Section 2.12 Exercises
Herstein's Topics In Algebra

Spencer T. Parkin

March 27, 2016

Thoughts On First Proof Of Sylow's First Theorem

It was left to the reader to show that $|G| = n|H|$. What we want to show is that H has exactly n right cosets in G. Since $H = \{g \in G | M_1 g = M_1\}$, we see that the every right-coset of H in G can be written as

$$Ha = \{g \in G | M_1 g a^{-1} = M_1\} = \{g \in G | M_1 g = M_1 a\}.$$

But now $M_1 a = M_i$ for some $1 \leq i \leq n$, and as a ranges over G, we get every M_i in $\{M_i\}_{i=1}^n$; so there are exactly n such cosets.

Other Thoughts

At the end, he uses Lemma 2.12.5 to say that the number of p-Sylow subgroups, which number has the form $1 + kp$, must divide the order of the group. This is not immediately obvious to me.

That this would be the case seems to follow from the proof of Theorem 2.12.3.

Problem 11

Let $|G| = pq$, p and q distinct primes, $p < q$.

Part A

Show that if p doesn't divide $q-1$, then G is cyclic.

Admittedly, without the sample analyses Herstein gives at the end of the chapter, I couldn't've figured this one out.

By Theorem 2.12.3, we have $1+kq$, for some integer k, as the number of q-Sylow subgroups of G, and $1+kq$ divides pq. Now since

$$(1+kq)(1)+q(-k)=1,$$

we see that $\gcd(1+kq,q)=1$, and therefore, $1+kq$ divides p. But now $p<q$, so we must have $k=0$ and the number of q-Sylow subgroups of G is one.

Turning our attention now to the number of p-Sylow subgroups of G, we see, again by Theorem 2.12.3, that there must be, for some integer k, $1+kp$ of them, and this divides pq. Again, it is easy to show that $1+kp$ and p are coprime; therefore, $1+kp$ must divide q, and so we write

$$r(1+kp)=q.$$

Now, if $k>0$, we must have $r=1$ since q is prime. We then have

$$kp=q-1,$$

but, by hypothesis, p does not divide $q-1$, so $k=0$ and the number of q-Sylow subgroups of G is just one.

What we know now is that there are at most $p-1$ elements of order p, and $q-1$ elements of order q. But this doesn't account for all non-identity elements; specifically,

$$(pq-1)-(p-1)-(q-1)=pq-p-q+1>0.$$

It follows that there must exist an element of order pq; hence, G is cyclic.

Part B

Show that if $p|(q-1)$, then there exists a unique non-abelian group of order pq.

I have no idea. Herstein also brings this up in section 10, problem 10 where more clues can be found. Clearly there is an existence and then a uniqueness portion to this. First show existence, then uniqueness through isomorphism.

We might consider the external direct product of two cyclic groups: one of order p, the other of q. This group has the right order. Is it non-abelian? No, it's abelian.