D&F alternate proofs

inter 3.4.-3: For $S \subseteq G$, $(uS)v = u(Sv)$

Proof: $(uS)v = \{hv \ : \ h \in uS\} = \{usv \ : \ s \in S\} = \{ui \ : \ i \in Sv\} = u(Sv)$

So writing uSv is unambiguous. Similarly for uvS and Suv. Same .

inter 3.4.-2: For $S, T \subseteq G$, $gS = gT \iff S = T \iff Sg = Tg$

Proof: The right/left action of g on G is a permutation, so this follows from the invertibility of bijections.

inter 3.4.-1: For $S \subseteq G$, $h^{-1}g \in S \iff g \in hS$

Proof: $h^{-1}g \in S \implies \exists s \in S \ : \ h^{-1}g = s \implies g = hs \implies g \in hS$

$g \in hS \implies \exists s \in S \ : \ g = hs \implies h^{-1}g = s \Rightarrow h^{-1}g \in S$

Similarly, $gh^{-1} \in S \iff g \in Sh$

prop 3.4: $N \leq G \implies \{gN \ : \ g \in G\}$ and $\{Ng \ : \ g \in G\}$ are both partitions of G

Proof: Let $g \sim h$ to mean $g \in hN$

Then $\exists n \in N \ : \ g = hn \implies gn^{-1} = h \implies h \in gN \implies h \sim g$

Let $g \sim h$ and $h \sim i$, then $\exists n, m \in N \ : \ g = hn, \, h = im \implies g = imn \Rightarrow g \in iN \Rightarrow g \sim i$

$1 \in N \implies g \sim g$, so $\sim$ is an equivalence relation partitioning G

inter 3.4.1: For $N \leq G$, $uN = vN \iff u \in vN \iff v \in uN$

Proof: Follows from prop 3.4 and $1 \in N$.

Note we can restate the equivalence relation in the proof for 3.4 as $g \sim h \iff gN = hN$ now.

Similarly, $Nu = Nv \iff u \in Nv \iff v \in Nu$

inter 3.4.2: For $N \leq G$, $\forall n \in N, \ uN = unN$

Proof: $1 \in nN \iff N = nN \implies uN = unN$

inter 3.4.3: $\{gN \ : \ g \in G\} = \{Ng \ : \ g \in G\} \iff N \trianglelefteq G$

Proof: $\{gN \ : \ g \in G\} = \{Ng \ : \ g \in G\} \iff \forall g \in G, \ gN = Ng$ as $1 \in N$ and from prop 3.4.

$gN = Ng \iff \forall r \in gN \left(r \in Ng \iff rg^{-1} \in N \right) \iff gNg^{-1} = N$

(the outer $\iff$ arrows hold due to $S \subseteq G$, $gS \leftrightarrow S \leftrightarrow Sg$ being bijections)

prop 3.5: multiplication $uN \bullet vN = uvN$ is well defined $\iff N \trianglelefteq G$

Proof: Let $uN \bullet bN = uvN$ be well defined, i.e. for $u, v \in uN, \ b, d \in bN$, we have $ubN = vdN$. Then, $\forall g \in G, \left(\forall n \in N, \left(1gN = ngN \iff ng \in gN \iff g^{-1}ng \in N \right) \iff gNg^{-1} = N \right) \iff N \trianglelefteq G$

Conversely, $N \trianglelefteq G \implies \forall n, m \in N, \ unN \bullet vmN = unvmN = unNmv = uNv = uvN$.

Technically the first line suffices, but adding the extra variable makes it messy. And the converse is cool.

prop 3.13: For $H, K \leq G, \ |HK| = \dfrac{|H||K|}{|H \cap K|}$

Proof: $HK = \bigcup\limits_{h \in H} hK$, $\quad K \leq G$ means any two hK's are either disjoint or identical.

$h_1K = h_2K \iff h_2^{-1}h_1 \in K \iff h_2^{-1}h_1 \in H \cap K \iff h_1H \cap K = h_2H \cap K$

$\implies |HK| = \dfrac{|H|}{|H \cap K|}|K|$

prop 3.14: For $H, K \leq G, \quad HK \leq G \iff HK = KH$

coll 3.15: $H, K \leq G$ and $H \leq N_G(K) \iff HK \leq G$

Proof: $\forall h \in H, k \in K \left(hkh^{-1} \in K \implies hk \in Kh \in KH\right) \implies HK \subseteq KH$

Similarly, $kh = h(h^{-1}kh) \in hK \in HK \implies KH \subseteq HK$, so $KH = HK$.