Lecture 07: Semi-direct product

Friday, October 19, 2018 2:05 AM

Two important observations:

- If $f \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ is the trivial homomorphism (that means $f(h) = \mathrm{id}_N$ $\forall h \in H$), then $H \ltimes_f N = H \times N$:
(as groups)

$$(h_1, n_1) \cdot (h_2, n_2) = (h_1 h_2, f(h_2^{-1})(n_1) n_2)$$
$$= (h_1 h_2, n_1 n_2).$$

- If $f \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ is non-trivial, then $H \ltimes_f N$ is not abelian;

  Since f is not trivial, $\exists\, h \in H$, $n \in N$ s.t. $f(h)(n) \neq n$.

  Then $(h, 1)(1, n) = (h, n)$
  $$\#$$
  $(1, n)(h, 1) = (h, f(h^{-1})(n))$.

- Let G be a group of order pq where $p < q$ are prime. We have proved that $\exists\, Q \trianglelefteq G$, $|Q| = q$, $\exists\, P \leq G$, $|P| = p$. And so $G/Q \simeq \mathbb{Z}/p\mathbb{Z} \simeq P$, which implies there is a split S.E.S. $1 \to \mathbb{Z}/q\mathbb{Z} \to G \to \mathbb{Z}/p\mathbb{Z} \to 1$.

Lecture 07: Groups of order pq

Friday, October 19, 2018 2:15 AM

And so $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_f \mathbb{Z}/q\mathbb{Z}$ for some

$f \in \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}))$.

<u>Ex.</u> $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, where $\theta_a(x+n\mathbb{Z}) := ax+n\mathbb{Z}$

$\theta_a \longleftarrow a+n\mathbb{Z}$

(<u>Outline of pf.</u> $\theta(\bar{1})$ is a generator of $\mathbb{Z}/n\mathbb{Z}$; so $o(\theta(\bar{1})) = n$ which implies $\gcd(\theta(\bar{1}), n) = 1$. Hence $\theta(\bar{1}) \in (\mathbb{Z}/n\mathbb{Z})^\times$.)

<u>Ex.</u> $(\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ if q is prime.

(This is true for any finite field as we will learn later.)

So we need to understand $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/(q-1)\mathbb{Z})$.

<u>Claim.</u> • If $p \nmid q-1$, then $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/(q-1)\mathbb{Z}) = 0$;

• If $p \mid q-1$, then there are non-trivial elements in $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/(q-1)\mathbb{Z})$.

<u>Pf of Claim.</u> $\forall f \in \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/(q-1)\mathbb{Z})$,

$o(f(1+p\mathbb{Z})) \mid \gcd(p, q-1)$. So, if $p \nmid q-1$, f is trivial.

Lecture 07: Groups of order pq

Friday, October 19, 2018 8:41 AM

If $p \mid q-1$, then $\frac{q-1}{p} + (q-1)\mathbb{Z}$ is an element of order p

and so $f: \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$, $f(a+p\mathbb{Z}) = a\left(\frac{q-1}{p}\right) + (q-1)\mathbb{Z}$

is a non-trivial group homomorphism. $\blacksquare$

<u>Corollary</u>. (a) If $p \nmid q-1$, then any group of order pq is cyclic.

(b) If $p \mid q-1$, then there is a non-abelian gp of order pq.

Pf (a) $G \simeq \mathbb{Z}/p\mathbb{Z} \ltimes_f \mathbb{Z}/q\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$

f is trivial as $p \nmid q-1$

Chinese Remainder Thm

(b) $\exists$ a non-trivial $f \in \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}))$ and so $\mathbb{Z}/p\mathbb{Z} \ltimes_f \mathbb{Z}/q\mathbb{Z}$ is non-abelian. $\blacksquare$

Next we will mention Schur–Zassenhaus theorem which is a strong tool to show a S.E.S. splits.

Lecture 07: Schur-Zassenhaus theorem

Friday, October 19, 2018 8:54 AM

Schur-Zassenhaus Theorem. A S.E.S.

$$(*) \qquad 1 \to N \to G \to H \to 1$$

splits if $\gcd(|N|, |H|) = 1$.

In the lecture we will make a few reductions; and in your HW assignment you will finish the proof.

Step 1. It is enough to prove the following:

Suppose $N \trianglelefteq G$, $\gcd(|N|, |G/N|) = 1$. Then $\exists\, H \leq G$ s.t. $|H| = |G/N|$. $(\star)$

Pf of Step 1. For a given S.E.S. as in $(*)$, $\exists\, N' \trianglelefteq G$ s.t.

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, "\wr"] \arrow[dr, phantom, "\circlearrowleft"] & G \arrow[r] \arrow[d, "="] \arrow[dr, phantom, "\circlearrowleft"] & H \arrow[r] \arrow[d, "\wr"] & 1 \\
1 \arrow[r] & N' \arrow[r] & G \arrow[r] & G/N' \arrow[r] & 1
\end{tikzcd}$$

And so $|N| = |N'|$, $|H| = |G/N'|$, which implies $\gcd(|N'|, |G/N'|) = 1$.

By $(\star)$, $\exists\, H' \leq G$ s.t. $|H'| = |G/N'|$. Since $\gcd(|N'|, |H'|) = 1$, $N' \cap H' = 1$. And so $1 \to N' \to G \to G/N' \to 1$ splits; which implies $(*)$ splits. (why?) ∎

Lecture 07: Schur-Zassenhaus theorem

Friday, October 19, 2018 9:08 AM

So we will focus on proving the statement in the blue box; and we proceed by strong induction on $|G|$. We present proof in a backward fashion by making a few reductions and get to the case where N is abelian.

Step 2. For proving the strong induction step we can further assume that N is a minimal normal subgroup.

pf. of Step 2. Suppose N is not a minimal normal subgp. Then $\exists\, 1 \neq N_0 \subsetneq N$ s.t. $N_0 \lhd G$.

Claim. $N/N_0 \lhd G/N_0$ satisfy conditions of $(\star)$.

Pf of Claim.
$$\left.\begin{array}{l} |N/N_0| \mid |N| \\ [G/N_0 : N/N_0] = [G:N] \\ \gcd(|N|, [G:N]) = 1 \end{array}\right\} \Rightarrow \gcd(|N/N_0|, [G/N_0 : N/N_0]) = 1.$$
□

By the above claim, $|G/N_0| < |G|$, and strong induction hypothesis, $\exists\ \overline{H} \leq G/N_0$ s.t. $|\overline{H}| = [G/N_0 : N/N_0] = |G/N|$.

Therefore $\exists\ \widetilde{H} \leq G$ s.t. $\overline{H} = \widetilde{H}/N_0$. Hence $|\widetilde{H}/N_0| = |G/N|$.

As $|N_0| < |N|$, $|\widetilde{H}| < |G|$.

Lecture 07: Schur-Zassenhaus theorem

Friday, October 19, 2018 9:30 AM

<u>Claim</u> $N_0 \lhd \tilde{H}$ satisfy conditions of (★).

<u>Pf of Claim.</u>
$$\left.\begin{array}{l} |N_0| \mid |N| \\ |\tilde{H}/N_0| = |G/N| \\ \gcd(|N|, |G/N|) = 1 \end{array}\right\} \Rightarrow \gcd(|N_0|, |\tilde{H}/N_0|) = 1.$$

$\square$

By the above claim, $|\tilde{H}| < |G|$, and the strong induction hypothesis, $\exists\, H \leq \tilde{H} \leq G$ s.t. $|H| = |\tilde{H}/N_0| = |G/N|$.

<u>Step 3.</u> For proving the strong induction step we can further assume that N is a minimal normal subgroup and a <u>p-group</u>.

<u>Pf of Step 3.</u> Suppose $p \mid |N|$ and N is not a p-group. Let $P \in \mathrm{Syl}_p(N)$. Since $1 \neq P \lneq N$ and N is a minimal normal subgp of G, $P \ntrianglelefteq G$; and so $N_G(P) \lneq G$.

By Frattini's argument that you proved in your HW assignment, $G = N_G(P)\, N$. And so

$$G/N = N_G(P)N/N \simeq N_G(P)/N_G(P) \cap N.$$

Lecture 07: Schur-Zassenhaus theorem

Friday, October 19, 2018 9:49 AM

Claim. $N_G(P)\cap N \trianglelefteq N_G(P)$ satisfy conditions in (☆).

Pf of Claim.
$$\left.\begin{array}{c} |N_G(P)\cap N| \mid |N| \\ \left|N_G(P)/N_G(P)\cap N\right| = |G/N| \\ \gcd(|N|, |G/N|)=1 \end{array}\right\} \Rightarrow \gcd(|N_G(P)\cap N|, |N/N_G(P)\cap N|)=1.$$
$\square$

By the above claim, $|N_G(P)|<|G|$, and the strong induction hypothesis, $\exists\ H \le N_G(P) \le G$ s.t.
$$|H| = \left|N_G(P)/N_G(P)\cap N\right| = |G/N|.$$

Step 4. For proving the strong induction step we can further assume that N is a minimal normal subgroup, a p-group, and abelian.

Pf of Step 4. The following lemma implies this step.

Lemma. $N \trianglelefteq G \Rightarrow Z(N) \trianglelefteq G$.

Conjugation is an auto.

Pf of Lemma. $\forall g\in G$, $gZ(N)g^{-1} = Z(gNg^{-1}) = Z(N)$. $\square$

(In your HW, you will learn about characteristic subgps and show $K \le_{\text{char}} N$, $N \trianglelefteq G \Rightarrow K \trianglelefteq G$.)

Lecture 07: Schur-Zassenhaus theorem

Friday, October 19, 2018 9:58 AM

Corollary. If N is a minimal normal subgp of G and N is a finite p-group, then N is abelian.

Pf of Corollary. Since $1 \neq N$ is a finite p-group, $1 \neq Z(N)$. By the previous lemma, $Z(N) \triangleleft G$. By the minimality of N, we get that $N = Z(N)$. ∎

In your HW assignment you will learn about basics of cohomology and prove the abelian case of Schur-Zassenhaus theorem; and thereby finishing its proof.

So far to understand structure of a group, we tried to find a normal subgroup N, and having groups N and G/N tried to describe G. What if G does not have a non-trivial normal subgroup? Such a group is called a simple group. In the next few lectures we will work with the symmetric group S_n; and show it has a subgroup of index 2 that is simple (if $n \geq 5$).

Lecture 07: Symmetric group

Friday, October 19, 2018 3:07 PM

As we have pointed out earlier, $S_n \curvearrowright \{1,2,\dots,n\}$. And so for any $\sigma \in S_n$, $\langle\sigma\rangle \curvearrowright \{1,\dots,n\}$. The set of orbits gives us a partition of $[1..n] := \{1,2,\dots,n\}$.

__Def.__ Let $\mathrm{Fix}(\sigma) := \{ i \in [1..n] \mid \sigma(i) = i\}$, and

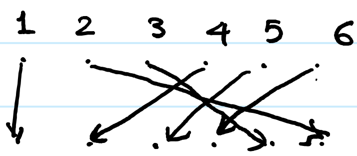
$$\mathrm{supp}(\sigma) := [1..n] \setminus \mathrm{Fix}(\sigma).$$

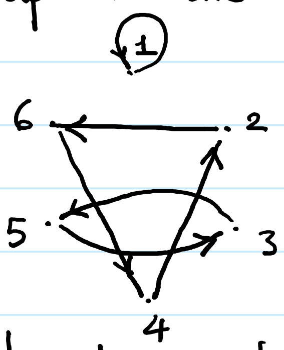
__Ex.__ $\mathrm{supp}(\mathrm{id.}) = \emptyset$; or $|\mathrm{supp}(\sigma)| \neq 1$.

__Observation.__ $\sigma(\mathrm{Fix}(\sigma)) = \mathrm{Fix}(\sigma)$ and so $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$.

And so $\mathrm{Supp}(\sigma)$ is invariant under $\langle\sigma\rangle$.

We can make a directed graph via the action of σ;

__Ex.__ 



$i \to \sigma(i)$

Since σ is a bijection, any vertex has an outgoing deg. 1; and an ingoing deg. 1.

So the undirected graph is a 2-regular graph. One can see that such a graph is a disjoint union of cycles.

So on each orbit σ acts like a "cycle".

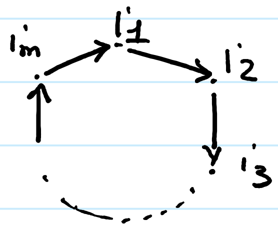
Lecture 07: Cycles; disjoint support

Friday, October 19, 2018 3:20 PM

<u>Def</u>. $\sigma \in S_n$ is called a cycle of length $\underline{m}$ if $\exists\, i_1, \ldots, i_m \in [1..n]$ s.t. $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \ldots,\ \sigma(i_m) = i_1$ and

$\sigma(j) = j$ if $j \in [1..n] \setminus \{i_1, \ldots, i_m\}$. In particular, if $m \neq 1$, then $\operatorname{supp} \sigma = \{i_1, \ldots, i_m\}$. We denote it by $(i_1\ i_2 \cdots i_m)$.

<u>Observation</u>. The directed graph attached to $(i_1\ i_2 \cdots i_m)$ consists of $n-m$ self-loops and



.

<u>Lemma</u>. Suppose $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$. Then $\sigma\tau = \tau\sigma$.

<u>Pf</u>. • $i \in \operatorname{Supp}(\sigma) \Rightarrow \sigma(i) \in \operatorname{Supp}(\sigma) \Rightarrow i, \sigma(i) \in \operatorname{Fix} \tau$

$$\Rightarrow \begin{cases} \tau(i) = i \\ \tau(\sigma(i)) = \sigma(i) \end{cases} \Rightarrow \tau(\sigma(i)) = \sigma(i) = \sigma(\tau(i)).$$

• Similarly for $i \in \operatorname{Supp}(\tau)$, $(\tau \circ \sigma)(i) = (\sigma \circ \tau)(i)$.

• If $i \notin \operatorname{Supp} \sigma \cup \operatorname{Supp} \tau$, then $i \in \operatorname{Fix} \sigma \cap \operatorname{Fix} \tau$; and so

$\tau \circ \sigma(i) = i = \sigma \circ \tau(i)$. ∎

Next we will show

Lecture 07: Disjoint supports

Friday, October 19, 2018 4:01 PM

<u>Lemma.</u> Suppose $\mathrm{supp}(\sigma_i) \cap \mathrm{Supp}(\sigma_j) = \emptyset$ if $i \neq j$. Then

(a) $\sigma_1 \sigma_2 \cdots \sigma_m \big|_{\mathrm{Supp}\,\sigma_i} = \sigma_i \big|_{\mathrm{Supp}\,\sigma_i}$;

(b) $\mathrm{Supp}(\sigma_1 \sigma_2 \cdots \sigma_m) = \bigcup_{i=1}^{m} \mathrm{supp}\,\sigma_i$.

(we will continue next time.)