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

Moritz Hartlieb, Jonas Lippert

8. März 2020

1 Einleitung

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 Bahnenformel 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 Gruppentheorie, endliche Mengen sowie natürliche Zahlen, Primzahlen und Modulo-Rechnung benötigt. Hierzu bieten sich unterschiedliche Herangehensweisen an. Es stellt sich heraus, dass Naproche 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 die Formalisierung von Nebenklassen. Um unnötige Begriffsbildung im Sinne einer kleinen Theorie zu vermeiden, bietet sich in Naproche 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...

2 Formalisierung in Naproche

2.1 Struktur + Einbettung

Die Formalisierung in Naproche teilt sich in 8 Dateien auf:

Name	Inhalt	Abschnitt
01basicgrouptheory.ftl	Pescadero	23.09.2002
02numbers.ftl	Glendale	17.05.2003
03cards.ftl	Glendale	17.05.2003
04lagrange.ftl	Glendale	17.05.2003
05staborb.ftl	Glendale	17.05.2003
06fixedpointsmodp.ftl	Glendale	17.05.2003
07grpaction.ftl	Glendale	17.05.2003
08sylow2.ftl		

Da das Naproche System Probleme hatte, alle Dateien als ganzes zu verifizieren, haben wir in jeder Datei jeweils die Axiome eingefügt anstatt Theoreme. Grundsätzlich wäre es möglich über den Befehl `[read dateiname.ftl]` da dieser Befehl jedoch in der jetzigen Version von Naproche nicht auf allen Betriebssystemen wie gewünscht funktioniert haben wir und dies durch Kommentare im Quelltext vermerkt.

In den folgenden Abschnitten beschreiben wir den Inhalt dieser Datein

2.2 Grundlegende Definitionen

Zunächst führen wir einige grundlegenden Definitionen ein. Interessant ist hier insbesondere der Begriff der `disjunct collection` den wir einführen um später über disjunkte Vereinigung und deren Kardinalitäten ßprechenßu können.

```
Let M, N denote sets.
Let x << M stand for x is an element of M.

Definition.
Prod(M,N) = { (x,y) | x << M and y << N }.

Definition.
A subset of M is a set N such that every element of N is an element of M.

Definition.
Let M be a set.
M is empty iff there is no element x of M such that x = x.

Definition.
Let M be a set such that for all elements N of M N is a set.
\-/ M = {x | There is an element N of M such that x is an element of N}.

Definition.
Let N1, N2 be sets.
N1 \-/ N2 = {x | x is an element of N1 or x is  an element of N2}.

Definition.
Let N1 be a set.
Let N2 be a subset of N1.
N1 \\ N2 = {x | x is an element of N1 and (x is not an element of N2)}.
```

```
Definition.
Let N1, N2 be a sets.
N1 and N2 are disjunct iff there is no element x of N1 such that x is an element of
    N2.

Definition.
A disjunct collection is a set M such that
(for all elements N of M N is a set) and for all elements N1, N2 of M (N1 = N2 or (
    N1 and N2 are disjunct)).

Definition.
Let f be a function. Let M,N be sets. f is from M to N iff Dom(f) = M and for every
    element x of M f[x] is an element of N.

Definition.
Let f be a function. Range(f) = {f[x] | x << Dom(f)}.

Definition.
Let f be a function. f is injective iff for all elements x,y of Dom(f) we have (x!=y
    => f[x] != f[y]).

Definition.
Let f be a function. f is surjective onto M iff
(f is from Dom(f) to M
and for every y << M there is an element x of Dom(f) such that f[x]=y).
```

2.3 Einführung des Gruppenbegriffs

Wir führen den Begriff der Gruppe ganz allgemein als Notion ein, zu der ein Einselement, Ein Inverses auch das Produkt wird nicht als "Funktionßondern.

```
[synonym group/-s]
[synonym subgroup/-s]

Signature.
A group is a notion.

Let G denote a group.

Signature.
El(G) is a  set.

Signature.
One(G) is an object.

Axiom.
```

```
One(G) << El(G).

Signature.
Let a, b be elements of El(G).
a *^{G} b is an element of El(G).

Signature.
Let a be an element of El(G).
Inv(a, G) is an element of El(G).

Axiom Assoc.
Let x, y, z be elements of El(G). x *^{G} ( y *^{G} z) = (x *^{G} y) *^{G} z.

Axiom InvOne.
Let x be an element of El(G). x *^{G} Inv(x, G) = One(G) = Inv(x, G) *^{G} x.

Axiom MulOne.
Let x be an element of El(G). x *^{G} One(G) = x =  One(G) *^{G} x.

Lemma InvUniq.
Let x, y be elements of El(G).
If x *^{G} y = One(G) then y = Inv(x, G).

Lemma OneUniq.
Let x, y be elements of El(G).
If x *^{G} y = x then y = One(G).
```

2.4 Untergruppen

Untergruppen definieren wir als Teilmengen.

In diesem Sinne sind Untergruppen keine Gruppen.

Da wir die Gruppen sehr abstrakt eingeführt haben, lässt sich nicht zeigen, dass Untergruppen auch eine Gruppee bilden.

Da der Beweis des zweiten Satzes von Sylow die Untergruppen als Gruppen auffassen muss, fordern wir dieses allgemein bekannte Korollar aus der Definiton von Untergruppen axiomatisch.

```
Definition.
A subgroup of G is set H such that
(H is a subset of El(G))
and (One(G) << H)
and (for every x << H Inv(x, G) << H)
and (for all elements x, y of H x *^{G} y << H).

Definition.
Let U be a subgroup of G.
Gr(U, G) is a group H such that
```

```
(El(H) = U)
and (One(H) = One(G))
and (for every x << U Inv(x, H) = Inv(x, G))
and (for all elements x, y of U x *^{Gr(U, G)} y = x *^{G} y).

Lemma.
Let G be a group.
Let H be a subset of El(G).
Assume ((There is a x << H such that x = x) and (for all elements  y, z of H  z *^{G}
     Inv(y, G) << H)).
H is a subgroup of G.
Proof.
  One(G) << H.
    Proof.
      Take x << H.
      Then One(G) = x *^{G} Inv(x, G).
      Thus One(G) << H.
    end.

  For every x << H Inv(x, G) << H.
    Proof.
      Let x be an element of H.
      Then Inv(x, G) = One(G) *^{G} Inv(x, G).
      Thus Inv(x, G) << H.
    end.

  For all elements x, y of H x *^{G} y << H.
  Proof.
    Let x, y be elements of H.
    Then Inv(x, G) << H.
    x *^{G} y = x *^{G}  Inv(Inv(y, G), G).
    Hence x *^{G} y << H.
    end.
Qed.
```

2.5 Nebenklassen

Wir führen Untergruppen als Teilmengen von G ein und zeigen dann, dass sich die Trägermenge der Gruppe als disjuntke Vereinigung aller Nebenklassen ergibt.

```
Definition.
Let g be an element of El(G).
Let H be a subgroup of G.
Coset(g, H, G) = {g *^{G} h | h << H}.

Lemma.
Let H be a subgroup of G.
```

```
Let g1, g2 be elements of El(G).
Assume Coset(g1, H, G) and Coset(g2, H, G) are not disjunct.
Inv(g2, G) *^{G} g1 << H.
Proof.
  Take y << El(G) such that (y << Coset(g1, H, G) and y << Coset(g2, H, G)).
  Take b << H such that y = g1 *^{G} b.
  Take c << H such that y = g2 *^{G} c.

  We have g1 = y *^{G} Inv(b, G).
          g2 = y *^{G} Inv(c, G).
          Inv(g2, G) = c *^{G} Inv(y, G).
          Inv(y, G) *^{G} g1 = Inv(b, G).

  Therefore Inv(g2, G) *^{G}  g1 = c *^{G} (Inv(b, G)).
qed.


Lemma.
Let H be a subgroup of G.
Let g1, g2 be elements of El(G).
If Inv(g2, G) *^{G} g1 << H
Then Coset(g1, H, G) = Coset(g2, H, G).
Proof.
Assume Inv(g2, G) *^{G} g1 << H.

Every element of Coset(g1, H, G) is an element of Coset(g2, H, G).
Proof.
  Let y be an element of Coset(g1, H, G).
  Take a << H such that y = g1 *^{G} a.
  (Inv(g2, G) *^{G}  g1) *^{G}  a << H.
  Then y = g1 *^{G}  a = g2 *^{G} ((Inv(g2, G) *^{G}  g1) *^{G}  a).
end.

Every element of Coset(g2, H, G) is an element of  Coset(g1, H, G).
Proof.
  Let y be an element of Coset(g2, H, G).
  Take a << H such that y = g2 *^{G} a.
  (Inv(g2, G) *^{G}  g1) *^{G}  a << H.
  Then y = g2 *^{G} a =g1 *^{G} ((Inv(g1, G)*^{G} g2)*^{G} a).
end.

Therefore Coset(g1, H, G) = Coset(g2, H, G).
Qed.

Lemma CosEq.
Let H be a subgroup of G.
Let g1, g2 be elements of El(G).
If Coset(g1, H, G) and  Coset(g2, H, G) are not disjunct
```

```
then Coset(g1, H, G) = Coset(g2, H, G).

Lemma.
Let H be a subgroup of G.
Let g1, g2 be elements of El(G).
Inv(g2, G)*^{G} g1 << H iff Coset(g1, H, G) = Coset(g2, H, G).

Definition.
Let H be a subgroup of G.
Cosets(H, G) = {Coset(g, H, G) | g << El(G)}.

[synonym coset/-s]
Let a coset of H in G denote an element of Cosets(H, G).

Lemma.
Let U be a subgroup of G.
El(G) = \-/ Cosets(U, G).
Proof.
Let us show that every element of El(G) is an element of \-/ Cosets(U, G).
  Let g be an element of El(G).
  g is an element of Coset(g, U, G).
end.

Let us show that every element of \-/ Cosets(U, G) is an element of El(G).
  Let h be an element of \-/ Cosets(U, G).
  Take an element k of El(G) such that h is an element of Coset(k, U, G).
  Coset(k, U, G) is a subset of El(G).
  Hence h is an element of El(G).
end.

Therefore El(G) = \-/ Cosets(U, G).
Qed.

Lemma.
Let G be a group.
Let U be a subgroup of G.
Cosets(U, G) is a disjunct collection.
Proof.
Let us show that for every elements N1, N2 of Cosets(U, G) N1 = N2 or (N1 and N2 are
    disjunct).
  Let N1, N2 be cosets of U in G.
  Take elements g1, g2 of El(G) such that N1 = Coset(g1, U, G) and N2 = Coset(g2, U,
    G).
  If N1 and N2 are not disjunct then N1 = N2 (by CosEq).
  Therefore the thesis.
end.
Qed.
```

```
Lemma.
Let G be a group.
Let U be a subgroup of G.
U is a coset of U in G.
Proof.
  We have U = Coset(One(G), U, G).
  Therefore the thesis.
Qed.
```

Nun führen wir den Begriff der Konjugation ein.

```
Definition.
Let g be an element of El(G).
Let U be a subgroup of G.
Conjugate(g, U, G) = {(g *^{G} (u *^{G} Inv(g, G)))| u is an element of U}.

Definition.
Let U, V be subgroups of G.
U and V are conjugates in G iff there is an element g of El(G) such that U =
    Conjugate(g, V, G).
```

2.6 Zahlen

```
 [synonym integer/-s]
 [synonym number/-s]

 Signature Integers. An integer is a notion.

 Signature Naturals. A natural number is an integer.

 Let a,b,c,d,e,n,m stand for integers.

 Signature NatZero.  0 is a natural number.
 Signature NatOne.   1 is a natural number.

 Signature IntNeg.   -a is an integer.
 Signature IntPlus.  a + b is an integer.
 Signature IntMult.  a * b is an integer.

 Signature NatPot. Let b be a natural number.  a ^ b is an integer.

 Axiom NatPlus. If a and b are natural numbers then a + b is a natural number.
 Axiom NatMult. If a and b are natural numbers then a * b is a natural number.

 Signature NatLT. a < b is an atom.

 Let a is smaller than b stand for a < b.
```

```
Axiom TriCh.
a = b \/ a < b \/ b < a.

Axiom.
a < b iff a != b.

Let a - b stand for a + (-b).

Axiom NatSub.
If a < b then b - a is natural number.

Axiom AddAsso.      a + (b + c) = (a + b) + c.
Axiom AddComm.      a + b = b + a.
Axiom AddZero.      a + 0 = a = 0 + a.
Axiom AddNeg.       a - a = 0 = -a + a.

Axiom MulAsso.      a * (b * c) = (a * b) * c.
Axiom MulComm.      a * b = b * a.
Axiom MulOne.       a * 1 = a = 1 * a.

Axiom Distrib.      a * (b + c) = (a*b) + (a*c) and
     (a + b) * c = (a*c) + (b*c).

Axiom ZeroDiv.      a != 0 /\ b != 0 => a * b != 0.

Axiom PotInj.   Let p be an integer. Let n,m be natural numbers. (p ^ n = p ^  m) =>
    n = m.
Axiom PotAdd. Let p be an integer. Let n, m be natural numbers. p ^ (n + m) = (p ^ n
   ) * (p  ^ m).
Axiom PotNotZero. Let p be an integer. Let k be a natural number. p ^ k  != 0.


Lemma MulZero.      a * 0 = 0 = 0 * a.
Proof.
  a*(1+(-1)) = (a*1)+(a*(-1))=0.
Qed.

Lemma MulMinOne.    (-1) * a = -a = a * -1.
Proof.
  a+(-1 * a)= (1*a)+(-1 * a) = 0.
Qed.

Lemma IntCanc.
c != 0 /\ a * c = b * c => a = b.
Proof.
  Assume c != 0 /\ a * c = b * c.

  (1) (a+ (-b))*c = (a * c) + ((-b) * c) = 0.
```

```
  Therefore a - b = 0 (by ZeroDiv, 1).
Qed.

Let a is nonzero stand for a != 0.
Let p,q stand for nonzero integers.

[synonym divisor/-s] [synonym divide/-s]

Definition Divisor. A divisor of b is a nonzero integer a
     such that for some n (a * n = b).

Let a divides b stand for a is a divisor of b.
Let a | b stand for a is a divisor of b.

Lemma DivPlus.
q | a /\ q | b =>  q | (a + b).

Definition EquMod.  a = b (mod q) iff q | a-b.

Definition NeqMod.  a != b (mod q) iff not (a = b (mod q)).

Lemma EquModRef.    a = a (mod q).

[ontored on]
Lemma EquModSym.    a = b (mod q) => b = a (mod q).
Proof.
 Assume that a = b (mod q).
 (1) Take n such that q * n = a - b.
 q * -n .= (-1) * (q * n) (by MulMinOne, MulAsso,MulComm,MulBubble)
       .= (-1) * (a - b) (by 1).
 Therefore q | b-a.
qed.

Lemma EquModTrn.    a = b (mod q) /\ b = c (mod q) => a = c (mod q).
Proof.
 Assume that a = b (mod q) /\ b = c (mod q).
 Take n such that q * n = a - b.
 Take m such that q * m = b - c.
 We have q * (n + m) = a - c.
qed.

Lemma EquModMul. a = b (mod p * q) => a = b (mod p) /\ a = b (mod q).
Proof.
 Assume that a = b (mod p * q).
 Take m such that (p * q) * m = a - b.
 We have p * (q * m) = a - b = q * (p * m).
qed.
```

```
[/ontored]
```

2.7 Primzahlen

Primzahlen.

Wichtigste Eigenschaft, das erste Axiom.

```
Signature Prime.    a is prime is an atom.

Let a prime stand for a prime nonzero integer.

Axiom.
Let n be a natural number.
Let p be a prime.
Let k be a natural number.
If k | p^n then k = 1 or p | k.

Axiom.
Let k be a natural number.
k != 0 => p | p^k.
```

2.8 Ein Lemma über Potenzen

Das folgende Lemma wird eine zentrale Rolle im Beweis des zweiten Teiles des Satzes einnehmen.

Wir liefern einen Beweis. In diesem wird deutlich, dass sich Symmetrie argumente nicht im deklarativen Stil des Naproche umsetzen lassen.

```
Lemma DLogN.
Let p be a prime.
Let a, b be natural numbers.
If n = (p^a)*c /\ n = (p^b)*d and p does not divide c and p does not divide d then a
    = b.
Proof.
Assume n = (p^a)*c and n = (p^b)*d and p does not divide c and p does not divide d.

b is not smaller than a.
Proof by Contradiction.
  Assume b < a.
  We have p^a = (p^(a-b))*(p^b).

  (1) (p^a)*c = (p^b)*d.
  (2) ((p^(a-b))*(p^b))*c = (p^b)*d.
  (3) ((p^b)*(p^(a-b)))*c = (p^b)*d (by 1, MulComm).
  (4) (p^b)*((p^(a-b))*c) = (p^b)*d (by 3, MulAsso).
  (5) ((p^(a-b))*c)*(p^b) = d*(p^b) (by 4, MulComm).
```

```
  (6)((p^(a-b))*c) = d (by 5, IntCanc, PotNotZero).

  a-b != 0.

  p is a divisor of p^(a-b).
  p is a divisor of ((p^(a-b))*c).

  p does divide d.
  p does not divide  d.

  Contradiction.
end.

a is not smaller than b.
Proof by Contradiction.
  Assume a < b.
  We have p^b = (p^(b-a))*(p^a).

  (1) (p^b)*d = (p^a)*c.
  (2) ((p^(b-a))*(p^a))*d = (p^a)*c.
  (3) ((p^a)*(p^(b-a)))*d = (p^a)*c (by 1, MulComm).
  (4) (p^a)*((p^(b-a))*d) = (p^a)*c (by 3, MulAsso).
  (5) ((p^(b-a))*d)*(p^a) = c*(p^a) (by 4, MulComm).

  (6)((p^(b-a))*d) = c (by 5, IntCanc, PotNotZero).

  b-a != 0.

  p is a divisor of p^(b-a).
  p is a divisor of ((p^(b-a))*d).

  p does divide c.
  p does not divide  c.

  Contradiction.
end.

Therefore the thesis.
qed.
```

2.9 Endliche Mengen

Endliche Mengen und deren Eigenschaften führen wir auch axiomatisch und abstrakt ein.

Betrachte Abschnitt für eine examplerische konstruktive Einführung des Kardinalitätsbegriffes.

```
Signature.
A finite set is a set.

Axiom.
Let M be a finite set.
Let N be a subset of M.
N is a finite set.

Axiom.
Let f be a function such that Dom(f) is a finite set.
Range(f) is a finite set.

Axiom.
Let M, N be finite set.
Prod(M, N) is a finite set.

Signature.
Let M be a finite set.
card(M) is a natural number.

Axiom.
Let M be a finite set.
Let N be a subset of M.
If card(M) = card(N) then M = N.

Axiom.
Let M be a set such that for all elements N of M N is a finite set.
\-/ M is a finite set.

Axiom.
Let N1, N2 be finite sets.
N1 \-/ N2 is a finite set.

Axiom.
Let N1, N2 be finite sets.
If N1 and N2 are disjunct then card(N1 \-/ N2) = card(N1) + card(N2).

Axiom cardUnion1.
Let M be a set.
Let N be an element of M.
If M is a finite set such that every element of M is a finite set
and M is a disjunct collection
and for all elements N1, N2 of M card(N1) = card(N2)
then card(\-/M) = card(N)*card(M).

Axiom cardUnion2.
Let M be a set.
```

```
Let k be an integer.
If M is a finite set such that every element of M is a finite set
and M is disjunct collection
and for all elements N of M k | card(N)
then k  |card(\-/ M).

Axiom.
Let N1, N2 be finite sets.
card(N1) = card(N2) iff there is a function f such that (f is from N1 to N2 and f is
    injective and f is surjective onto N2).

Axiom.
Let M be a finite set.
If card(M) != 0 then M is not empty.

Axiom.
Let M be a finite set.
card(M) = 1 iff there is y <<  M such that for all x << M x = y.

Axiom.
Let M be a finite set.
Assume 1 < card(M).
Let x be an element of M.
There is y <<  M such that x != y.
```

2.10 Der Satz von Lagrange

Der Satz von Lagrange ist grundlegend um über die Kardinalitäten von Gruppen und Untergruppen zu argumentieren.

```
Definition.
A finite group is a group G such that El(G) is a finite set.

Lemma.
Let G be a finite group.
Let U be a subgroup of G.
Cosets(U, G) is a finite set.
Proof.
  Define f[g] = Coset(g, U, G) for g in El(G).
  Cosets(U, G) is a subset of  Range(f).
  Therefore the thesis.
Qed.


Definition.
Let G be a finite group.
Let U be a subgroup of G.
```

```
Index(G, U) = card(Cosets(U, G)).

Lemma.
Let G be a finite group.
Let U, V be subgroups of G such that V and U are conjugates in G.
card(U) = card(V).
Proof.
Take an element g of El(G) such that V = Conjugate(g, U, G).
Define f[u] = g *^{G} (u *^{G} Inv(g, G)) for u in U.
Let us show that f is from U to V.
  Dom(f) = U.
  Let us show that for all elements u of U f[u] is an element of V.
    Let u be an element of U.
    f[u] is an element of V.
  end.
end.

Let us show that f is injective.
  Let us show that for all elements u1, u2 of U if f[u1] = f[u2] then u1 = u2.
     Let u1, u2 be elements of U such that f[u1] = f[u2].
     We have u1 = (Inv(g, G) *^{G}  (g *^{G} (u1 *^{G} Inv(g, G)))) *^{G} g.
     We have u2 = (Inv(g, G) *^{G}  (g *^{G} (u2 *^{G} Inv(g, G)))) *^{G} g.
     Therefore u1 = (Inv(g, G) *^{G}  f[u1]) *^{G} g = (Inv(g, G) *^{G}  f[u2]) *^{G}
     g = u2.
  end.
end.

Let us show that f is surjective onto V.
  Let us show that for every element v of V there is an element u of U such that f[u]
     = v.
    Let v be an element of V.
    We can take an element u of U such that v = (g *^{G} u) *^{G} Inv(g, G).
    Hence v = f[u].
  end.
end.
qed.

Theorem Lagrange.
Let G be a finite group.
Let U be a subgroup of G.
card(El(G)) = card(U)*card(Cosets(U, G)).
Proof.
Let us show that for all elements g of El(G) card(Coset(g, U, G)) = card(U).
  Let g be an element of El(G).
  Define f[u] = g *^{G} u for u in U.
  f is from U to Coset(g, U, G).
  f is injective.
  Proof.
```

```
    Let us show that for all  elements u1, u2 of U If f[u1] = f[u2] then u1 = u2.
      Let u1, u2 be elements of U such that f[u1] = f[u2].
      We have u1 = Inv(g, G) *^{G} (g *^{G} u1) = Inv(g, G) *^{G} (g *^{G} u2) = u2.
      Thus u1 = u2.
    end.

    Therefore the thesis.
  end.

  f is surjective onto Coset(g, U, G).
  Proof.
    Let us show that for every element y of Coset(g, U, G) there is an element u of U
     such that f[u] = y.
      Let y be an element of Coset(g, U, G).
      Take an element u of U such that y = g*^{G} u.
      Then f[u] = y.
    end.

    Therefore the thesis.
  end.
end.

(1) Cosets(U, G) is a disjunct collection and for all elements N1, N2 of Cosets(U, G)
     card(N1) = card(N2).
(2) Cosets(U, G) is a finite set such that for all element N1 of Cosets(U, G) N1 is a
     finite set.
(3) U is an element of Cosets(U, G).

Therefore card(\-/ Cosets(U, G)) = card(U)*card(Cosets(U, G)) (by cardUnion, 1, 2, 3)
    .
Qed.
```

2.11 Gruppenaktionen

Gruppenaktionen

```
Definition.
Let M be a set.
Let G be a group.
A group action from G on M is a function f
such that f is from Prod(El(G), M) to M
and (for every element x of M f[(One(G), x)] = x)
and for every element x of M for all elements a, b of El(G)
f[((a *^{G}  b), x)] = f[(a, f[(b, x)])].

Definition.
Let M be a set.
```

```
Let G be a group.
Let f be a function from Prod(El(G), M) to M.
Let x be an element of M.
Orbit(x, f, M, G) = { f[(a, x)] | a << El(G)}.


Definition.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
Let x << M.
Stab(x,f, M, G) = {y | y << El(G) and f[(y, x)] = x}.

Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
Let x << M.
Stab(x,f,M, G) is a subgroup of G.
Proof.

One(G) is an element of Stab(x, f, M, G).

Let us show that for all elements y, z of Stab(x, f, M, G)  z *^{G} Inv(y, G) << Stab
    (x, f, M, G).
  Let y, z be elements of Stab(x, f, M, G).
  We have f[(z *^{G} Inv(y, G), x)] = x.
  Therefore z *^{G} Inv(y, G) is an element of Stab(x, f, M, G).
end.

Therefore the thesis.
Qed.

Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
Let x << M.
Let g, h be elements of El(G).
If Coset(g, Stab(x, f, M, G), G) = Coset(h, Stab(x, f, M, G), G) then f[(g, x)] = f[(
    h, x)].
```

2.12 Stabilisator und Orbit

In FTL lässt sich nicht die Wohldefiniertheit von Funktionen nachweisen. Man könnte dies über Tupel + Axiome herleiten, dass führt jedoch weg von der natürlichen Art. Das vorangegangen Lemma begründet hier die Existenz der im folgenden Axiom geforderten Funktion.

```
Axiom.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
Let x << M.
There is a function h such that
h is from Cosets(Stab(x, f, M, G), G) to Orbit(x, f, M, G)
and (for all elements i of El(G) h[Coset(i,Stab(x, f, M, G),G)] = f[(i, x)]).

Lemma.
Let G be a finite group.
Let f be a group action from G on M.
Let x << M.
Orbit(x,f, M, G) is a finite set.
Proof.
  Define h[g] = f[(g, x)] for g in El(G).
  Dom(h) is a finite set.
  Orbit(x, f, M, G) is a subset of Range(h).
  Proof.
    Let us show that every element of Orbit(x, f, M, G) is an element of Range(h).
       (1) Let y be an element of Orbit(x, f, M, G).

       We can take an element g1 of El(G) such that y = f[(g1, x)] (by 1).

       Thus y is an element of Range(h).
    end.
  end.
  Therefore Orbit(x, f, M, G) is a finite set.
Qed.

Lemma.
Let M be a set.
Let G be a finite group.
Let f be a group action from G on M.
Let x << M.
Index(G, Stab(x, f, M, G)) = card(Orbit(x, f, M, G)).
Proof.

Take a function h such that
h is from Cosets(Stab(x, f, M, G), G) to Orbit(x, f, M, G)
and (for all elements i of El(G) h[Coset(i,Stab(x, f, M, G),G)] = f[(i, x)]).

h is surjective onto Orbit(x, f, M, G).
Proof.
  Let us show that for every element y of Orbit(x, f, M, G) there is an element z of
    Dom(f) such that f[z] = y.
    Let y be an element of Orbit(x, f, M, G).
```

```
    Take an element i of El(G) such that f[(i, x)] = y.
    Then we have h[Coset(i,Stab(x, f, M, G),G)] = y.
  end.
end.

h is injective.
Proof.
  Let us show that for all elements h1, h2 of Cosets(Stab(x, f, M, G), G) if h[h1] =
    h[h2] then h1 = h2.
    Let h1, h2 be elements of Cosets(Stab(x, f, M, G), G) such that h[h1] =h[h2].

    Take elements g1, g2 of El(G) such that h1 = Coset(g1,Stab(x, f, M, G),G) and h2
    = Coset(g2, Stab(x, f, M, G),G).

    Then f[(g1, x)] = f[(g2, x)].
    f[((Inv(g2, G) *^{G} g1), x)] = f[((Inv(g2, G)*^{G} g2), x)] = x.

    Thus Inv(g2, G) *^{G} g1 is an element of Stab(x, f, M, G).
    Therefore h1 = h2.
  end.
end.
qed.
```

2.13 Fipunkte

Fixpunkt Lemma.

```
Definition.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
A fixed point of f on M on G is an element y of M such that
for every element a of El(G) f[(a, y)] = y.

Definition.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
fixedPoints(f, M, G) = {y | y is a fixed point of f on M on G}.

Lemma.
Let M be a finite set.
Let G be a group.
Let f be a group action from G on M.
fixedPoints(f, M, G) is a finite set.
Proof.
  Let us show that  every fixed point of f on M on G is an element of M.
 Let x be a fixed point of f on M on G.
```

```
 Then x is an element of M.
  end.

   fixedPoints(f, M, G) is a subset of M.

   Therefore the thesis.
Qed.

Lemma.
Let M be a set.
Let G be a finite group.
Let f be a group action from G on M.
Let x be an element of M.
x is a fixed point of f on M on G iff card(Orbit(x, f, M, G)) = 1.


Lemma OrbitsIntersect.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
Let x1, x2 be elements of M such that Orbit(x1, f, M, G) and Orbit(x2, f, M ,G) are
   not disjunct.
x1 is an element of Orbit(x2,  f, M, G).
Proof.
Take y <<  M such that y << Orbit(x1, f, M, G) and y << Orbit(x2, f, M, G).
Take g1 << El(G) such that f[(g1, x1)] = y.
Take g2 << El(G) such that f[(g2, x2)] = y.

x1 = f[(Inv(g1, G) *^{G} g1, x1)] = f[(Inv(g1, G), y)] = f[(Inv(g1, G) *^{G} g2, x2)
   ].

Therefore the thesis.
Qed.

Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
Let x1, x2 be elements of M such that Orbit(x1,  f, M, G) and Orbit(x2,  f, M, G)
   are not disjunct.
Orbit(x1,  f, M, G) = Orbit(x2, f, M, G).
Proof.
Let us show that every element of Orbit(x1,  f, M, G) is an element of Orbit(x2,  f,
    M, G).
  Let x3 be an element of Orbit(x1,  f, M, G).
  x1 is an element of Orbit(x2,  f, M, G) (by OrbitsIntersect).
  Thus x3 is an element of Orbit(x2,  f, M, G).
end.
```

```
Let us show that every element of Orbit(x2, f, M, G) is an element of Orbit(x1,  f,
   M, G).
  Let x3 be an element of Orbit(x2, f, M, G).
  x2 is an element of Orbit(x1,  f, M, G) (by OrbitsIntersect).
  Thus x3 is an element of Orbit(x1,  f, M, G).
end.
Qed.

Definition.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
OrbitsNotFix(f, M, G) = {Orbit(x,  f, M, G) | x is an element of M and x is not a
   fixed point of f on M on G}.

Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
OrbitsNotFix(f, M, G) is a disjunct collection.

Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
\-/ OrbitsNotFix( f, M, G) = M \\ fixedPoints(f, M, G).
Proof.
Let us show that every element of \-/ OrbitsNotFix( f, M, G) is an element of  M \\
   fixedPoints(f, M, G).
  Let x be an element of  \-/ OrbitsNotFix( f, M, G).
  Take an element y of M such that x is an element of Orbit(y,  f, M, G) and y is
   not an element of fixedPoints(f, M, G).
  x is an element of M.
  x is not a fixed point of f on M on G.
  fixedPoints(f, M , G) is a subset of M.
  Therefore  x is an element of M \\ fixedPoints(f, M, G).
end.

Let us show that every element of M \\ fixedPoints(f, M, G) is an element of  \-/
   OrbitsNotFix( f, M, G).
  Let x be an element of M \\ fixedPoints(f, M , G).
  x is an element of M.
  x is not a fixed point of f on M on G.
  Orbit(x, f, M, G) is an element of OrbitsNotFix( f, M, G).
  x is an element of Orbit(x,  f, M, G).
  Therefore  x is an element of  \-/ OrbitsNotFix( f, M, G).
end.
qed.
```

```
Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
\-/  OrbitsNotFix( f, M, G) and fixedPoints(f, M, G) are disjunct.

Lemma.
Let M be a set.
Let G be a group.
Let f be a group action from G on M.
(\-/ OrbitsNotFix( f, M, G)) \-/ fixedPoints( f, M, G) = M.

Lemma.
Let M be a finite set.
Let G be a finite group.
Let f be a group action from G on M.
OrbitsNotFix( f, M, G) is a finite set.
Proof.
Define h[x] = Orbit(x,  f, M, G) for x in M.

OrbitsNotFix( f, M, G) is a subset of Range(h).
Qed.

Lemma.
Let M be a finite set.
Let G be a finite group.
Let f be a group action from G on M.
card(M) = card(( \-/ OrbitsNotFix( f, M, G)) \-/ fixedPoints( f, M, G))
= card(fixedPoints(f, M, G)) + card(\-/ OrbitsNotFix( f, M, G)).

Signature.
Let p be a prime.
A group of order p is a finite group H such that
(there is a natural number n such that card(El(H)) = p ^ n).

Lemma.
Let M be a finite set.
Let p be a prime.
Let G be a group of order p.
Let f be a group action from G on M.
card(fixedPoints(f, M, G)) = card(M) (mod p).
Proof.

\-/ OrbitsNotFix(f, M, G) is a subset of M.

Let us show that p | card( \-/  OrbitsNotFix( f, M, G)).
```

```
  Let us show that for all elements N1 of OrbitsNotFix( f, M, G) p | card(N1).

 Let N be an element of OrbitsNotFix( f, M, G).

 Take an element x of M such that N = Orbit(x, f, M, G).

 Let us show that card(N) != 1.
   Assume the contrary.

   x is not a fixed point of f on M on G .
   x is an element of N.
   Thus x is a fixed point of f on M on G.

   Contradiction.
 end.

 We have card(N) = Index(G, Stab(x, f, M, G)).
 Hence card(El(G)) = card(Stab(x,  f, M, G))*card(N) and card(N) | card(El(G)).
 Therefore p | card(N).
  end.

  (1) OrbitsNotFix( f, M, G) is a finite set such that every element of OrbitsNotFix
   ( f, M, G) is a finite set.
  (2) OrbitsNotFix( f, M, G) is a disjunct collection and for all elements N of
   OrbitsNotFix( f, M, G) p | card(N).

  Therefore  p | card(\-/ OrbitsNotFix( f, M, G)) (by cardUnion2, 1, 2).
end.

We have card(M) = card(fixedPoints(f, M, G)) + card(\-/ OrbitsNotFix( f, M, G)).

Therefore  card(M) = card(fixedPoints(f, M, G)) (mod p).
qed.
```

2.14 Eine Gruppenaktion

```
Lemma.
Let P be a subgroup of G.
Let U be a subgroup of G.
Let u be an element of U.
Let x, y be elements of El(G) such that Coset(x, P, G) = Coset(y, P, G).
Every element of Coset(u *^{G} x, P, G) is an element of  Coset(u *^{G} y, P, G).
Proof.
    Let i be an element of Coset(u *^{G} x, P, G).
    Take an element p of P such that i =  (u *^{G} x) *^{G} p.
    Then we have Inv(u, G) *^{G} i = Inv(u, G) *^{G} ((u *^{G} x) *^{G} p)
     =((Inv(u, G) *^{G} u ) *^{G} x) *^{G} p
```

```
    = x *^{G} p.
    Inv(u, G) *^{G} i is an element of Coset(x, P, G).
    Therefore Inv(u, G) *^{G} i is an element of Coset(y, P, G)
    and i is an element of Coset(u *^{G} y, P, G).
qed.

Lemma.
Let P be a subgroup of G.
Let U be a subgroup of G.
Let u be an element of U.
Let x, y be elements of El(G) such that Coset(x, P, G) = Coset(y, P, G).
Coset(u *^{G} x, P, G) = Coset(u *^{G} y, P, G).
Proof.
  Every element of Coset(u *^{G} x, P, G) is an element of  Coset(u *^{G} y, P, G).
  Every element of Coset(u *^{G} y, P, G) is an element of  Coset(u *^{G} x, P, G).

  Therefore the thesis.
Qed.
```

Aufgrund des vorangegangen Lemmas führt die folgende Definition nicht zu Problemen hinsichtlich der "Konsistenz".

```
Definition.
Let P be a subgroup of G.
Let U be a subgroup of G.
Op(U, P, G) is a function f
such that f is from Prod(El(Gr(U, G)), Cosets(P, G)) to Cosets(P, G) and
for all elements u of U for all elements x of El(G)
f[(u, Coset(x, P, G))] = Coset(u *^{G}  x,P, G).

Lemma.
Let P be a subgroup of G.
Let U be a subgroup of G.
Op(U, P, G) is a group action from Gr(U, G) on Cosets(P, G).
Proof.
Take a function f such that f = Op(U, P, G).
Take a group H such that  H = Gr(U, G).
Take a set M such that M = Cosets(P, G).

For every element x of M we have f[(One(H), x)] = x.

Let us show that for every element x of M for all elements a, b of El(H)
 f[(a *^{H} b, x)] =  f[(a,  f[(b, x)])].
  Let x be an element of M.
  Let a, b be elements of El(H).

  Take an element g of El(G) such that x = Coset(g, P, G).

  We have f[(b, x)] = Coset(b *^{G} g,P, G).
```

```
  f[(a, f[(b, x)])] = Coset(a *^{G} (b *^{G} g),P, G).

  f[(a *^{H}  b, x)] = Coset((a *^{G} b)*^{G} g,P, G).

  Thus f[(a, f[(b, x)])] = f[(a *^{H} b, x)].
end.

Therefore the thesis.
Qed.
```

2.15 Vorbereitung für den zweiten Satz von Sylow

```
Signature.
Let p be a prime.
A subgroup of G of order p is a subgroup U of G such that
Gr(U, G) is a group of order p.

Definition.
Let p be a prime.
Let G be a finite group.
Syl(p, G) = {P | P is a subgroup of G of order p and  not (p | Index(G, P))}.

Lemma SylSize.
Let p be a prime.
Let G be a finite group.
Let P, U be elements of Syl(p, G).
card(U) = card(P).
Proof.
Take natural numbers n, m such that p^n = card(U) and p^m = card(P).

(1) card(El(G)) = (p^n)*Index(G, U)
  and card(El(G)) = (p^m)*Index(G, P)
  and p does not divide Index(G, U)
  and p does not divide Index(G, P).

Thus we have n = m (by DLogN, 1).

Therefore the thesis.
Qed.
```

2.16 Der zweite Satz von Sylow

Der Satz von Sylow

```
Theorem Sylow2a.
Let p be a prime.
Let G be a finite group.
```

```
Let P be an element of Syl(p, G).
Let U be a subgroup of G of order p.
There is an element g of El(G) such that Conjugate(g, U, G) is a subset of P.
Proof.
  Take a group action f from Gr(U, G) on Cosets(P, G) such that f = Op(U, P, G).

  Let us show that card(fixedPoints(f, Cosets(P, G), Gr(U, G))) !=  0.
  We have card(fixedPoints(f, Cosets(P, G), Gr(U, G))) = Index(G, P) (mod p).
    p does not divide Index(G, P).
  Therefore Index(G, P) != 0 (mod p).
  end.

  We can take an element x of fixedPoints(f, Cosets(P, G), Gr(U, G))
  and an element g of El(G) such that x = Coset(g, P, G).

  Let us show that every element of Conjugate(Inv(g, G), U, G) is an element of P.
 Let h  be an element of Conjugate(Inv(g, G), U, G).

 Take an element u of U such that h = Inv(g, G) *^{G} (u *^{G}  g).

 We have Coset(g, P, G) = f[(u,x)] = Coset((u *^{G} g) ,P, G).

 Therefore Inv(g, G) *^{G} (u *^{G}  g) is an element of P.

 Thus h is an element of P.
  end.
Qed.

Theorem Sylow2b.
Let p be a prime.
Let G be a finite group.
Let P, U be elements of Syl(p, G).
P and U are conjugates in G.
Proof.
  Take an element g of El(G) such that Conjugate(g, U, G) is a subset of P.

  card(Conjugate(g, U, G)) = card(U) = card(P).

  Hence Conjugate(g, U, G) = P.
qed.
```

3 Anmerkungen zur Formalisierungen in Naproche

3.1 Dateistruktur

Kleine Theorien (Ansatz auch in der Mathematik zu finden In einem fortgeschritteren Beweis der komplexen Analysis werden viele Eingeschaften der Reellen Zahlen als bekannt vorraus-

gesetzt..)

3.2 Definition der Gruppe über Funktionen

Unsere Definition ermöglicht nicht, für bestimmte Gruppen zu zeigen, dass etwas eine Gruppe ist. Das fehlen von algebraischen Strukturen

Hier ist im arbeiten an unserem Projket insbesondere aufgefallen, dass das arbeiten mit Funktionen ind

3.3 Wohldefiniertheit von Funktionen

Funktionen nicht optimal fällt insbesondere auf. So ist es zwar möglich, Funktionen innerhalb von Beweisen zu definieren, jedoch auf Allgemeinerer Ebene nicht. An zwei Schritten im Beweis ist dies notwendig. In weiterer Entwicklung von Naproche wäre es hier sinnvoll, einen Mechanismus zum definierne von Funktionen / des verifizierrens der Wohldefiniertheit selbiger zu ermöglichen.

3.4 Kardinalitäten durch natürliche Zahlen mit Induktion

Ähnlich wie die Gruppen, haben wir auch Kardinalitäten auf einer sehr abstrakten Ebene eingfeführt.

3.5 Ganze Zahlen + Möglichkeit der Umsetzuung innerhalb unserer Dateistruktur

Im Sinne der Vervollständigung unsere Formalisierung wäre es in einem weiteren Projekt sicherlich auch sinnvoll, eine Bibliothek über ganze Zahlen / .. zu de

3.6 Konventionen

Ein Beispiel : Formalisieren wir das was wir formalisieren wollen?

Informatik : Bibliotheken und Einbindung.

4 Formalisierung in Lean

Woher kommt die Datei?

5 Vergleich

5.1 Direkte Gegenüberstellung

5.1.1 Mathematik

(i) Sei $X := G/P$. Dann ist

$$\phi : U \times X \to X$$

eine Gruppenaktion. Nach einem Lemma gilt dann

$$|X^U| = |X| mod p$$

Da p kein Teiler von $|X|$ ist, gilt $X^U \neq \varnothing$. Es gibt also ein $g \in G$ mit

$$ugP = P$$

für alle $u \in U$. Es folgt dann $g^{-1}ug$ für alle $u \in U$.

(ii) Alle p-Sylowgruppen von G haben nach Definition die gleiche Ordnung. Daher folgt aus (ii) direkt (i).

5.1.2 Naproche

```
Proof.
Take a group action f from Gr(U, G) on Cosets(P, G) such that f = Op(U
   , P, G).

Let us show that card(fixedPoints(f, Cosets(P, G), Gr(U, G))) !=  0.
  We have card(fixedPoints(f, Cosets(P, G), Gr(U, G))) = Index(G, P) (
  mod p).
    p does not divide Index(G, P).
 Therefore Index(G, P) != 0 (mod p).
end.

We can take an element x of fixedPoints(f, Cosets(P, G), Gr(U, G))
and an element g of El(G) such that x = Coset(g, P, G).

Let us show that every element of Conjugate(Inv(g, G), U, G) is an
  element of P.
  Let h  be an element of Conjugate(Inv(g, G), U, G).

  Take an element u of U such that h = Inv(g, G) *^{G} (u *^{G}  g).

   We have Coset(g, P, G) = f[(u,x)] = Coset((u *^{G} g) ,P, G).

  Therefore Inv(g, G) *^{G} (u *^{G}  g) is an element of P.

  Thus h is an element of P.
end.
Qed.
```

5.1.3 LEAN

```
lemma sylow_2 [fintype G] {p : ℕ} (hp : nat.prime p)
(H K : set G) [is_sylow H hp] [is_sylow K hp] :
∃ g : G, H = conjugate_set g K :=

have hs : card (left_cosets K) = card G / (p ^ dlogn p (card G)) :=
(nat.mul_right_inj (pos_pow_of_pos (dlogn p (card G)) hp.pos)).1
$ by rw ←[ card_sylow K hp, ← card_eq_card_cosets_mul_card_subgroup,
  card_sylow K hp,
nat.div_mul_cancel (dlogn_dvd _ hp.1)],

have hmodeq : card G / (p ^ dlogn p (card G)) ≡ card (fixed_points H (
  left_cosets K)) [MOD p] :=
eq.subst hs (mul_action.card_modeq_card_fixed_points hp (card_sylow H
  hp)),

have hfixed : 0 < card (fixed_points H (left_cosets K)) := nat.
  pos_of_ne_zero
(λ h, (not_dvd_div_dlogn (fintype.card_pos_iff.2 ⟨(1 : G)⟩) hp.1)
(by rwa [h, nat.modeq.modeq_zero_iff] at hmodeq)),


let ⟨⟨x, hx⟩⟩ := fintype.card_pos_iff.1 hfixed in
begin

revert hx,

refine quotient.induction_on x
(λ g hg, ⟨g, set.eq_of_card_eq_of_subset _ _⟩),
{
rw [conjugate_set_eq_image, set.card_image_of_injective _
  conj_inj_left,
card_sylow K hp, card_sylow H hp] },
{
assume y hy,
have : (y⁻¹ * g)⁻¹ * g ∈ K :=
quotient.exact ((mem_fixed_points' (left_cosets K)).1 hg ⟦y⁻¹ * g⟧
⟨⟨y⁻¹, inv_mem hy⟩, rfl⟩),
simp [conjugate_set_eq_preimage],
simp only [*, mul_assoc, mul_inv_rev] at *,
simp [*, inv_inv] at *}
end
```

Ähnlichkeiten, Mathematik, Naproche + Latex einbindung + Implizite Typerkennung wie sie in Lean erfolgt.

6 Diskussion

7 Bibliographie