Eine Formalisierung des zweiten Satzes von Sylow aus der Gruppentheorie in Isabelle im Vergleich zu einer Implementierung in Lean

Moritz Hartlieb, Jonas Lippert

25. Februar 2020

1 Einführung

Der zweite Satz von Sylow lautet wie folgt.

Satz. Sei p eine Primzahl und G eine endliche Gruppe mit $|G| = p^r * m$, sodass $p \nmid m$. Sei $U \leq G$ eine p-Untergruppe, und sei $P \leq G$ eine p-Sylowgruppe. Dann gilt:

(i) Es gibt ein $g \in G$ mit
$$gUg^{-1} \subseteq P.$$

(ii) Je zwei p-Sylowgruppen sind konjugiert.

Die Beweisidee ist, die Untergruppe U auf den Linksnebenklassen von P operieren zu lassen. Bezüglich dieser Gruppenoperation existieren Fixpunkte, weil deren Anzahl nach Bahnenfornmel kongruent zur Anzahl der Nebenklassen von P (mod p) ist. Da $P \in \mathrm{Syl}_p(G)$, gilt nach Definition $p \nmid |G/P|$.

Ein solcher Fixpunkt gP mit $g \in G$ liefert dann $gUg^{-1} \subseteq P$.

Es werden also zunächst Grundbegriffe der Mengenlehre und Gruppentheorie sowie natürliche Zahlen, Primzahlen und Teilbarkeitseigenschaften benötigt. Hierzu bieten sich unterschiedliche Herangehensweisen an. Es stellt sich heraus, dass Isabelle für kleine Theorien gut geeignet ist, deren Grundlagen axiomatisch eingeführt werden, die ihrerseits in einer eigenen Theorie entwickelt werden (können). Die Implementierung in Lean baut hingegen auf bereits formalisierte Grundlagen auf und ist somit Teil einer einzigen großen Theorie der Mathematik.

Interessant ist im weiteren Verlauf die Formalisierung von Nebenklassen. Um unnötige Begriffsbildung im Sinne einer kleinen Theorie zu vermeiden, bietet sich in ForTheL eine direkte Konstruktion an:
$$Coset(g, H, G) \coloneqq \left\{ g *^G h \mid h << H \right\}.$$
Anschließend ist zu zeigen, dass G disjunkte Vereinigung von Nebenklassen bzgl. einer beliebigen Untergruppe H ist. In Lean wird dagegen bzgl. einer Untergruppe S von G folgende Äquivalenzrelation auf G eingeführt:

$$x \sim_S y :\Leftrightarrow x^{-1} * y \in S.$$

Lean erlaubt uns, den Quotient $G/\sim_S$ zu betrachten. Es wird verwendet, dass $x \sim_S y$ genau dann, wenn xS und yS die selbe Nebenklasse repräsentieren.

Im Folgenden werden zunächst die jeweiligen Formalisierungen im Detail dargestellt...