Vortrag 4 — Anzahl von p -Untergruppen

Länge bedeute Kardinalität (meist von gewissen Teilmengen).

1. Zyklische Gruppe

Sei $m \geq 1$. Sei $\mathcal{C}_m := \langle x \rangle$ die zyklische Gruppe von Ordnung m .

Bemerkung 1. Sei d ein Teiler von m . Es hat $\mathcal{C}_m$ genau eine Untergruppe von Ordnung d .

Beweis. Schreibe $m = de$. Das Element x^e hat Ordnung d . Damit ist $|\langle x^e \rangle| = d$.

Bleibt zu zeigen, daß jede Untergruppe $U \leq \mathcal{C}_m$ von Ordnung d mit $\langle x^e \rangle$ übereinstimmt. Für $x^i \in U$ gilt $1 = (x^i)^{|U|} = x^{id}$. Also ist $m = ed$ ein Teiler von id . Also ist e ein Teiler von i . Somit ist $x^i \in \langle x^e \rangle$. Also ist $U \leq \langle x^e \rangle$. Wegen $|U| = d = |\langle x^e \rangle|$ ist $U = \langle x^e \rangle$. $\square$

2. Satz von Sylow-Wielandt

Sei G eine endliche Gruppe. Sei p prim. Schreibe $|G| = p^t n$ mit $t \in \mathbf{Z}_{\geq 0}$ und $n \not\equiv_p 0$. Sei $s \in [0, t]$. Setze

$$A_G(p^s) := |\{H \leq G : |H| = p^s\}|.$$

Satz (Sylow-Wielandt). Es ist $A_G(p^s) \equiv_p 1$.

Im Falle $s = t$ ist dies die Aussage des dritten Sylowsatzes: die Anzahl der p -Sylowgruppen von G ist kongruent zu 1 modulo p .

3. Vorarbeiten zum Beweis

Sei

$$\Omega := \{M \subseteq G : |M| = p^s\}.$$

Es ist $|\Omega| = \binom{p^t n}{p^s}$.

Es operiert G auf Ω via $g \cdot M := \{gm : m \in M\}$.

Wir schreiben $C_G(M) = \{g \in G : g \cdot M = M\} \leq G$.

Bemerkung 2. Sei $M \in \Omega$. Es ist $|C_G(M)|$ ein Teiler von p^s .

Ist ferner $|C_G(M)| = p^s$, so ist $M = C_G(M)m$ für ein $m \in M$.

Beweis. Aus $g \cdot M = M$ für alle $g \in C_G(M)$ folgt, daß $gm \subseteq M$ für alle $g \in C_G(M)$ und alle $m \in M$, d.h. daß $C_G(M)m \subseteq M$ für alle $m \in M$. Also ist

$$M = \bigcup_{m \in M} C_G(M)m.$$

Da zwei solche Rechtsnebenklassen $C_G(M)m$ und $C_G(M)m'$ aber disjunkt oder gleich sind, gibt es $m_i \in M$ mit

$$M = \bigsqcup_i C_G(M)m_i.$$

Da alle Teilnehmer dieser disjunkten Vereinigung Länge $|C_G(M)|$ haben, folgt, daß $|M| = p^s$ ein Vielfaches von $|C_G(M)|$ ist.

Ist nun $p^s = |C_G(M)|$, so hat diese disjunkte Vereinigung nur einen Teilnehmer. $\square$

Bemerkung 3. *Es enthält jede Bahn von Ω höchstens eine Untergruppe.*

Beweis. Seien $H, \tilde{H} \leq G$ mit $|H| = |\tilde{H}| = p^s$ in derselben Bahn von Ω . Dann gibt es ein $g \in G$ mit $\tilde{H} = gH$. Insbesondere ist $1 \in gH$, d.h. $1 = gh$ für ein $h \in H$. Somit ist $\tilde{H} = gH = h^{-1}H = H$. $\square$

Bemerkung 4. *Enthält eine Bahn von Ω eine Untergruppe, so hat sie Länge $p^{t-s}n$.*

Beweis. Sei $H \leq G$ mit $|H| = p^s$. Dann ist $G \cdot H = \{gH : g \in G\} = G/H$, und also $|G \cdot H| = |G/H| = |G|/|H| = p^{t-s}n$. $\square$

Bemerkung 5. *Ist eine Bahn von Ω von Länge $p^{t-s}n$, so enthält sie eine Untergruppe.*

Beweis. Sei $M \in \Omega$ so gegeben, daß $|G \cdot M| = p^{t-s}n$.

Mit dem Bahnenlemma folgt $|C_G(M)| = \frac{|G|}{|G \cdot M|} = p^s$.

Aus Bemerkung 2 folgt $M = C_G(M)m$ für ein $m \in M$. Nun ist aber die Untergruppe $m^{-1}C_G(M)m = m^{-1}M$ in der Bahn von M . $\square$

Bemerkung 6. *Ist eine Bahn von Ω nicht von Länge $p^{t-s}n$, so wird ihre Länge von $p^{t-s+1}n$ geteilt.*

Beweis. Sei $M \in \Omega$. Mit dem Bahnenlemma und Bemerkung 2 sehen wir, daß $\frac{|G|}{|G \cdot M|} = |C_G(M)|$ ein Teiler von p^s ist. Also gibt es ein $u \geq 0$ mit

$$\frac{p^t n}{|G \cdot M|} \cdot p^u = p^s.$$

Es folgt

$$|G \cdot M| = p^{t-s+u}n.$$

Ist nun $|G \cdot M| \neq p^{t-s+u}n$, so ist $u \geq 1$. $\square$

4. Beweis zu Sylow-Wielandt

Sei

$$\Omega = G \cdot M_1 \sqcup \dots \sqcup G \cdot M_k \sqcup G \cdot M_{k+1} \sqcup \dots \sqcup G \cdot M_\ell$$

die disjunkte Zerlegung in Bahnen, so sortiert, daß $|G \cdot M_i| = p^{t-s}n$ genau dann, wenn $i \in [1, k]$.

Aus den Bemerkungen 4 und 5 folgt, daß eine Bahn von Ω genau dann eine Untergruppe enthält, wenn sie von Länge $p^{t-s}n$ ist.

Mit Bemerkung 3 ist also die Anzahl k der Bahnen von Ω von Länge $p^{t-s}n$ gleich der Anzahl $A_G(p^s)$ der Elemente von Ω , die Untergruppen von G sind.

Mit Bemerkung 6 wird

$$\binom{p^t n}{p^s} = |\Omega| = \sum_{i \in [1, \ell]} |G \cdot M_i| \equiv_{p^{t-s+1}n} \sum_{i \in [1, k]} |G \cdot M_i| = A_G(p^s) \cdot p^{t-s}n.$$

Da man so für jede Gruppe von Ordnung $p^t n$ schließen kann, also auch für $C_{p^t n}$, ist mit Bemerkung 1

$$A_G(p^s) \cdot p^{t-s}n \equiv_{p^{t-s+1}n} \binom{p^t n}{p^s} \equiv_{p^{t-s+1}n} \underbrace{A_{C_{p^t n}}(p^s)}_{=1} \cdot p^{t-s}n = p^{t-s}n.$$

Entfernen des Faktors $p^{t-s}n$ gibt

$$A_G(p^s) \equiv_p 1.$$

5. Beispiel $G = \mathcal{S}_4$, $p = 2$.

Untergruppen von Ordnung 1: $\{\text{id}\}$. Also $A_{\mathcal{S}_4}(1) = 1 \equiv_2 1$.

Untergruppen von Ordnung 2: $\langle(1, 2)\rangle$, $\langle(1, 3)\rangle$, $\langle(1, 4)\rangle$, $\langle(2, 3)\rangle$, $\langle(2, 4)\rangle$, $\langle(3, 4)\rangle$,
 $\langle(1, 2)(3, 4)\rangle$, $\langle(1, 3)(2, 4)\rangle$, $\langle(1, 4)(2, 3)\rangle$. Also $A_{\mathcal{S}_4}(2) = 9 \equiv_2 1$.

Untergruppen von Ordnung 4: $\langle(1, 2), (3, 4)\rangle$, $\langle(1, 3), (2, 4)\rangle$, $\langle(1, 4), (2, 3)\rangle$,
 $\langle(1, 2)(3, 4), (1, 3)(2, 4)\rangle$, $\langle(1, 2, 3, 4)\rangle$, $\langle(1, 3, 2, 4)\rangle$, $\langle(1, 3, 4, 2)\rangle$. Also $A_{\mathcal{S}_4}(4) = 7 \equiv_2 1$.

Untergruppen von Ordnung 8: $\langle(1, 2, 3, 4), (1, 3)\rangle$, $\langle(1, 3, 2, 4), (1, 2)\rangle$,
 $\langle(1, 2, 4, 3), (1, 4)\rangle$. Also $A_{\mathcal{S}_4}(8) = 3 \equiv_2 1$.

Beachte, daß die Untergruppen von Ordnung 2 nicht alle zueinander konjugiert sind. Auch die Untergruppen von Ordnung 4 sind nicht alle zueinander konjugiert. Wohl aber sind dies, in Übereinstimmung mit dem zweiten Sylowsatz, die Untergruppen von Ordnung 8, denn dies sind die 2-Sylowgruppen in $\mathcal{S}_4$.