegt erst fest, wenn die Multiplikation in G bestimmt ist. Wir betrachten also ein beliebiges Produkt

$$\rho \cdot \rho' = (\sigma\tau) \cdot (\sigma'\tau') = \sigma(\tau\sigma'\tau^{-1}) \cdot \tau\tau' \qquad (*)\,.$$

Da N ein Normalteiler ist, ist $\tau\sigma'\tau^{-1} \in N$ und jedes $\tau \in H$ bestimmt eine Gruppenoperation auf N: $\sigma' \mapsto \tau\sigma'\tau^{-1}$. Umgekehrt bestimmt diese Gruppenoperation die Struktur von G, denn durch $(*)$ ist die Multiplikation in G zurückgeführt auf die Multiplikationen in N und in H sowie die Kenntnis der *Operation* von H auf N.

Beispiele: a) Das oben definierte Kranzprodukt ist das semidirekte Produkt des Normalteilers G^k mit der Gruppe H, wobei die Operation von H auf G^k durch Permutation der Komponenten erfolgt:

$$\tau \in H \to S_k : (\sigma_1, \ldots, \sigma_k) \mapsto (\sigma_{\tau 1}, \ldots, \sigma_{\tau k})\,.$$

b) Die Diedergruppe D_{2n} wird erzeugt von dem n-Zyklus $\sigma = (1, \ldots, n)$ und dem Element der Ordnung 2 $\tau = (1,n) \circ (2,n-1) \circ (3,n-2) \ldots$. Damit ist $N = \langle \sigma \rangle$ eine Untergruppe der Ordnung n, also vom Index 2 und folglich Normalteiler in D_{2n}, während $H := \langle \tau \rangle$ eine Untergruppe der Ordnung 2 ist. Wegen $\tau \notin N$ ist $N \cap H = \{1\}$ und daher $D_{2n} = NH$ semidirektes Produkt von $N \simeq C_n$ und $H \simeq C_2$. Die Operation von H auf N ist gegeben durch

$$\tau \circ \sigma \circ \tau^{-1} = \tau \circ \sigma \circ \tau = (1, n, n-1, \ldots, 2) = \sigma^{-1} .$$

Damit operiert $\tau \in H$ auf σ und damit auf allen Potenzen σ^l durch Inversenbildung! Wir erhalten so eine andere, strukturelle Definition der Diedergruppen D_{2n}:
Die Diedergruppe der Ordnung $2n$ ist das semidirekte Produkt der zyklischen Gruppe C_n der Ordnung n mit der zyklischen Gruppe C_2 der Ordnung 2, wobei die Operation von C_2 auf C_n die Inversenbildung in C_n ist.

Nachtrag 3

Die Gruppen der Ordnung $2p$: Ist G eine Gruppe der Ordnung $2p$, p eine Primzahl, so gilt α) G ist zyklisch, 9/12.12.
oder β) $p = 2$ und $G \simeq V_4$ ist die Kleinsche Vierergruppe,
oder γ) $p \neq 2$ und $G \simeq D_{2p}$ ist die Diedergruppe.

Beweis: Nach dem ersten Sylowsatz gibt es zu jedem Primteiler der Gruppenordnung auch eine Untergruppe dieser Ordnung. Als Gruppe von Primzahlordnung ist diese dann zyklisch, also gibt es auch stets ein *Element* von Primzahlordnung. In G existiert also ein σ mit $\operatorname{ord} \sigma = p$. Damit ist $H := \langle \sigma \rangle$ eine Untergruppe von G von der Ordnung p und dem Index 2, insbesondere also Normalteiler in G.

1. Fall $p \neq 2$: Wir wählen wieder gemäß dem Sylowsatz ein Element τ in G mit $\operatorname{ord} \tau = 2$. Wegen $2 \not| \, p = \# H$ gilt $\tau \notin H$ und wegen $(G : H) = 2$ folgt $G = \langle \sigma, \tau \rangle$, genauer

$$G = H \,\dot\cup\, \tau H = \{\tau^i \sigma^k \mid i = 0, 1 \,,\ 0 \leq k < p\} .$$

Die Struktur von G liegt daher fest, wenn die Multiplikationstafel bekannt ist:

$$\tau^i \sigma^k \cdot \tau^j \sigma^l = \tau^I \sigma^K .$$

Da die Ordnungen von σ, τ gegeben sind, genügt es die Vertauschungsregel $\sigma \cdot \tau = \tau^\mu \sigma^\nu$ zu kennen. Wegen $\tau \notin H$ ist $\mu \neq 0$, also $\mu = 1$. Die Struktur der Gruppe G liegt also fest, wenn die Zahl ν bestimmt ist mit

$$\sigma \cdot \tau = \tau \sigma^\nu .$$

Wir definieren nun ν und bestimmen alle Möglichkeiten. Da H Normalteiler in G ist, folgt

$$\tau^{-1} \sigma \tau \in H \,, \text{ also } \tau^{-1} \sigma \tau = \sigma^\nu .$$

Dabei ist ν modulo $p = \operatorname{ord} \sigma$ eindeutig bestimmt. Wegen $\tau^2 = 1$ folgt

$$\sigma = \tau^{-2} \sigma \tau^2 = \tau^{-1} \sigma^\nu \tau = \sigma^{(\nu^2)} .$$

Daraus folgt aber

$$\nu^2 \equiv 1 \bmod p \iff p \mid (\nu^2 - 1) = (\nu+1)(\nu-1) \iff p \mid \nu+1 \ \vee \ p \mid \nu-1 \iff \nu \equiv \pm 1 \bmod p .$$

(Oder anders formuliert: Im Körper $\mathbb{F}_p$ hat $X^2 - 1$ nur die beiden Wurzeln ± 1.) Es gibt (modulo p) also nur zwei Möglichkeiten für ν, und das heißt nur zwei mögliche Vertauschungsregeln

$$\sigma\tau = \tau\sigma^\nu \text{ mit } \nu = \pm 1 .$$

Fall (I) $\nu = 1$: Dann gilt $\sigma\tau = \tau\sigma$, G ist abelsch. Wegen $p \neq 2$ ist G sogar zyklisch; wir zeigen nämlich, dass $\tau\sigma$ die Ordnung $2p$ hat:

$$\operatorname{ord}(\tau\sigma) = 2p = \#G\,.$$

Beweis: Wegen der Vertauschbarkeit und $\operatorname{ord}\tau = 2$, $\operatorname{ord}\sigma = p$ mit p ungerade gilt

$$(\tau\sigma)^{2p} = 1\,,\ (\tau\sigma)^2 = \sigma^2 \neq 1\,,\ (\tau\sigma)^p = \tau^p = \tau \neq 1\,.$$

Die Ordnung von $\tau\sigma$ teilt also $2p$, ist aber weder Teiler von 2 noch von p, also gleich $2p$; G ist zyklisch.
Fall (II) $\nu = -1$: Dann ist $G = \langle\tau, \sigma\rangle$ mit $\operatorname{ord}\tau = 2$, $\operatorname{ord}\sigma = p$ und $\sigma\tau = \tau\sigma^{-1}$. Dies ist aber genau die oben gegebene Beschreibung der Diedergruppe (durch Erzeugende und Relationen) als semidirektes Produkt.

2. Fall: $p = 2$: In diesem Fall ist $H = \{1, \sigma\}$ von der Ordnung 2 und G von der Ordnung 4. Wir wählen nun $\tau \in G$, $\tau \notin H$, so dass wieder $G = \langle\sigma, \tau\rangle$ ist. Die Faktorgruppe G/H hat die Ordnung 2, ist daher zyklisch und wird erzeugt von $\bar\tau = \tau H$, also $\bar\tau^2 = \bar 1$ bzw. $\tau^2 \in H = \{1, \sigma\}$. Damit ergeben sich wieder zwei Fälle, nämlich $\tau^2 = 1$ oder $\tau^2 = \sigma$.
Fall (I) $\tau^2 = 1$: Dann können wir wie oben schließen $\sigma\tau = \tau\sigma^\nu$, wobei hier $\nu = 1$ sein muss (denn $\nu = 0 \implies \sigma = 1$). Damit ist $G = \langle\sigma, \tau\rangle$ mit $\sigma^2 = \tau^2 = 1$ und $\sigma\tau = \tau\sigma$: G ist also die (abelsche) Kleinsche Vierergruppe V_4.
Fall (II) $\tau^2 = \sigma$: In diesem Fall hat $\tau^2 = \sigma$ die Ordnung 2, also τ die Ordnung 4. Damit erzeugt τ ganz G: G ist zyklisch. □

Ende Nachtrag 3

Wir kommen nun wieder zurück zur Untersuchung der Blöcke in transitiven Permutationsdarstellungen. 6/21.11.

(2.10) Proposition: *Es sei $P\colon G \to S_\Omega$ eine transitive Permutationsdarstellung. $B \subseteq \Omega$ sei ein nicht-leerer G-Block und $H := G_B = \{\sigma \in G \mid \sigma B = B\}$ die Stabilisatorgruppe des Blockes B. Dann gilt für $a \in B$:*
a) $G_a \subset G_B$ und die Gruppe G_B operiert transitiv auf B. Die Bilder σB ($\sigma \in G$) des Blockes B sind ebenfalls G-Blöcke und bilden eine Klasseneinteilung von Ω. G operiert transitiv auf der Menge $\mathcal{B} = \{\sigma B \mid \sigma \in G\}$ dieser Blöcke.
b) Sind G und Ω endlich, so gilt:

$$\begin{aligned} \textit{Blocklänge} \quad & b := \#B = (H : G_a)\,, \\ \textit{Anzahl der Blöcke} \quad & k := \#\mathcal{B} = (G : H)\,, \\ \textit{Grad} \quad & n := \#\Omega = b \cdot k \end{aligned}$$

c) Sind unter den Voraussetzungen von b) $B_1, \ldots, B_k$ die verschiedenen unter den Blöcken σB ($\sigma \in G$), so bildet die Permutationsdarstellung $P\colon G \to S_\Omega$ die Gruppe G in das Kranzprodukt $S(B_1|\ldots|B_k)$ ab:

$$P(G) \subset S(B_1|\ldots|B_k)\,.$$

Beweis: a) Sei $\sigma \in G_a$ und angenommen $\sigma B \neq B$. Da B ein Block ist, folgt $\sigma B \cap B = \emptyset$, im Widerspruch zu $\sigma a = a \in \sigma B \cap B$.
Zum Nachweis der Transitivität sei $b \in B$ beliebig. Da G transitiv ist, gibt es zunächst ein $\sigma \in G$ mit $\sigma a = b$. Wir zeigen, dass σ bereits in G_B liegt, womit dann die Transitivität von G_B auf B gezeigt wäre. Wegen $a, b \in B$ folgt $b = \sigma a \in B \cap \sigma B$, also $\sigma B \cap B \neq \emptyset$. Gemäß Blockeigenschaft von B folgt dann aber $\sigma B = B$, d. h. $\sigma \in G_B$.
Gemäß Blockeigenschaft sind die verschiedenen σB disjunkt, und wegen der Transitivität von G ist $\Omega = \bigcup_{\sigma\in G} \sigma B$.
Definitionsgemäß ist $\mathcal{B} = G.B$ die Bahn von B unter der Operation von G, also ist die Operation transitiv.

b) $H = G_B$ operiert transitiv auf B, also $B = Ha$. Gemäß der Bahngleichung folgt $b = \#B = \#(Ha) = (H : H_a)$. Nun gilt aber gemäß a) $G_a \subset G_B = H$, also $H_a = G_a \cap H = G_a$.
Wieder verwenden wir die Bahngleichung, diesmal für die Operation von G auf $\mathcal{B}$. Dies ergibt $k = \#\mathcal{B} = \#G.B = (G : G_B) = (G : H)$.
Die dritte Behauptung $n = b \cdot k$ ergibt sich aus der disjunkten Zerlegung von Ω durch die σB, die alle die gleiche Mächtigkeit b haben.

c) Sei $\sigma \in G$ und $B_i = \rho B$ einer der Blöcke. Dann ist $\sigma B_i = \sigma\rho B \in \mathcal{B}$, also $\sigma B_i = B_j$. Also respektiert die Permutation $P(\sigma)$ die Zerlegung $\Omega = \bigcup B_i$, gehört also zum Kranzprodukt $S(B_1|\ldots|B_k)$.

(2.11) Korollar: *Operiert eine Gruppe G auf einer Menge Ω, deren Mächtigkeit eine Primzahl ist, so ist die Operation primitiv.*

Eine Übersicht über die möglichen Blöcke einer Permutationsgruppe gibt der folgende

(2.12) Satz: *Es operiere G transitiv auf Ω und es sei G_a die Fixgruppe einer Ziffer $a \in \Omega$. Dann gilt:*
a) Die Zuordnungen

$$G_a \leq H \leq G \mapsto B := H.a \quad \text{und} \quad a \in B \text{ Block } \mapsto H := \mathrm{Stab}_G(B)$$

sind zueinander inverse, inklusionstreue Bijektionen zwischen den Obergruppen von G_a und den G-Blöcken B, die a enthalten.
Dabei gilt $\#B = (H : G_a)$.
Die verschiedenen Zerlegungen von Ω in G-Blöcke gemäß (2.10), a) entsprechen daher bijektiv den Obergruppen H von G_a.
b) Genau dann operiert G primitiv auf Ω, wenn die Fixgruppe G_a einer beliebigen Ziffer $a \in \Omega$ eine maximale Untergruppe in G ist.

Beweis: a) rechnet man leicht nach. Gemäß a) gibt es Blöcke B mit $1 < \#B < \#\Omega$ genau dann, wenn es Untergruppen H gibt mit $G_a < H < G$, wenn also G_a nicht maximal ist in G.

(2.13) Proposition: *Operiert G transitiv auf Ω und ist N ein Normalteiler in G, so bilden die N-Bahnen Blöcke bzgl. G. Insbesondere sind Normalteiler $N \neq 1$ in primitiven Permutationsgruppen $G \leq S_\Omega$ stets transitiv auf Ω.* 9/12.12.

Beweis: Ist $a \in \Omega$ und Na die Bahn von a unter N, so ist für alle $\sigma \in G$ offenbar $\sigma Na = \sigma N\sigma^{-1} \cdot \sigma a = N\sigma a$ wieder eine Bahn unter N, also disjunkt zu Na oder damit identisch. Die N-Bahnen sind also G-Blöcke und der erste Teil der Behauptung folgt.

Wäre nun in einer primitiven Permutationsgruppe $G \leq S_\Omega$ ein Normalteiler N nicht transitiv, so wären die N-Bahnen $Na \neq \Omega$, also als Blöcke der primitiven Gruppe G einpunktig. Also wären alle $a \in \Omega$ Fixpunkte unter N. Wegen $N \subset S(\Omega)$ folgte $N = 1$.

c. Die Sätze von Jordan. Aus der Definition der 2-Transitivität folgt unmittelbar: Enthält eine 2-transitive Permutationsgruppe $G \subset S(\Omega)$ eine Transposition, so enthält sie alle Transpositionen (siehe (1.4), Formel iii) im Beweis von b)), ist also ganz $S(\Omega)$. Wir wollen nun zeigen, dass für diesen Schluss schon die Primitivität ausreicht, und verwandte Resultate beweisen.

Eine beweistechnisch wichtige Eigenschaft primitiver Permutationsgruppen ist das folgende

(2.14) Lemma: *Operiert G primitiv auf einer endlichen Menge Ω und ist $\Delta \subsetneq \Omega$ eine echte Teilmenge, so gilt: Sind $a, b \in \Delta$ und $a \neq b$, so gibt es eine Permutation $\sigma \in G$ mit*

$$a \in \sigma\Delta\,,\ b \notin \sigma\Delta\,.$$

Beweis: Wir setzen

$$\Delta_a = \bigcap_{\substack{\sigma \in G \\ a \in \sigma\Delta}} \sigma\Delta$$

und zeigen, dass Δ_a ein Block ist. Wegen der Primitivität von G und $\Delta \neq \Omega$ muss dann $\Delta_a = \{a\}$ sein und (2.14) ist bewiesen.

Sei also nun $\tau \in G$ und $c \in \Delta_a \cap \tau\Delta_a$. Dann exisitiert ein $\rho \in G$ mit $\rho a = c$, also

$$a \in \Delta_a \cap \rho^{-1}\Delta_a \cap \rho^{-1}\tau\Delta_a \,. \tag{1}$$

Wir zeigen nun allgemein für beliebiges $\tau \in G$

$$a \in \Delta_a \cap \tau\Delta_a \implies \Delta_a = \tau\Delta_a \,. \tag{2}$$

Begründung: $a \in \tau\Delta_a = \bigcap\limits_{\sigma\Delta \ni a} \tau\sigma\Delta$ heißt nichts anderes als

$$\bigwedge_{\sigma \in G} a \in \sigma\Delta \Rightarrow a \in \tau\sigma\Delta \tag{3}$$

und daher

$$\tau\Delta_a = \bigcap_{a \in \sigma\Delta} \tau\sigma\Delta \supset \bigcap_{a \in \tau\sigma\Delta} \tau\sigma\Delta = \bigcap_{a \in \rho\Delta} \rho\Delta = \Delta_a \,. \tag{4}$$

da gemäß (3) die Durchschnittsbildung $\bigcap\limits_{a \in \sigma\Delta}$ weniger umfassend ist als $\bigcap\limits_{a \in \tau\sigma\Delta}$. Da Δ_a und $\tau\Delta_a$ gleichmächtig sind, folgt aus (4) die Behauptung $\Delta_a = \tau\Delta_a$ von (2). Mit (2) folgt dann aber aus (1) $\rho^{-1}\Delta_a = \Delta_a = \rho^{-1}\tau\Delta_a$ bzw. $\tau\Delta_a = \Delta_a$, womit Lemma (2.14) bewiesen ist.

Als weitere Vorbereitungen für die nachfolgenden Beweise zeigen wir zunächst das folgende nützliche Primitivitätskriterium

(2.15) Proposition: *G operiere auf Ω. Es seien $U_1, U_2 \leq G$ Untergruppen mit $G = \langle U_1, U_2\rangle$ und $\Omega_i \subset \Omega$ ($i = 1, 2$) U_i-Bahnen mit $\Omega = \Omega_1 \cup \Omega_2$. Dann gilt:*
a) G operiert transitiv auf $\Omega \iff \Omega_1 \cap \Omega_2 \neq \emptyset$.
b) Sind die Bedingungen von a) erfüllt und operieren zusätzlich U_i primitiv auf Ω_i (i=1,2), so ist G primitiv auf Ω.

Beweis: a) Ist $\Omega_1 \cap \Omega_2 \neq \emptyset$, etwa $c \in \Omega_1 \cap \Omega_2$, so gilt $U_i c = \Omega_i$, also $Gc \supset \Omega_1 \cup \Omega_2 = \Omega$. Damit ist $Gc = \Omega$ eine Bahn unter G, G operiert transitiv.
Ist umgekehrt $\Omega_1 \cap \Omega_2 = \emptyset$, so ist Ω_1 nicht nur stabil unter U_1, sondern wegen $\Omega_1 = \Omega \setminus \Omega_2$ auch unter U_2, also unter $G = \langle U_1, U_2\rangle$. Damit ist Ω_1 eine Bahn unter G und G ist nicht transitiv, da die Bahn $\Omega_2 \neq \emptyset$ und somit $\Omega_1 = \Omega \setminus \Omega_2 \neq \Omega$ ist.
b) Da $\Omega = \Omega_1 \cup \Omega_2$ eine nicht-disjunkte Vereinigung ist, muss eine der beiden Mengen Ω_i die Bedingung $\#\Omega_i > \#\Omega/2$ erfüllen, und die Behauptung b) ergibt sich aus dem nachfolgenden

(2.16) Hilfssatz: *G operiere transitiv auf Ω. Es sei $U \leq G$ eine Untergruppe und $\Delta \subseteq \Omega$ ein U-Orbit, auf dem U primitiv operiert. Ist dann $\#\Delta > \#\Omega/2$, so operiert G primitiv auf Ω.*

Beweis: Es sei B ein Block für G mit $1 \leq \#B < \#\Omega$. Dann ist $D := B \cap \Delta$ ein Block für U in Δ: Sei nämlich $\tau \in U$ und $D \cap \tau D \neq \emptyset$. Dann gilt erst recht $B \cap \tau B \neq \emptyset$ und damit $B = \tau B$. Also erhält man

$$\tau D = \tau(B \cap \Delta) = \tau B \cap \tau\Delta = B \cap \Delta = D \,.$$

Damit ist $D = \Delta \cap B$ ein U-Block in Δ, also gilt nach Voraussetzung entweder $D = \Delta$ oder $\#D \leq 1$. Im ersten Falle folgt $\Delta \subseteq B$ und damit

$$\#\Omega/2 < \#\Delta \leq \#B < \#\Omega \,,$$

im Widerspruch zu $\#B \mid \#\Omega$.

Also ist für alle Blöcke σB der Schnitt $\sigma B \cap \Delta$ höchstens einpunktig. Seien $B_1, \ldots, B_r$ die verschiedenen Bilder von B, also

$$\Omega = \dot{\bigcup_{i=1}^{r}} B_i \implies \Delta = \dot{\bigcup_{i=1}^{r}} B_i \cap \Delta \implies \#\Delta = \sum_{i=1}^{r} \underbrace{\#(B_i \cap \Delta)}_{\leq 1} \leq r \,.$$

Daraus folgt nun

$$\#B\#\Delta \leq \#B \cdot r = \#\Omega < 2\#\Delta \implies \#B < 2\,,$$

also ist B einpunktig, G ist primitiv.

Wie man mehrfache Transitivität rekursiv über die Fixgruppen einzelner Ziffern beschreiben kann, so definiert man die sog. *mehrfach primitiven* Permutationsgruppen rekursiv durch: 10/19.12.

1-fach primitiv bedeutet dasselbe wie primitiv, und für $n \geq 2$ heißt G n-fach primitiv, wenn G transitiv und die Fixgruppe G_a irgendeiner Ziffer a $(n-1)$-fach primitiv ist.

Aus Bemerkung (2.7) entnimmt man die Implikationen

$$(k+1)\text{-fach transitiv} \implies k\text{-fach primitiv} \implies k\text{-fach transitiv.}$$

(2.17) Satz: (Jordan) *Es sei $G \leq S_\Omega$ primitiv und $\Omega = \Omega_1 \dot\cup \Omega_2$ eine Zerlegung von Ω mit $2 \leq \#\Omega_1$ und $1 \leq \#\Omega_2$. Dann gilt:*

a) Ist $\mathrm{Fix}_G(\Omega_2)$ transitiv auf Ω_1, so ist G ist 2-transitiv auf Ω.

b) Ist $\mathrm{Fix}_G(\Omega_2)$ primitiv auf Ω_1, so ist G 2-fach primitiv.

Der *Beweis* erfolgt durch Induktion über $\#\Omega_2$. Im Fall $\#\Omega_2 = 1$ ist aufgrund der rekursiven Beschreibung mehrfacher Transitivität (Prop. (2.2)) bzw. der Definition mehrfacher Primitivität nichts zu zeigen. Sei also nun $\#\Omega_2 \geq 2$.

1. Fall: $\#\Omega_2 < \#\Omega/2$, also $\#\Omega_1 > \#\Omega/2$. Dann folgt

$$\bigwedge_{\sigma\in G} \sigma\Omega_1 \cap \Omega_1 \neq \emptyset\,. \tag{1}$$

Wegen der Transitivität von $\mathrm{Fix}_G(\Omega_2)$ auf Ω_1, und daher der von $\sigma\mathrm{Fix}_G(\Omega_2)\sigma^{-1} = \mathrm{Fix}_G(\sigma\Omega_2)$ auf $\sigma\Omega_1$, folgt aus (1) für alle $\sigma \in G$

$$H := \langle \mathrm{Fix}_G(\Omega_2), \sigma\mathrm{Fix}_G(\Omega_2)\sigma^{-1}\rangle \text{ operiert transitiv auf } \Omega_1' := \Omega_1 \cup \sigma\Omega_1\,. \tag{2}$$

Da andererseits H trivial auf $\Omega_2 \cap \sigma\Omega_2 = \Omega \setminus \Omega_1' =: \Omega_2'$ operiert, also $H \leq \mathrm{Fix}_G(\Omega_2')$ gilt, folgt erst recht

$$\mathrm{Fix}_G(\Omega_2') \text{ operiert transitiv auf } \Omega_1' = \Omega \setminus \Omega_2'\,. \tag{3}$$

Weiter gilt offensichtlich

$$2 \leq \#\Omega_1' \quad \text{und} \quad \#\Omega_2' \leq \#\Omega_2\,. \tag{4}$$

Wir wollen nun $\sigma \in G$ so wählen, dass

$$1 \leq \#\Omega_2' < \#\Omega_2 \tag{5}$$

gilt und die Induktionsvoraussetzung für $\Omega = \Omega_1' \dot\cup \Omega_2'$ angewendet werden kann.

Dazu wenden wir Lemma (2.14) auf $\Delta = \Omega_2$ und zwei verschiedene Elemente $a, b \in \Omega_2$ an. (Es ist $\#\Omega_2 \geq 2$!) Für ein $\sigma \in G$ mit den Eigenschaften aus Lemma (2.14) gilt dann (5), denn $a \in \Omega_2'$ und $b \in \Omega_2 \setminus \Omega_2'$.

Ad a): Gemäß (3) operiert $\mathrm{Fix}_G(\Omega_2')$ transitiv auf Ω_1', so dass gemäß (4) und (5) die Voraussetzungen von (2.17) für die Zerlegung $\Omega = \Omega_1' \dot\cup \Omega_2'$ erfüllt sind. Wegen $\#\Omega_2' < \#\Omega_2$ folgt nach Induktionsvoraussetzung die Behauptung.

Ad b): Hier schließen wir genauso, nachdem wir gezeigt haben:

$$H := \langle \mathrm{Fix}_G(\Omega_2), \sigma\mathrm{Fix}_G(\Omega_2)\sigma^{-1}\rangle \text{ operiert primitiv auf } \Omega_1' := \Omega_1 \cup \sigma\Omega_1\,. \tag{6}$$

Aus der Voraussetzung von b) folgt aber genau dies mit Proposition (2.15) angewendet auf die transitive Permutationsgruppe (siehe (2)) $H|_{\Omega_1'}$.

Wir kommen nun zum *2. Fall:* $\#\Omega \leq 2\#\Omega_2$, also $2\#\Omega_1 \leq \#\Omega$.

Wir wenden nun Lemma (2.14) an auf $\Delta = \Omega_1$ und zwei verschiedene Elemente $a, b \in \Omega_1$. (Hier

wird die Voraussetzung $\#\Omega_1 \geq 2$ von Satz (2.17) benutzt.) Sei also $\sigma \in G$ mit $a \in \sigma\Omega_1$ und $b \notin \sigma\Omega_1$. Dann folgt $a \in \Omega_1 \cap \sigma\Omega_1 \neq \emptyset$, so dass wieder gilt:

$$H := \langle \mathrm{Fix}_G(\Omega_2), \sigma \mathrm{Fix}_G(\Omega_2)\sigma^{-1} \rangle \text{ operiert transitiv auf } \Omega_1' := \Omega_1 \cup \sigma\Omega_1 \,. \tag{7}$$

Aus $\Omega_1 \cap \sigma\Omega_1 \neq \emptyset$ folgt

$$\#\Omega_1' = \#(\Omega_1 \cup \sigma\Omega_1) < 2\#\Omega_1 \leq \#\Omega \implies \Omega' 2 = \Omega \setminus \Omega_1' \neq \emptyset. \tag{8}$$

Wegen $b \in \Omega_1$ und $b \notin \sigma\Omega_1$ gilt $\sigma\Omega_1 \subsetneq \Omega_1'$, also $\#\Omega_1 = \#\sigma\Omega_1 < \#\Omega_1'$ bzw. $\#\Omega_2 > \#\Omega_2'$. Zusammen mit (8) also

$$1 \leq \#\Omega_2' < \#\Omega_2 \,, \tag{9}$$

so dass man wie im ersten Fall weiterschließt.

(2.18) Satz: (Jordan) *Sei G eine primitive Permutationsgruppe auf Ω und Ω_1 eine Teilmenge mit $1 < \#\Omega_1 =: m < n := \#\Omega$. Operiert nun $\mathrm{Fix}_G(\Omega \setminus \Omega_1)$ primitiv auf Ω_1, so operiert G sogar $(n-m+1)$-fach primitiv auf Ω.*

Beweis: Wir schließen induktiv über $\#(\Omega \setminus \Omega_1) = n - m$.
Nach (2.17), b) folgt aus den Voraussetzungen in jedem Falle: G ist 2-fach primitiv. Für $n-m = 1$ ist daher nichts mehr zu zeigen.
Sei nun $n - m \geq 2$ und $a \in \Omega_2 := \Omega \setminus \Omega_1$. Wie schon erwähnt operiert G_a primitiv auf $\Omega' = \Omega \setminus \{a\}$. Außerdem operiert die Untergruppe $\mathrm{Fix}_G(\Omega_2)$ von G_a primitiv auf $\Omega_1 \subset \Omega'$. Wegen $\#\Omega' - \#\Omega_1 = n - 1 - m < n - m$ folgt aus der Induktionsvoraussetzung, dass G_a $(n-1)-m+1 = (n-m)$-fach primitiv auf Ω', also G $(n-m+1)$-fach primitiv auf Ω operiert.

(2.19) Korollar: *G operiere primitiv auf n Objekten und enthalte einen p-Zyklus für eine Primzahl p. Dann ist G $(n-p+1)$-fach primitiv.*
Speziell: Ist $p = 2$, so ist G die volle symmetrische Gruppe: $G = S_n$.
Ist $p = 3$, so umfasst G die alternierende Gruppe: $G \supseteq A_n$.

Beweis: Sei $\sigma \in G$ ein p-Zyklus und Ω_1 seine Bahn, also $\#\Omega_1 = p$. σ operiert transitiv, nach (2.11) also primitiv auf Ω_1. Wegen $\sigma\,|_{\Omega\setminus\Omega_1} = \mathrm{id}$, also $\sigma \in \mathrm{Fix}_G(\Omega \setminus \Omega_1)$ sind die Voraussetzungen von (2.18) erfüllt, und die Behauptung folgt.

Der erste Zusatz ist ebenfalls klar, denn für $p = 2$ ist G $(n-1)$-fach transitiv. Bei Operation auf n Objekten muss G dann aber n-fach transitiv und damit S_n sein. Sei nun $p = 3$, also G $(n-2)$-fach transitiv auf n Elementen und folglich $n!/2$ ein Teiler von $\#G$ (Proposition (2.2)). Ist $n \geq 5$, so ist G 3-fach transitiv, so dass mit dem 3-Zyklus σ *sämtliche* 3-Zyklen in G liegen. Da diese die alternierende Gruppe A_n erzeugen, ist die Behauptung gezeigt. Es bleibt nun nur noch der Fall $n = 4$ zu untersuchen. Wäre $A_4 \not\subset G$, also $N := G \cap A_4 \subsetneq A_4$, so hätte N die Ordnung 6 und wäre Normalteiler in S_4 (denn wegen $(S_4 : G) \leq 2$ gilt $G \lhd S_4$). Wir betrachten nun eine 3-Sylowuntergruppe U_3 von N. Wegen $(N : U) = 2$ ist U Normalteiler von N, also die einzige 3-Sylowgruppe von N (Sylowsätze). Dann muss U aber auch Normalteiler von S_4 sein, denn: Ist $\sigma \in S_4$, dann ist die Konjugation $(\ldots)^\sigma$ ein Automorphismus von N, bildet die 3-Sylowuntergruppe U auf eine Untergruppe der Ordnung 3 von N ab, U^σ wäre also ebenfalls 3-Sylowgruppe von N und damit gleich U: $U^\sigma = U$. Dies kann aber nicht sein, da S_4 mehrere 3-Sylowgruppen enthält. Die Annahme $A_4 \not\subset G$ ist also zum Widerspruch geführt. 11/9.1.

Wir folgern nun aus diesem Resultat von Jordan den folgenden interessanten

(2.20) Satz: (Bochert) *Ist $G \leq S_n$ eine primitive Permutationsgruppe und der Index $(S_n : G) < [(n+1)/2]!$, so umfasst G bereits die alternierende Gruppe A_n.*

Beweis: Wir wählen $\Delta \subset \Omega = \{1, \ldots, n\}$ mit der Eigenschaft

$$S(\Delta) \cap G = \{1\} \,. \tag{1}$$

Ein solches Δ gibt es (etwa Δ einpunktig), und wir wählen Δ nun so, dass $k = \#\Delta$ *maximal* ist mit dieser Eigenschaft (1). Aufgrund der Voraussetzung muss gelten

$$\#\Delta = k < \frac{n}{2} \,, \tag{2}$$

denn aus (1) folgt

$$(S_n : G) \geq \#S(\Delta) = k!\,,$$

so dass nach Voraussetzung $[(n+1)/2]! > k!$ gilt. Dies bedeutet aber gerade $k < n/2$.

Aus (2) folgt nun $\#(\Omega \setminus \Delta) > \frac{n}{2} > \#\Delta = k$, so dass man gemäß der Wahl von k ein

$$\sigma \in S(\Omega \setminus \Delta) \cap G\,,\ \sigma \neq 1$$

wählen kann. Also existiert eine Ziffer i mit

$$i \notin \Delta \text{ und } \sigma i \neq i\,. \tag{3}$$

Wir setzen nun $\Delta' = \Delta \cup \{i\}$. Wieder folgt aus $\#\Delta' = k+1 > k$ die Existenz eines

$$\tau \in S(\Delta') \cap G\,,\ \tau \neq 1\,.$$

Wäre $\tau i = i$, so folgte $\tau \in S(\Delta) \cap G$, was (1) widerspricht. Also folgt auch $\tau i \neq i$. Da σ ganz Δ, τ hingegen das Komplement von $\Delta' = \Delta \cup \{i\}$ elementweise festlässt, ist i die *einzige* Ziffer mit

$$\sigma i \neq i \neq \tau i\,. \tag{4}$$

Wir wollen nun zeigen, dass die primitive Gruppe G einen 2- oder 3-Zyklus enthält, und zwar den Kommutator $\gamma := \sigma\tau\sigma^{-1}\tau^{-1} \in G$. Dazu definieren wir zunächst j, k durch

$$\sigma j = i = \tau k\,.$$

Wir behaupten nun, dass der Träger von γ in $\{i, j, k\}$ liegt, oder äquivalent formuliert:

$$\sigma\tau l = \tau\sigma l \quad \text{für alle } l \notin \{i, j, k\}\,. \tag{5}$$

Begründung: Da $l \neq i$ ist und nur i die Eigenschaft (4) hat, muss $\sigma l = l$ oder $\tau l = l$ sein. Wegen der Symmetrie der Behauptung (5) kann man o. E. annehmen $\sigma l = l$. Ist nun auch $\tau l = l$, so ist (5) natürlich erfüllt. Wenn jedoch $\tau l \neq l$ ist, also $\tau(\tau l) \neq \tau l$, so folgern wir daraus wegen $\tau l \neq \tau k = i$, dass $\sigma(\tau l) = \tau l$ gelten muss (Einzigkeit von i mit (4)). Damit ist dann aber wiederum (5) erfüllt.

Wir zeigen nun, dass dieser Kommutator γ nicht-trivial, wegen $\mathrm{Tr}(\gamma) \subset \{i, j, k\}$ also ein 2- oder 3-Zyklus ist. Dazu beweisen wir

$$\sigma\tau i \neq \tau\sigma i\,. \tag{6}$$

Zum Beweis von (6) gehen wir aus von $\sigma i \neq i$, also $\sigma(\sigma i) \neq \sigma i$. Wieder folgt wegen der Eindeutigkeit von i mit (4), dass $\tau\sigma i = \sigma i$ ist. Genauso folgert man $\sigma\tau i = \tau i$. Wäre nun aber $\sigma i = \tau i$, so folgte aus $\sigma(\sigma i) \neq \sigma i = \tau i \neq \tau(\tau i)$ wegen der Eindeutigkeit von i:

$$\sigma i = \tau i = i$$

im Widerspruch zu (4).

Mit diesem Widerspruch ist gezeigt, dass $\gamma \in G$ ein 2- oder 3-Zyklus ist, die primitive Gruppe G also A_n umfassen muss (nach (2.19)). Damit ist der Satz von Bochert vollständig bewiesen.

d. Abschließende Bemerkungen ohne Beweise. Aufgrund der Klassifikation der endlichen einfachen Gruppen sind auch die 2-transitiven Gruppen klassifiziert (siehe P. J. Cameron: Finite permutation groups and finite simple groups. Bull. London Math. Soc. **13** (1981) 1–22). Die umfangreiche Liste ist nicht ganz einfach anzugeben. Einprägsamer ist die folgende Konsequenz (siehe dazu auch den Übersichtsartikel C. E. Praeger: Finite primitive permutation groups: A survey. in: Proc. Int. Conf. Group Theory (Canberra 1989)):

Satz: *Die einzigen mindestens 4-fach transitiven Gruppen vom Grade n, die nicht die alternierende Gruppe A_n umfassen, sind die folgenden vier Mathieugruppen:*
M_{24}: 5-fach transitiv vom Grad 24; Ordnung $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 244823040$,
M_{12}: scharf 5-fach transitiv vom Grad 12; Ordnung $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$,
und darin die jeweiligen Fixgruppen einer Ziffer:
M_{23}: 4-fach transitiv vom Grad 23; Ordnung $23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 10200960$,
M_{11}: scharf 4-fach transitiv vom Grad 11; Ordnung $11 \cdot 10 \cdot 9 \cdot 8 = 7920$.
Insbesondere ist eine mindestens 6-fach transitive Permutationsgruppe die alternierende oder symmetrische Gruppe.

Neben den erwähnten 4 Mathieugruppen gibt es noch die 3-transitive Mathieugruppe M_{22}, Fixgruppe einer Ziffer in der M_{23}. Die 5 Mathieugruppen wurden 1861 von E. Mathieu entdeckt. Sie sind einfache nicht-abelsche Gruppen, die in keine der üblichen Serien passen. Eine mögliche Beschreibung der M_{24} ist die folgende (E. Witt: Die 5-fach transitiven Gruppen von Mathieu. Abh. Math. Sem. Hamb. Univ. **12** (1938) 256–264 und E. Witt: Über Steinersche Systeme. Abh. Math. Sem. Hamb. Univ. **12** (1938) 265–275):

Ein Steiner-System $S(5, 8, 24)$ ist ein System von 8-elementigen Teilmengen einer 24-elementigen Menge (etwa von $\underline{24} = \{1, \ldots, 24\}$), derart dass jede 5-elementige Menge M in genau einer Menge $S \in \mathcal{S}(5, 8, 24)$ enthalten ist:

$$\mathcal{S}(5,8,24) \subset \binom{\underline{24}}{8} \text{ und } \bigwedge_{M \subset \underline{24}, \# M = 5} \dot{\bigvee}_{S \in \mathcal{S}(5,8,24)} M \subset S\,.$$

Witt zeigte, dass es im wesentlichen nur ein solches Steinersystem $\mathcal{S}(5, 8, 24)$ gibt und dass die Untergruppe der symmetrischen Gruppe S_{24}, die ein solches Steinersystem in sich überführt, gerade die Mathieugruppe M_{24} ist: Die M_{24} ist 'Automorphismengruppe' des Steinersystems $\mathcal{S}(5, 8, 24)$. Analog kann man die M_{12} als Automorphismengruppe des einzigen Steinersystems $\mathcal{S}(5, 6, 12)$ beschreiben.

Solche Steinersysteme sind komplizierte kombinatorische Objekte. Ihre Existenz ist eng mit höher-transitiven Gruppen verknüpft: Wir gehen aus von einer l-transitiven Permutationsgruppe $G \subset S_n$ und der Fixgruppe $H = G_{1,\ldots,l}$ von l Ziffern. Ist nun $U \subset H$ eine Untergruppe, die $m > l$ Punkte fixiert und zu der keine andere Untergruppe von H isomorph ist, so bilden die G-Konjugierten der Fixmenge M von U ein Steinersystem $\mathcal{S}(l, m, n)$, welches von G stabilisiert wird.

Witt konstruiert die M_{24} (und damit dann das Steinersystem $\mathcal{S}(5, 8, 24)$) als geeignete 5-transitive Erweiterung der Gruppe $\mathrm{PSL}_3(4) = \mathrm{PSL}_3(\mathbb{F}_4)$, die 2-transitiv auf den 21 Punkten der projektiven Ebene $\mathbb{P}^2(\mathbb{F}_4) = \mathbb{F}_4^3 \setminus \{0\}/\mathbb{F}_4^\times$ operiert.

§3 Bestimmung von Galoisgruppen

In diesem Abschnitt sollen die Begriffsbildungen und Resultate der Permutationsgruppen angewendet werden, um Galoisgruppen zu bestimmen.

a. Die Galoisgruppe eines Polynoms.

(3.1) Definition: Sei k ein Körper, $f \in k[X]$ ein Polynom vom Grade n und $\tilde{k}$ die algebraisch abgeschlossene Hülle von k. Wir bezeichnen mit W_f die Menge aller Wurzeln von f in $\tilde{k}$. Wir setzen voraus, dass das Polynom separabel ist, d. h. die Zahl der verschiedenen Wurzeln in $\tilde{k}$ ist gleich dem Grad n des Polynoms. Es sei $W_f = \{\alpha_1, \ldots, \alpha_n\}$ eine feste Abzählung der Wurzeln von f.
a) Eine *k-Relation* von f ist ein Polynom $r \in k[T_1, \ldots, T_n]$ in n Unbestimmten mit $r(\alpha_1, \ldots, \alpha_n) = 0$.
b) Die *Galoisgruppe* $G_k(f)$ des (separablen) Polynoms f über dem Grundkörper k ist die Gruppe (!) aller Permutationen $\sigma \in S_{W_f}$ der Wurzeln von f, die die k-Relationen von f respektieren:

$$\sigma \in G_k(f) \iff \bigwedge_{r \in k[T_1,\ldots,T_n]} \big(r(\alpha_1, \ldots, \alpha_n) = 0 \implies r(\alpha_{\sigma 1}, \ldots, \alpha_{\sigma n}) = 0\big)\,.$$

Anmerkungen: 1) $G_k(f)$ ist multiplikativ abgeschlossene Teilmenge in der symmetrischen Gruppe S_{W_f} und somit selbst eine Gruppe (Endlichkeit von S_{W_f}!).
2) Daher gilt für $\sigma \in G_k(f)$ und alle $r \in k[T_1, \ldots, T_n]$ die *Äquivalenz*

$$r(\alpha_1, \ldots, \alpha_n) = 0 \iff r(\alpha_{\sigma 1}, \ldots, \alpha_{\sigma n}) = 0\,.$$

3) Der Relationenbegriff setzt eine *feste* Abzählung von W_f voraus. Die Definition von $G_k(f) \subset S_{W_f}$ ist von der gewählten Abzählung von W_f unabhängig.
4) Die Galoisgruppe misst die Abhängigkeiten zwischen den Wurzeln von f: Je mehr Relationen zwischen den Wurzeln bestehen, desto kleiner ist $G(f)$.
5) Die Galoisgruppe wird relativ zum vorgegebenen Grundkörper gebildet und ist von diesem abhängig.

Wir wollen nun diese (historisch ältere) Definition der Galoisgruppe mit der üblichen körpertheoretischen in Verbindung bringen. Es gilt der 12/16.1.

(3.2) Satz: Sei k ein Körper, $f \in k[X]$ ein separables Polynom vom Grad n. Es sei $N_f = k(W_f)$ der Zerfällungskörper von f über k. Dann ist die Restriktionsabbildung

$$G(N_f|k) \xrightarrow{\sim} G_k(f)\,, \quad \sigma \mapsto \sigma\,|_{W_f}$$

ein Gruppenisomorphismus.

Beweis: $N_f|k$ ist galoissch, da N_f Zerfällungskörper (also normal) eines separablen Polynoms (also separabel algebraisch) ist.

Für $\sigma \in G(N_f|k)$ gilt $f(\sigma a) = \sigma f(a)$, da σ den Körper k und damit die Koeffizienten von f festlässt. Ist also a eine Wurzel von f: $f(a) = 0$, so folgt $f(\sigma a) = 0$, also $\sigma W_f \subseteq W_f$. Da W_f endlich und σ injektiv ist, liegt $\sigma' = \sigma\,|_{W_f}$ in S_{W_f}. Da σ ein k-Monomorphismus ist, werden die k-Relalionen zwischen den Wurzeln von f respektiert und $\sigma' \in G_k(f)$. Damit ist die obige Abbildung wohldefiniert.

Da ein k-Automorphismus σ, der die Wurzeln von f festlässt, bereits auf ganz $N_f = k(W_f)$ die Identität ist, ist die in (3.2) gegebene Abbildung injektiv.

Zum Beweis der Surjektivität fixieren wir eine Abzählung $\alpha_1, \ldots, \alpha_n$ von W_f und geben eine Permutation $\rho \in S_n$ vor mit

$$r(\alpha_1, \ldots, \alpha_n) = 0 \iff r(\alpha_{\rho 1}, \ldots, \alpha_{\rho n}) \quad (r \in k[T_1, \ldots, T_n])\,.$$

Zu zeigen: ρ ist die Einschränkung eines k-Automorphismus σ von N_f auf W_f. Da die α_i algebraisch über k sind, gilt

$$N_f = k(W_f) = k(\alpha_1, \ldots, \alpha_n) = k[\alpha_1, \ldots, \alpha_n] \,.$$

Damit ist N_f epimorphes Bild des Polynomrings $k[T_1, \ldots, T_n]$ unter dem Einsetzungshomomorphismus $E_{\underline{\alpha}}$:

$$E_{\underline{\alpha}} : k[T_1, \ldots, T_n] \twoheadrightarrow k[\alpha_1, \ldots, \alpha_n] = N_f \,, \quad r = r(T_1, \ldots, T_n) \mapsto r(\alpha_1, \ldots, \alpha_n) \,.$$

Der Kern dieses Einsetzungshomomorphismus $\mathrm{Ke}\,(E_\alpha)$ besteht genau aus den k-Relationen zwischen den Wurzeln von f (Definition (3.1) a)).

Jede Permutation $\rho \in S_n$ bestimmt eine Permutation der Unbestimmten T_i und dadurch einen k-Automorphismus $\hat{\rho}$ des Polynomrings $k[T_1, \ldots, T_n]$: $\hat{\rho}(r) = r(T_{\rho 1}, \ldots, T_{\rho_n})$. Die Permutationen $\rho \in G(f)$, $\alpha_i \mapsto \alpha_{\rho i}$ sind dann genau die $\rho \in S_n$, deren zugehöriges $\hat{\rho}$ den Kern $\mathrm{Ke}\,(E_{\underline{\alpha}})$ auf sich abbilden und daher einen Automorphismus $\sigma = \bar{\hat{\rho}}$ von

$$k[T_1, \ldots, T_n]/\mathrm{Ke}\,(E_{\underline{\alpha}}) \;\simeq_k\; k[\alpha_1, \ldots, \alpha_n] = N_f$$

induzieren mit

$$\bar{\hat{\rho}}(\alpha_i) = \overline{\hat{\rho}(T_i)} = \bar{T}_{\rho i} = \alpha_{\rho i} = \rho\alpha i \,.$$

Das bedeutet:

$$\rho \in G(f) \implies \bigvee_{\sigma \in G(N_f|k)} \sigma\,|_{W_f} = \rho \,.$$

Damit ist auch die Surjektivität von (3.2) bewiesen. □

Anmerkungen: 1) Die Galoisgruppe $G(f)$ besteht also aus all den Permutationen der Wurzeln von f, die sich zu k-Automorphismen des Zerfällungskörpers $k(W_f)$ fortsetzen lassen.
2) Als abstrakte Gruppe ist also die Galoisgruppe G(f) des – separablen – Polynoms f nichts anderes als die Galoisgruppe des Zerfällungskörpers.
3) Die Galoisgruppe $G(f)$ trägt aber zusätzlich noch die Struktur einer Permutationsgruppe: $G(f)$ operiert in natürlicher Weise auf der Wurzelmenge W_f von f. Dadurch erhält man weitere strukturelle Ansätze zur Bestimmung von $G(f) \simeq G(N_f|k)$.

(3.3) Proposition: *Sei k ein Körper, $f \in k[X]$ ein separables Polynom, W_f seine Wurzelmenge und $G(f) \subset S_{W_f}$ die Galoisgruppe von f über k. Dann gilt:*

$$G(f) \textit{ operiert transitiv auf } W_f \iff f \textit{ ist irreduzibel über } k \,.$$

Beweis: $\underline{\Leftarrow}$: Seien $\alpha, \beta \in W_f$ zwei beliebige Wurzeln von f; gesucht ist ein $\sigma \in G(f)$ mit $\sigma\alpha = \beta$.

Nach Satz (3.2) besteht $G(f)$ aus allen Restriktionen von Automorphismen in $G(k(W_f)|k)$, der Galoisgruppe des Zerfällungskörpers $N_f = k(W_f)$ von f über k. Da f irreduzibel ist, haben wir folgende Isomorphien

$$k(\alpha) = k[\alpha] \simeq k[X]/fk[X] \simeq k[\beta] = k(\beta) \,,$$

wobei die beiden Isomorphismen durch Einsetzungshomomorphismen gegeben sind: $X \mapsto \alpha$ bzw. $X \mapsto \beta$. Man erhält also einen k-Isomorphismus der *Stammkörper* $\sigma : k[\alpha] \xrightarrow{\sim} k[\beta]$ mit $\sigma\alpha = \beta$.

Da N_f normal ist über k, lässt sich dieser k-Isomorphismus zu einem Automorphismus von $N_f|k$ fortsetzen. Dieser hat dann die gewünschte Eigenschaft.

$\underline{\Rightarrow}$: Sei $f = f_1 \cdot \ldots \cdot f_r$ die Primzerlegung von f über k. Dann gilt (wegen der Separabilität von f)

$$W_f = \dot{\bigcup_i} W_{f_i} \,.$$

Jedes $\sigma \in G(f) \simeq G(N_f|k)$ fixiert k, also die Koeffizienten der f_i, so dass α und $\sigma\alpha$ Wurzeln desselben Polynoms f_i sein müssen. Also gilt $\sigma W_{f_i} = W_{f_i}$ und σ ist nicht transitiv auf W_f (falls $r \geq 2$, d. h. f *nicht* irreduzibel ist). □

Der Beweis zeigt, dass die Wurzelmengen W_{f_i} der irreduziblen Teiler von f gerade die Bahnen von $G(f)$ bilden.

(3.4) Proposition: *Sei k ein Körper und $f \in k[X]$ ein irreduziebles Polynom vom Grad p, p eine Primzahl. Ist $k \subseteq \mathbb{R}$ ein reeller Körper (etwa $k = \mathbb{Q}$) und hat f genau 2 nicht-reelle Wurzeln, so ist die Galoisgruppe von f die volle symmetrische Gruppe S_p.*

Beweis: Da f irreduzibel ist, ist $G(f)$ eine transitive Untergruppe von S_p (siehe (3.3)). Da p eine Primzahl ist, ist $G(f)$ primitiv (vgl. (2.11)). Wir zeigen nun, dass $G(f)$ eine Transposition enthält und daher gemäß (2.19) $G(f) = S_p$ folgt.

Da f reelle Koeffizienten hat, sind die beiden nicht-reellen Wurzeln von f konjugiert komplex und werden von der komplexen Konjugation vertauscht, während die übrigen reellen Wurzeln unter c festbleiben. Damit ist $c\,|_{W_f}$ eine Transposition in $G(f)$. □

(3.5) Beispiel: Das Polynom $f(X) = 2X^5 - 5X^4 + 5 \in \mathbb{Q}[X]$ hat die Galoisgruppe S_5, ist also insbesondere nicht durch Radikale auflösbar.

Beweis: Das Polynom ist ein Eisenstein-Polynom zur Primzahl 5 (d. h. $5 \mid a_0, \ldots, a_{n-1}$, $5 \nmid a_n$ und $5^2 \nmid a_0$) und ist daher irreduzibel, die Galoisgruppe also transitiv. Die Polynomfunktion $f : \mathbb{R} \to \mathbb{R}$ hat die Ableitung $f'(x) = 10x^4 - 20x^3 = 10x^3(x-2)$ und damit nur zwei Extremstellen 0 und 2. Dabei liegt bei 0 ein Maximum und bei 2 ein Minimum vor. Aus $f(0) = 4$ und $f(2) = -11$ folgt dann, dass f genau drei verschiedene reelle Wurzeln besitzt. Im algebraischen Abschluss hat f dann noch zwei konjugiert komplexe Wurzeln, insgesamt ist also f separabel (dies folgt auch direkt aus der Irreduzibilität und $\operatorname{char} k = 0$, s.u.) und die Voraussetzungen von (3.4) sind erfüllt. □ 13/23.1.

b. Die Diskriminante.

(3.6) Definition: Sei k ein Körper, $f \in k[X]$ ein normiertes Polynom vom Grade n und $\alpha_1, \ldots, \alpha_n$ sämtliche Wurzeln von f im algebraischen Abschluss $\tilde{k}$ von k (mit Vielfachheiten gezählt). Dann definiert man die Diskriminante von f als

$$D(f) := \prod_{i<j} (\alpha_i - \alpha_j)^2 .$$

Bei dieser Definition ist klar:

$$D(f) \neq 0 \iff f \text{ separabel} .$$

Für separables f folgt aus der Galoistheorie:

$$D(f) \in k ,$$

denn für alle Körperautomorphismen σ, die die Koeffizienten von f festlassen, gilt $W_f^\sigma = W_f$, also $D(f)^\sigma = D(f)$.

Die Kenntnis der Diskriminante gibt weitere Informationen über die Galoisgruppe:

(3.7) Proposition: *Sei $f \in k[X]$ ein separables Polynom vom Grade n über einem Körper k und $D(f) \neq 0$ die Diskriminante. Dann gilt:*

$$D(f) \in (k^\times)^2 \iff G(f) \subset A_n .$$

Beweis: Es ist

$$\sqrt{D(f)} = \prod_{i<j} (\alpha_i - \alpha_j) ,$$

also für $\sigma \in G(f) \subset S_n$

$$\sigma\sqrt{D(f)} = \prod_{i<j} \frac{\sigma(\alpha_i) - \sigma(\alpha_j)}{\alpha_i - \alpha_j} \cdot \prod_{i<j} (\alpha_i - \alpha_j) = sign(\sigma) \cdot \sqrt{D(f)} .$$

Aus dieser Äquivalenz folgt dann mittels Galoistheorie (N_f sei der Zerfällungskörper von f):

$$D(f) \in (k^\times)^2 \iff \sqrt{D(f)} \in k \iff \bigwedge_{\sigma \in G(N_f|k)} \sigma(\sqrt{D(f)}) = \sqrt{D(f)}$$
$$\iff \bigwedge_{\sigma \in G(f)} sign(\sigma) = 1 \iff G(f) \subseteq A_n\,.$$

Diese Proposition ist natürlich nur dann sinnvoll anwendbar, wenn man die Diskriminante berechnen kann. Bei der gegebenen Definition benötigt man dazu die Wurzeln; man kann jedoch die Diskriminante unmittelbar aus den Koeffizienten des Polynoms berechnen. Eine Möglichkeit, dies zu zeigen, ist die Beziehung zur *Resultante* von zwei Polynomen. (Ein anderer Weg benutzt den Hauptsatz für symmetrische Polynome.)

(3.8) Definition: Für zwei Polynome $f = \sum_{i=0}^m a_i X^i$ $(a_m \neq 0)$ und $g = \sum_{i=0}^n b_i X^i$ $(b_n \neq 0)$ ist die Resultante $R(f,g)$ definiert als die Determinante der $n+m$-reihigen Matrix

$$\mathcal{R}(f,g) = \begin{pmatrix} a_0 & a_1 & \cdots & & a_m & & & \\ & a_0 & & & & a_m & & \\ & & \ddots & & & & \ddots & \\ & & & a_0 & & \cdots & & a_m \\ b_0 & b_1 & & \cdots & & b_n & & \\ & \ddots & & & & & \ddots & \\ & & b_0 & & \cdots & & & b_n \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{matrix}$$

Die Bedeutung der Resultante liegt in der folgenden

(3.9) Proposition: *Für Polynome f, g über einem faktoriellen (=ZPE-) Ring R sind die folgenden Aussagen äquivalent:*
(1) f und g haben einen gemeinsamen Faktor positiven Grades.
(2) $af + bg = 0$ für geeignete $a, b \in R[X] \setminus \{0\}$ mit $\deg a < \deg g$, $\deg b < \deg f$.
(3) $R(f,g) = 0$.

Die Bedingungen an a, b in (2) sind offenbar wichtig, da ohne sie (2) trivial erfüllt werden kann: $0f + 0g = 0$ und $(-g)f + fg = 0$. Aus der letzten Beziehung erkennt man auch schon die Implikation (1) $\Rightarrow$ (2): Ist u ein gemeinsamer Faktor von f und g mit $\deg u \geq 1$, so folgt

$$(-\frac{g}{u}) \cdot f + (\frac{f}{u}) \cdot g = 0\,,$$

wobei $a = -g/u$ und $b = f/u$ die Eigenschaften von (2) erfüllen.

(2) $\Rightarrow$ (1): Sei $af = -bg$ wie in (2) und $f = f_1 \cdot \ldots \cdot f_r$ die Primzerlegung von f (mit R ist auch $R[X]$ faktoriell, Satz von Gauß). Wäre (1) falsch, so gälte $f_i \not| g$ für alle i. Aus $f_1 \mid af = -bg$ folgte dann (wegen der eindeutigen Primzerlegung in $R[X]$): $f_1 \mid b$, also

$$a \cdot f_2 \cdot \ldots \cdot f_r = -\frac{b}{f_1} \cdot g\,.$$

Man schließt induktiv weiter und erhält schließlich $f \mid b$. Wegen $b \neq 0$ folgt daraus der Widerspruch $\deg f \leq \deg b$.

Ist $c = af + bg$ und a, b Polynome vom Grad $< n := \deg g$ bzw. $< m := \deg f$, so gilt für die Koeffizienten γ_k von c, α_i von a und β_j von b:

$$(\gamma_0, \ldots, \gamma_{n+m-1}) = (\alpha_0, \ldots, \alpha_{n-1}; \beta_0, \ldots, \beta_{m-1}) \cdot \mathcal{R}(f,g) \qquad (*)$$

mit der Resultantenmatrix $\mathcal{R}(f,g)$. Damit folgt die Äquivalenz von (2) und (3), denn (2) besagt: Das quadratische homogene lineare Gleichungssystem $(*)$ hat eine nicht-triviale Lösung (über R bzw. über dessen Quotientenkörper K).

Eine Beschreibung der Resultante durch die Wurzeln der Polynome erhält man aus der folgenden

(3.10) Proposition: *Seien $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$ Polynome über irgendeinem kommutativen Ring und $X - \xi$ ein Linearfaktor. Dann gilt:*

$$R(f\,,\,(X-\xi)g) = f(\xi)\cdot R(f,g)\,.$$

Beweis: Wegen

$$(X-\xi)\cdot g = -\xi b_0 + \sum_{j=1}^{n}(b_{j-1}-\xi b_j)X^j + b_n X^{n+1}$$

ist die linke Seite der Behauptung die Determinante der folgenden $(n+m+1)$-reihigen Matrix (der obere 'a'-Block umfasst $n+1$ Zeilen):

$$\begin{pmatrix}
a_0 & & \cdots & & a_{m-1} & a_m & & \\
& \ddots & & & & & \ddots & \\
& & a_0 & & \cdots & & a_{m-1} & a_m \\
-\xi b_0 & b_0-\xi b_1 & \cdots & b_{n-1}-\xi b_n & b_n & & & \\
& -\xi b_0 & & \cdots & b_{n-1}-\xi b_n & b_n & & \\
& & \ddots & & & & \ddots & \\
& & & -\xi b_0 & \cdots & & & b_n
\end{pmatrix}$$

Addiert man, bei der letzten Spalte beginnend, sukzessive das ξ-fache einer Spalte zur vorangehenden, so ergibt sich die folgende Matrix:

$$\begin{pmatrix}
f_0(\xi) & f_1(\xi) & \cdots & f_{m-1}(\xi) & a_m & & & \\
& f_0(\xi) & f_1(\xi) & \cdots & f_{m-1}(\xi) & a_m & & \\
& & \ddots & & & & \ddots & \\
& & & f_0(\xi) & f_1(\xi) & \cdots & f_{m-1}(\xi) & a_m \\
0 & b_0 & & \cdots & b_{n-1} & b_n & & \\
& \ddots & & & & & \ddots & \\
& & 0 & b_0 & \cdots & & b_{n-1} & b_n
\end{pmatrix}$$

mit $f_m(\xi) = a_m$ und $f_i(\xi) = a_i + f_{i+1}(\xi)\cdot\xi$, also $f_i(\xi) = \sum_{j=i}^{m} a_j \xi^{j-i}$ und daher $f_0(\xi) = f(\xi)$.

Entwicklung nach der ersten Spalte ergibt $R(f,(X-\xi)g) = f(\xi)\det M$ mit der folgenden $(m+n)$-reihigen Matrix

$$M = \begin{pmatrix}
f_0(\xi) & & \cdots & f_{m-1}(\xi) & a_m & & \\
& \ddots & & & & \ddots & \\
& & f_0(\xi) & \cdots & & f_{m-1}(\xi) & a_m \\
b_0 & & \cdots & b_{n-1} & b_n & & \\
& \ddots & & & & \ddots & \\
& & b_0 & \cdots & & b_{n-1} & b_n
\end{pmatrix}$$

Subtrahiert man, mit der letzten Zeile des oberen Blockes beginnend, sukzessive von jeder Zeile das ξ-fache der vorangehenden, so erhält man wegen $f_i(\xi) = f_{i+1}(\xi)\cdot\xi + a_i$

$$\det M = \det \begin{pmatrix}
a_0 & a_1 & \cdots & a_m & & \\
& a_0 & & & a_m & \\
& & \ddots & & & \ddots \\
& & & a_0 & \cdots & a_m \\
b_0 & b_1 & & \cdots & b_n & \\
& \ddots & & & & \ddots \\
& & b_0 & & \cdots & b_n
\end{pmatrix} = R(f,g)\,.$$

Insgesamt folgt die Behauptung $R(f,(X-\xi)g) = f(\xi)\cdot \det M = f(\xi)\cdot R(f,g)$ von (3.10).

(3.11) Folgerungen: *Seien $f = a_m \prod_{i=1}^m (X-\eta_i)$ und $g = b_n \prod_{j=1}^n (X-\xi_j)$ beliebige Polynome vom Grade m bzw. n.*
a) Dann berechnet sich die Resultante aus den Wurzeln der Polynome gemäß

$$R(f,g) = b_n^m \prod_{j=1}^n f(\xi_j) = a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (\xi_j - \eta_i) = (-1)^{mn} a_m^n \prod_{i=1}^m g(\eta_i)\,.$$

b) Die Diskriminante eines normierten Polynoms f ($a_m = 1$) berechnet sich als Resultante

$$D(f) = (-1)^{m(m-1)/2} R(f,f')$$

Die Diskriminante $D(f)$ ist unmittelbar aus den Koeffizienten berechenbar:
$D(f) = D_m(a_0,\ldots,a_{m-1})$. Dabei ist D_m ein universelles, nur vom Grad m abhängiges Polynom mit Koeffizienten in $\mathbb{Z}$.

Beweis: Teil a) ist eine einfache sukzessive Anwendung von (3.10) unter Beachtung der Beziehung

$$R(f,b_n) = b_n^m\,.$$

Für b) beachte man

$$f'(X) = \sum_{j=1}^m \prod_{\substack{k=1\\k\neq j}}^m (X-\eta_k)\,,\ \text{also } f'(\eta_i) = \prod_{\substack{k=1\\k\neq i}}^m (\eta_i - \eta_k)\,,$$

also nach (3.10)

$$\begin{aligned} R(f,f') &= (-1)^{m(m-1)} \prod_{i=1}^m f'(\eta_i) = \prod_{k\neq i} (\eta_i - \eta_k) \\ &= (-1)^{m(m-1)/2} \prod_{i<k} (\eta_i - \eta_k)^2 = (-1)^{m(m-1)/2} D(f)\,. \end{aligned}$$

Als Determinante einer Matrix, die nur die Koeffizienten von f (und die beim Ableiten auftretenden natürlichen Zahlen) enthält, ist die Diskriminante $D(f)$ ein universelles ganzzahliges Polynom in den Koeffizienten von f.

c. Galoisgruppen über $\mathbb{Q}$. Bei der Untersuchung der Galoisgruppe von Polynomen über $\mathbb{Q}$ kann man sich natürlich auf Polynome mit Koeffizienten aus $\mathbb{Z}$ beschränken. Geht man nun von einem ganzzahligen Polynom $f = \sum_{i=0}^n a_i X^i$ aus und multipliziert mit a_n^{n-1}, so erhält man

$$a_n^{n-1} f = \sum_{i=0}^{n-1} a_i a_n^{n-i-1} (a_n X)^i + (a_n X)^n = g(a_n X)$$

mit einem *normierten* ganzzahligen Polynom $g \in \mathbb{Z}[X]$. Da sich die Wurzeln von f und von g nur um den ganzzahligen Faktor a_n unterschieden, haben beide Polynome dieselbe Galoisgruppe. Man kann sich also auf die Bestimmung der Galoisgruppe von *normierten ganzzahligen* Polynomen beschränken.

Das entscheidende Hilfsmittel dabei ist der sogenannte Reduktionssatz, der eine Beziehung herstellt zwischen der Galoisgruppe eines normierten Polynoms $f \in \mathbb{Z}[X]$ und seiner Restklassenpolynome $\bar f = f \bmod p \in \mathbb{F}_p[X]$ modulo einer Primzahl p. Diese für die algebraische Zahlentheorie so typische Grundidee wollen wir hier für unsere Zwecke mit den uns hier zur Verfügung stehenden begrenzten Mitteln entwickeln.

(3.12) Satz: (Reduktionssatz) *Es sei $f \in \mathbb{Z}[X]$ normiert und separabel. Für eine beliebige Primzahl p sei $\bar f := f \bmod p \in \mathbb{F}_p[X]$ das modulo p reduzierte Polynom; dieses ist ebenfalls*

normiert und von gleichem Grad wie f. Dann gilt:
a) Für fast alle Primzahlen p ist $\bar{f}$ separabel; genauer:

$$f \bmod p \text{ ist separabel} \iff p \not| D(f)\,.$$

b) $\bar{f}$ sei nun separabel und zerfalle über $\mathbb{F}_p$ in r Primfaktoren mit den Graden $d_1, \ldots, d_r$ (o. E. $d_1 \geq \ldots \geq d_r$). Dann enthält die Galoisgruppe $G(f)$ von f über $\mathbb{Q}$ eine Permutation σ vom Zyklentyp $(d_1, \ldots, d_r)$.

Beweis: a) Da f und $\bar{f}$ normierte Polynome gleichen Grades sind und sich die Diskriminante als ganzzahliges Polynom in den Koeffizienten von f darstellen lässt (siehe Korollar (3.11)), gilt

$$D(\bar{f}) = D_n(\bar{a}_0, \ldots, \bar{a}_{n-1}) = D_n(a_0, \ldots, a_{n-1}) \bmod p = D(f) \bmod p\,.$$

Damit folgt $D(\bar{f}) = 0 \iff D(f) \equiv 0 \bmod p \iff p \mid D(f)$. Für separables f ist $D(f) \neq 0$ und besitzt damit nur endlich viele Primteiler. Dies beweist a).

Der erste Schritt zum Beweis von b) ist die folgende Bestimmung der Galoisgruppe von Polynomen über endlichen Körpern.

(3.13) Satz: *Sei k ein endlicher Körper, $\phi \in k[X]$ ein separables Polynom, $\phi = \phi_1 \cdot \ldots \cdot \phi_r$ seine Primzerlegung über k und d_i die Grade der Primfaktoren ϕ_i. Dann gilt:*
Die Galoisgruppe $G(\phi)$ über k ist eine zyklische Gruppe erzeugt von einem Produkt $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ von elementfremden Zyklen σ_i der Längen d_i.

Der *Beweis* basiert im wesentlichen auf der aus der Algebra bekannten Tatsache, dass endliche Erweiterungen endlicher Körper stets galoissch mit zyklischer Galoisgruppe sind. Wir wollen die dazu notwendigen Argumente der Vollständigkeit halber hier wiederholen. 14/30.1.
Ist k ein endlicher Körper, so gilt:

1. Die von der Eins 1_k erzeugte *additive* zyklische Untergruppe von k ist endlich, also isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$.
2. $\mathbb{Z}/n\mathbb{Z}$ ist der kleinste Unter*ring* von k und mit k selbst nullteilerfrei. Also ist $n = p$ eine Primzahl, die *Charakteristik* von k.
3. Als endlicher Erweiterungskörper von $\mathbb{F}_p$ ist k ein endlich-dimensionaler $\mathbb{F}_p$-Vektorraum, enthält also $q := p^f$ Elemente mit $f = (k : \mathbb{F}_p) = \dim_{\mathbb{F}_p} k$.
4. In k gilt
$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j} = a^p + b^p\,,$$
denn jeder Binomialkoeffizient $\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!}$ ist für $0 < j < p$ durch p teilbar (da der Zähler, nicht aber der Nenner $j!$ durch p teilbar ist), also gleich 0 in k.
5. Damit ist die Potenzierung mit p ein Körper*homomorphismus* $\varphi_p : k \to k$. Dieser ist nicht die Nullabbildung, muss also injektiv sein (der Kern ist ein echtes Ideal im Körper k). Als Selbstabbildung einer endlichen Menge ist dieser dann auch surjektiv.

Sei $K|k$ eine Erweiterung endlicher Körper und $\#k = q$.

6. Da q eine Potenz der Charakteristik ist, ist die Potenzierung φ_q mit $q = p^f$ ein Körperautomorphismus von K, denn φ_q ist die f-fache Hintereinanderausführung des Automorphismus $x \mapsto x^p$ (siehe 5.).
7. Der Fixkörper $\mathrm{Fix}_K(\varphi_q)$ von φ_q in K ist genau k:
a) Zunächst lässt φ_q ganz k fest, denn $k^\times$ ist eine multiplikative Gruppe der Ordnung $q-1$, also gilt nach dem Satz von Lagrange $\alpha^{q-1} = 1$ für alle $\alpha \in k^\times$. Nach Multiplikation mit α erhält man $\alpha^q = \alpha$, und diese Gleichung gilt selbstverständlich auch für $\alpha = 0$. Also sind alle $\alpha \in k$ Fixpunkte von $x \mapsto x^q$.
b) Es kann aber nicht mehr Fixpunkte geben als diese q Elemente von k, denn

$$\alpha = \alpha^q \iff \alpha \text{ ist Wurzel von } X^q - X\,,$$

und ein Polynom vom Grad q hat höchstens q Wurzeln in einem Körper.

8. Damit gilt nun

$$k = \mathrm{Fix}_K(\varphi_q) \supset \mathrm{Fix}_K(\langle\varphi_q\rangle) \supset \mathrm{Fix}_K(\mathrm{Aut}(K|k)) \supset k \qquad (*)$$

und daher $k = \mathrm{Fix}_K(\mathrm{Aut}(K|k))$. Dies besagt gerade, dass $K|k$ galoissch ist. (Insbesondere ist jede endliche Erweiterung separabel und daher jedes irreduzible Polynom über einem endlichen Körper selbst separabel.) Mit dem Hauptsatz der Galoistheorie folgt dann $\mathrm{Aut}(K|k) = \langle\varphi_q\rangle$, da gemäß $(*)$ $\mathrm{Fix}_K(\langle\varphi_q\rangle) = \mathrm{Fix}_k(\mathrm{Aut}(K|k))$ gilt. Die Galoisgruppe von $K|k$ ist also zyklisch, erzeugt vom sog. *Frobeniusautomorphismus* $x \mapsto x^{\#k}$.

Wir kommen nun zum Beweis von (3.13). Sei N_ϕ der Zerfällungskörper von ϕ über k und $G(N_\phi|k)$ dessen zyklische Galoisgruppe (siehe 8.). Gemäß Satz (3.2) ist daher $G(\phi)$ zyklisch. Ist σ ein Erzeugendes, so operiert σ auf W_ϕ und den W_{ϕ_j}. Wegen der Irreduzibilität der ϕ_j operiert σ transitiv auf den Wurzelmengen W_{ϕ_j} (Proposition (3.3)). Da ϕ separabel ist, haben die Primfaktoren ϕ_j keine gmeinsamen Wurzeln, sind also die W_{ϕ_j} disjunkt. Folglich operiert σ auf jeder dieser disjunkten Mengen als ein Zyklus: σ ist ein Produkt von elementfremden Zyklen der Längen $\#W_{\phi_j} = \deg\phi_j = d_j$. □

Unter Verwendung von (3.13) reduziert sich (3.12) b) unmittelbar auf

(3.14) Satz: *Ist $f \in \mathbb{Z}[X]$ ein normiertes separables Polynom und p eine Primzahl mit $p \nmid D(f)$, so gilt für das modulo p reduzierte Polynom $\bar{f}$:*
Die Galoisgruppe $G(\bar{f})$ ist (bis auf Konjugation) Untergruppe von $G(f)$:

$$G(\bar{f}) \hookrightarrow G(f)\,.$$

Der Beweis dieses Satzes wird üblicherweise im Rahmen der algebraischen Zahlentheorie erbracht. Diese ermöglicht es, eine direkte Beziehung zwischen den Wurzeln von f und denen von $\bar{f}$ herzustellen. Da die Wurzeln von f in einem endlichen Erweiterungskörper N von $\mathbb{Q}$ (einem algebraischen Zahlkörper) liegen und die Wurzeln von $\bar{f}$ in einem endlichen Erweiterungskörper $\mathbb{F}_q$ von $\mathbb{F}_p$ liegen, erfordert dies eine Verbindung zwischen N und $\mathbb{F}_q$.

d. Beispiele. Bei der konkreten Bestimmung von Galoisgruppen kann man sich o. E. auf irreduzible Polynome beschränken. In diesem Falle ist die Galoisgruppe transitiv. Mit Hilfe des Reduktionssatzes (3.12) kann man in der Galoisgruppe Permutationen bestimmter Zyklentypen nachweisen. Zusammen mit einer Übersicht über die transitiven Permutationsgruppen und den darin auftretenden Zyklentypen ermöglicht dies eine Einschränkung der möglichen Galoisgruppen bis hin zur genauen Bestimmung. Eine solche Übersicht ist zu finden in G. Butler, J. McKay: *The transitive groups of degree up to eleven,* Comm. Alg. **11** (1983) 863–911. In den folgenden Tabellen sind für die Grade $n = 3, 4, 5, 7$ die transitiven Untergruppen von S_n, ihre Ordnung sowie die absoluten Häufigkeiten der auftretenden Zyklentypen angegeben. (Dabei steht $1^2.2^3.3^1$ abkürzend für den Zyklentyp $(3, 2, 2, 2, 1, 1)$, die Basis gibt also die Länge, der Exponent die Zahl der auftretenden Zyklenfaktoren an.)

Zyklenhäufigkeiten

Grad 3:

G	$\#G$	1^3	1.2	3^1
A_3	3	1		2
S_3	6	1	3	2

Grad 4:

G	$\#G$	1^4	$1^2.2$	2^2	1.3	4
C_4	4	1		1		2
V_4	4	1		3		
D_8	8	1	2	3		2
A_4	12	1		3	8	
S_4	24	1	6	3	8	6

Grad 5:

G	$\#G$	1^5	$1^3.2$	1.2^2	2.3	$1^2.3$	1.4	5
C_5	5	1						4
$C_5 \rtimes C_2$	10	1		5				4
$C_5 \rtimes C_4$	20	1		5			10	4
A_5	60	1		15		20		24
S_5	120	1	10	15	20	20	30	24

Grad 7:

G	$\#G$	1^7	$1^5.2$	$1^3.2^2$	1.2^3	$1^4.3$	$1^2.2.3$	$2^2.3$	1.3^2	$1^3.4$	$1.2.4$	3.4	$1^2.5$	2.5	1.6	7
C_7	7	1														6
$D14$	14	1			7											6
$C_7 \rtimes C_3$	21	1							14							6
$C_7 \rtimes C_6$	42	1			7				14						14	6
$\mathrm{GL}_3(2)$	168	1		21					56		42					48
A_7	2520	1		105		70		210	280		630		504			720
S_7	5040	1	21	105	105	70	420	210	280	210	630	420	504	504	840	720

(3.15) Beispiele: a) $f(X) = X^4 + 8X^2 - 8X + 4$ hat die Galoisgruppe A_4.
b) $f(X) = X^4 - 8X^2 + 17$ hat als Galoisgruppe die Diedergruppe D_8.
c) $f(X) = X^5 + 20X + 16$ hat als Galoisgruppe die alternierende Gruppe A_5.
d*) (Trinks 1969) $f(X) = X^7 - 7X + 3$ hat als Galoisgruppe die einfache Gruppe $\mathrm{GL}_3(2)$ der Ordnung 168 (in ihrer Operation auf den 7 Punkten von $\mathbb{F}_2^3 \setminus \{0\}$).

Begründungen: a) Wir erstellen zunächst eine Wertetabelle für f und f' mit Primzerlegung der Funktionswerte:

x	-4	-3	-2	-1	0	1	2	3	4
$f(x)$	$2^2 \cdot 3 \cdot 5 \cdot 7$	181	$2^2 \cdot 17$	$3 \cdot 7$	2^2	5	$2^2 \cdot 3^2$	$7 \cdot 19$	$2^2 \cdot 89$
$f'(x)$	$-2^3 \cdot 41$	$-2^2 \cdot 41$	$-2^3 \cdot 3^2$	$-2^2 \cdot 7$	-2^3	$2^2 \cdot 3$	$2^3 \cdot 7$	$2^2 \cdot 37$	$2^3 \cdot 3 \cdot 13$

Aus solch einer Wertetabelle kann man zunächst entnehmen, dass $+1$ einzige Nullstelle von f modulo 5 ist (im Bereich $-2, \ldots, +2$ kommt in den Werten für $f(x)$ nur bei $x = +1$ der Primfaktor 5 vor), und diese ist einfach (wegen $f'(1) \not\equiv 0 \bmod 5$). Also ist modulo 5 $\bar{f} = (X-1)\bar{g}$ mit über $\mathbb{F}_5$ irreduziblem g (da g kubisch ist und keine Wurzel hat) und daher separablem $\bar{g}$ (siehe oben 8.) Mit $\bar{g}$ ist dann auch $\bar{f}$ und folglich auch f separabel. Damit ist der Reduktionssatz (3.12) anwendbar und $G(f)$ enthält eine Permutation vom Typ $(1, 3)$, d. h. einen 3-Zyklus.

Weiter zeigt die Wertetabelle, dass f in $\mathbb{Q}$ keine Nullstelle hat, da dafür nur die Teiler von 4, d. h. $\pm 1, \pm 2, \pm 4$ in Frage kämen.

Dann folgt aber sogar, dass f irreduzibel über $\mathbb{Q}$ ist, denn eine Zerlegung von f in zwei irreduzible quadratische Faktoren würde bedeuten $G(f) \subset S_2 \times S_2$, aber wie bereits gezeigt enthält $G(f)$ einen 3-Zyklus.

Da f nun irreduzibel ist, muss $G(f)$ eine transitive Permutationsgruppe sein, die einen 3-Zyklus enthält, also $G(f) \supseteq A_4$ (siehe Beweis des zweiten Zusatzes in Korollar (2.19) für $n = 4$.)

Ob $G(f) = S_4$ ist, entscheidet die Diskriminante $D(f)$ von f (siehe Prop. (3.8)). Eine Berechnung der Diskriminante (etwa entsprechend (3.11)) ergibt $D(f) = 2^{12} \cdot 7^2$. (Dies zeigt erneut, dass f mod 5 separabel ist.) (Aus der obigen Wertetabelle kann man bereits die beiden Primteiler 2 und 7 von $D(f)$ ablesen: Gemeinsame Primteiler von $f(x)$ und $f'(x)$ zeigen, dass x eine mehrfache Wurzel von f modulo dieser Primzahl ist, diese Primzahl also die Diskriminante teilt.) Da nun $D(f)$ ein Quadrat ist, muss die Galoisgruppe von f die alternierende Gruppe A_4 sein.

b) Bei diesem Polynom kann man die Wurzeln berechnen und so mit rein körpertheoretischen Mitteln die Galoisgruppe bestimmen. Wir benutzen hier zur Demonstration die Reduktionsmethode. Wieder berechnen wir zunächst eine kleine Wertetabelle:

x	-3	-2	-1	0	1	2	3
$f(x)$	$2 \cdot 13$	1	$2 \cdot 5$	17	$2 \cdot 5$	1	$2 \cdot 13$
$f'(x)$	$-2^2 \cdot 3 \cdot 5$	0	$2^2 \cdot 3$	0	$-2^2 \cdot 3$	0	$2^2 \cdot 3 \cdot 5]$

Wir sehen, dass 1 eine mehrfache Wurzel modulo 2 ist und daher 2 ein Diskriminantenteiler ist. Genauer gilt modulo 2 $\bar{f}(X) = X^4+1 = (X+1)^4$, also $\bar{f}(X-1) = X^4$, so dass alle Koeffizienten von $f(X-1)$ außer dem führenden durch 2 teilbar sind. Da $f(-1)$ nicht durch 4 teilbar ist (siehe Wertetabelle), ist $f(X-1)$ 2-Eisenstein'sch, also irreduzibel und folglich separabel. Dann ist natürlich auch $f(X)$ selbst irreduzibel und separabel.
Nun zeigt die Wertetabelle, dass f keine Nullstelle modulo 3 besitzt, so dass nach dem Reduktionssatz die Galoisgruppe eine Permutation ohne Fixpunkte enthalten muss, also einen 4-Zyklus oder das Produkt aus 2 Transpositionen.
Da f modulo 5 genau 2 (einfache) Nullstellen hat, enthält $G(f)$ eine Transposition.
Damit kommen für $G(f)$ gemäß der Liste von Butler-McKay nur die Gruppen D_8 oder S_4 in Frage. Wäre nun $G(f) = S_4$, so gäbe es in $G(f)$ eine Permutation mit nur einem Fixpunkt α. Aber mit α ist auch $-\alpha$ Wurzel von f, da f gerade ist. Also muss $\alpha = -\alpha$, d. h. $\alpha = 0$ sein, im Widerspruch zu obiger Wertetabelle. Damit ist die Galoisgruppe die symmetrische Gruppe S_4.
c) Stichworte: $D(f) = 2^{16} \cdot 5^4$, also $G(f) \subseteq A_5$.
Eine Werteabelle ergibt: f mod 7 hat genau zwei einfache Wurzeln (nämlich $-3, -2$), der kubische Cofaktor ist notwendig irreduzibel und die Galoisgruppe enthält folglich eine Permutation vom Zyklentyp $(3, 1, 1)$, d. h. einen 3-Zyklus.
Modulo 3 hat f keine Wurzeln. Wäre f mod 3 reduzibel, so zerfiele es in zwei Faktoren der Grade 2 bzw. 3. Die Galoisgruppe enthielte also eine Permutation vom Zyklentyp $(3, 2)$, diese wäre aber ungerade, Widerspruch! Also ist f mod 3 irreduzibel, dann aber erst recht auch f.
Fazit: $G(f)$ ist transitiv von Primzahlgrad 5 und enthält einen 3-Zyklus, also nach Korollar (2.19) $G(f) \supseteq A_5$.
d*) Dieses Polynom ist das erste Beispiel für ein Polynom mit der G_{168} als Galoisgruppe (Leopoldt/Trinks 1969). Es markiert zugleich einen wichtigen Forschungsbereich der Galoistheorie, nämlich das sog. *Umkehrproblem* der Galoistheorie: Welche endlichen Gruppen sind Galoisgruppen über $\mathbb{Q}$? Diese Frage ist bisher nicht abschließend beantwortet, man vermutet, dass alle endlichen Gruppen auftreten können.
Ansätze zur Lösung von d*):
1. Da das Polynom spärlich besetzt ist, ist die Berechnung der Diskriminante nicht problematisch: $D(f) = 3^8 \cdot 7^8$. (Erst recht nicht bei Benutzung eines Computers.) Also $G(f) \subseteq A_7$.
2. Eine Wertetabelle zeigt: 4 ist einzige Nullstelle von f mod 7. Wegen $7 \mid D(f)$ könnte $f(X+4)$ 7-Eisensteinsch sein. In der Tat (vgl. endliche Körper, Punkte 3. und 6.a)

$$f(X+4) = (X+4)^7 - 7(X+4) + 3 \equiv (X+4)^7 + 3 \equiv X^7 + 4^7 + 3 \equiv X^7 + 4 + 3 \equiv X^7 \bmod 7\,,$$

und $f(4) = 16359 \not\equiv 0 \bmod 7^2$. Damit sind $f(X+4)$ und $f(X)$ irreduzibel über $\mathbb{Q}$.
3. f hat genau 3 reelle Nullstellen, also enthält $G(f)$ eine Permutation vom Zyklentyp $(2, 2, 1, 1, 1)$. Nach einem Vergleich mit der Liste von Butler-McKay bleiben nur die Möglichkeiten $G(f) = \mathrm{GL}_3(2)$ oder $G(f) = A_7$.
Hier enden zunächst unsere Bemühungen zum Beweis von d*).

Diese Beispiele verdeutlichen, wie der Reduktionssatz zur Bestimmung der Galoisgruppe eingesetzt werden kann: Man weist die Existenz gewisser Zyklentypen in der Galoisgruppe nach und schließt dadurch gewisse 'kleine' Galoisgruppen aus. Auf diese Weise erhält man also eine Beschränkung von $G(f)$ 'nach unten'. Eine Beschränkung nach oben ist so zunächst nicht möglich, da Satz (3.12) nicht aussagt, ob auf diesem Wege alle in $G(f)$ auftretenden Zyklentypen

erfasst werden. Dies ist aber tatsächlich der Fall nach dem folgenden fundamentalen Satz der algebraischen Zahlentheorie, der hier nicht bewiesen werden kann:

(3.16) Satz: (Dichtigkeitssatz von Čebotarev) Zu jedem in der Galoisgruppe $G(f)$ eines irreduziblen Polynoms $f \in \mathbb{Z}[X]$ auftretenden Zyklentyp $t = (l_1, \ldots, l_r)$ ($l_i \geq 1$, $\sum l_i = n$) gibt es unendlich viele Primzahlen $p \nmid D(f)$, für die das modulo p reduzierte Polynom $\bar{f} = f \bmod p$ über $\mathbb{F}_p$ in r Primfaktoren der Grade $l_1, \ldots, l_r$ zerfällt. Mehr noch:
Die *Wahrscheinlichkeit,* eine solche Primzahl zu finden[1)], ist gerade die relative Häufigkeit der Gruppenelemente in $G(f)$ mit diesem Zyklentyp t.
Oder suggestiver, aber auch laxer formuliert: Die Wahrscheinlichkeit, eine solche Primzahl zu finden, ist gleich der Wahrscheinlichkeit, den zugehörigen Zyklentyp in der Galoisgruppe zu finden.

Dieses Resultat erlaubt es aber noch nicht, die Möglichkeit A_7 auszuschließen, da alle Zyklentypen von $\mathrm{GL}_3(2)$ auch in A_7 auftreten.

Allerdings hat man auf der Basis dieses Satzes einen probabilistischen Ansatz zur Lösung von Problem d*). Wir betrachten die *Häufigkeit* der Permutationen in den möglichen Galoisgruppen $\mathrm{GL}_3(2)$ bzw. A_7 mit keinem bzw. genau einem Fixpunkt.

#Fixpunkte	$\mathrm{GL}_3(2)$	A_7
0	$\frac{48}{168} \approx 29\%$	$\frac{930}{2520} \approx 37\%$
1	$\frac{98}{168} \approx 58\%$	$\frac{910}{2520} \approx 36\%$

Wir berechnen nun (wieder mit einer Wertetabelle und deren Primzerlegungen) die Wurzeln von $f \bmod p$ in $\mathbb{F}_p$. Im Bereich der Primzahlen $p \leq 73$ tritt jeweils *höchstens* eine Wurzel auf. (Drei Wurzeln treten erstmals bei $p = 79$ auf.) Die Häufigkeitsverteilung in diesem Bereich ist 32% (keine Wurzel) und 68% (genau eine Wurzel). Ein Vergleich mit obigen Werten legt die Vermutung nahe: $G(f) = \mathrm{GL}_3(2)$.

Um nun statt dieses probabilistischen Ergebnisses einen Beweis zu erhalten, benutzt man, dass A_7 3-transitiv, also auf der Menge $\mathcal{P}_3(\underline{7}) = \{I \subset \underline{7} \mid \#I = 3\}$ der 3-elementigen Teilmengen transitiv operiert. Dagegen ist $\mathrm{GL}_3(2)$ jedoch nur 2-transitiv und operiert nicht transitiv auf $\mathcal{P}_3(\Omega)$ ($\Omega = (\mathbb{F}_p^3)^{\#} = \mathbb{F}_p^3 \setminus \{0\}$): Die Basen des $\mathbb{F}_p^3$ bilden eine Bahn, die übrigen (linear abhängigen) Mengen von 3 verschiedenen Vektoren $\neq 0$ die zweite. Letztere Mengen sind gerade die verschiedenen Ebenen in $\mathbb{F}_2^3$ (jeweils ohne den Nullvektor). Da die Hyperebenen in einem Vektorraum V gerade durch die Kerne der Linearformen $\neq 0$ gegeben sind, ist ihre Anzahl genauso groß wie die Zahl der Vektoren $\neq 0$ (V und Dualraum V^* sind isomorph!). Damit hat also $\mathrm{GL}_3(2)$ in seiner Operation auf $\mathcal{P}_3(\Omega)$ eine Bahn der Länge 7.

Man zeigt nun (in Analogie zu (3.3)), dass die Transitivität von $G(f)$ auf $\mathcal{P}_3(W_f)$ äquivalent ist zur Irreduzibilität des folgenden Polynoms

$$f_3 = \Big(\prod_{I \in \mathcal{P}_3(W_f)} (X - \alpha_I) \Big)_{\mathrm{sep}}$$

wobei $\alpha_I = \sum_{i \in I} \alpha_i$ die Summen von je 3 Wurzeln von f sind und der Zusatz $(\ldots)_{\mathrm{sep}}$ bedeutet, dass man den separablen Teil des Polynoms nimmt, d. h. die *verschiedenen* α_I treten nur *einmal* im Produkt auf. Dieses Polynom ist (da symmetrisch in den α_i) ein Polynom über $\mathbb{Q}$ (vom Grade $\binom{7}{3} = 35$).
Eine Möglichkeit die Behauptung d*) zu beweisen, ist der Nachweis der Reduzibilität von f_3. Da die Operation von $\mathrm{GL}_3(2)$ auf $\mathcal{P}_3(\Omega)$ eine Bahn der Länge 7 hat (s.o.), sucht man nach einem (irreduziblen) Faktor von f_3 vom Grade 7.

[1)] Präzise formuliert ist dies die sog. *Dirichletdichte* der entsprechenden Primzahlmenge.