Sylow-Sätze

Sei U eine Untergruppe von G.
Die Ordnung von U teilt $|G|$
(G wird von disjunkten Nebenklassen gleicher Elementeanzahl
überdeckt).
Umgekehrt kann für alle Teiler $k = p^s$ von $|G|$ die Existenz einer Untergruppe U
mit $|U| = k$ nachgewiesen werden (Satz 1).

Sei hierzu A eine k-elementige Teilmenge von G.
Die Elemente von G, die A bei einer Translation fix lassen, bilden eine Untergruppe
(Stabilisator) $S = \{g \in G \mid gA = A\}$. Es gilt

$|S| \leq |A|$

Nachweis:
Sei $a \in A$. Dann ist $Sa \subset A$. Daraus folgt: $|Sa| = |S| \leq |A|$

Die Teilmenge A wird so zu wählen sein, dass $|S| = |A| = k$ vorliegt.

Wir betrachten alle k-elementigen Teilmengen A_k.
Die Translationen $x \to ax$, $a \in G$, bilden diese Teilmengen aufeinander ab
(G operiert auf den Teilmengen).
Unter einer Bahn verstehen wir alle Bilder $\{aA, a \in G\}$ einer k-elementigen Teilmenge A.

Unschwer zu beweisen ist:

Die Menge der k-elementigen Teilmengen zerfällt in disjunkte Bahnen.
Die Summe der Bahnlängen beträgt daher $\binom{n}{k}$.

Die Länge (Anzahl der Elemente) einer Bahn ist die Anzahl der Nebenklassen $[G : S_A]$.
Hierbei ist A ein Element der Bahn und S_A dessen Stabilisator.

Sei $n = p^r \cdot m$ und p^r die höchste p-Potenz in n.
Wir haben dann folgende Situation:

$$\underbrace{|G|}_{p^r \cdot m} = \underbrace{[G : S_A]}_{\leq\, ?} \cdot \underbrace{|S_A|}_{\leq\, p^s}$$

Könnten wir letztendlich nachweisen, dass für ein A in der Anzahl $[G : S_A]$ der Nebenklassen die p-Potenz p^{r-s} nicht übertroffen wird, so hätte dies das Gewünschte $|S_A| = p^s$ zur Folge.

Es ist somit eine Bahn aufzufinden, in deren Länge die p-Potenz höchstens p^{r-s} ist. Die Bahnen können nicht sämtlich höhere p-Potenzen haben, denn dann träfe dies auch für $\binom{n}{k}$ zu.
Und das ist nicht der Fall, wie leicht zu sehen ist:

$$\binom{n}{k} = \binom{p^r \cdot m}{p^s} = \underbrace{\frac{p^r \cdot m}{p^s}}_{p^{r-s} \cdot m} \binom{p^r \cdot m - 1}{p^s - 1}, \qquad \text{beachte: } p \nmid \binom{p^r \cdot m - 1}{p^s - 1} = \prod_{i=1}^{p^s - 1} \frac{p^r \cdot m - i}{p^s - i}$$

Ein p im Zähler teilt auch ein i und damit den Nenner. Somit kürzt es sich heraus.

Sylow Satz 2

Leicht nachzuweisen ist:
Mit V (Untergruppe von G) ist auch $U = gVg^{-1}$, $g \in G$, eine Untergruppe,
die zudem isomorph zu V ist.

U und V heißen konjugiert.

Nach Satz 1 existiert zu jedem s eine Untergruppe der Ordnung p^s,
$s \leq r$ für $|G| = p^r \cdot m$ mit r maximal.

Eine Untergruppe V mit maximalem r heißt (die zu p gehörende) p-Sylowgruppe.

Zu jeder Untergruppe U mit Primzahlpotenz-Ordnung p^s kann ein $g \in G$ gefunden werden,
so dass $U \subset gVg^{-1}$ ist (Satz 2).

$U \subset gVg^{-1} \iff ug \in gV,\ u \in U \iff ugV = gV,\ u \in U$

Wir betrachten alle Linksnebenklassen von V. Auf ihnen operiert U.
Die m Nebenklassen zerfallen in Bahnen, deren Längen $|U|$ teilen.
Hierfür kommen daher nur 1 oder eine Potenz von p infrage.
Es muss eine Bahn der Länge 1 gefunden werden.
Wären alle Längen durch p teilbar, so träfe dies auch für m zu.
m ist jedoch nicht durch p teilbar. □

Insbesondere sind alle zu p gehörenden Sylowgruppen konjugiert.

Sylow Satz 3

Dieser Satz schließt an die Überlegungen von Satz 1 an und beinhaltet eine Aussage über die Anzahl der Untergruppen der Ordnung p^s.

Im Beweis von Satz 1 sahen wir, dass es zu jeder p^s-elementigen Teilmenge A, deren Bahnlänge höchstens durch p^{r-s} teilbar ist, eine (Stabilisator-)Untergruppe U mit gleicher Elementeanzahl existiert. Sei M die Menge dieser Teilmengen A.
Für $a \in A$ galt $Ua \subset A$. Aus der Gleichheit der Elementezahl folgt $A = Ua$.
Die Elemente (Teilmengen) aus M sind also Rechtsnebenklassen von Untergruppen.

Idee:
$|\,M\,|$ kann mithilfe der Nebenklassen bestimmt werden und damit auch die Anzahl der komplementären Menge $\overline{M}$ der p^s-elementigen Teilmengen B, deren Bahnlänge durch p^{r-s+1} teilbar ist. p^{r-s+1} teilt dann $|\,\overline{M}\,|$ ...

Die Anzahl der Gruppen mit der Ordnung p^s sei k.
Die Gesamtzahl der Nebenklassen beträgt dann $p^{r-s}mk$ (es war $|\,G\,| = p^r m$).
Hierbei wird berücksichtigt, dass unterschiedliche Untergruppen auch unterschiedliche Nebenklassen haben: $U_1 a = U_2 b \implies a \in U_2 b \implies U_2 a = U_2 b = U_1 a \implies U_1 = U_2$

Alle Nebenklassen sind in M enthalten, so dass gilt: $|\,M\,| = p^{r-s}mk$
Sei hierzu Ua ($a \in G$) eine Rechtsnebenklasse von U und $|\,U\,| = p^s$.
Ua liegt in M und hat U als Stabilisatorgruppe. Die Bahnlänge von Ua beträgt $[G : U] = p^{r-s}m$, d. h. $Ua \in M$.

Es gab $\binom{n}{p^s} = p^{r-s}ml$ p^s-elementige Teilmengen, $l = \prod_{i=1}^{p^s-1} \frac{p^r \cdot m - i}{p^s - i}$.

Daraus folgt $|\,\overline{M}\,| = p^{r-s}m(l-k)$.

p^{r-s+1} teilt $|\,\overline{M}\,|$ und damit ist p ein Teiler von $l - k$.

Mit einer einfachen Charakterisierung von l sind wir am Ziel.

Die in i auftauchenden p's (siehe l) kürzen sich heraus, Ausmultiplizieren ergibt:

$$l = \frac{pu + a}{pv + a} \text{ mit } u, v, a \in \mathbb{Z} \text{ und } p \nmid a \implies p \mid (l-1) \implies l = \lambda p + 1$$

Zusammenfassend ergibt sich für die Anzahl der p^s-elementigen Untergruppen:

$$k = \kappa p + 1,\ \kappa = 0, 1, 2, \ldots$$

Anzahl der p-Sylowgruppen

Nach Satz 2 sind die p-Sylowgruppen konjugiert. Ihre Anzahl k ist daher ein Teiler von $|\,G\,| = p^r m$.

Denn für eine Untergruppe U bilden alle $g \in G$ mit $gUg^{-1} = U$ eine Untergruppe N (Normalisator) und die Anzahl der Konjugierten von U ist gleich dem Index von N in G.

Mit Satz 3 folgt, dass k m teilt.