Section 2.11 Exercises
Herstein's Topics In Algebra

Spencer T. Parkin

March 23, 2016

Some Thoughts

It is interesting to observe that for any subgroup H of a group G, and any element $g \in G$, that $g^{-1}Hg$ is also a subgroup of G. If H is not normal in G, then there must exist $g \in G$ such that $g^{-1}Hg$ is some subgroup of G other than H.

For subgroups A and B of a group G, say that A is conjugate to B, and write this as $A \sim B$, if and only if there exists an element $g \in G$ such that $g^{-1}Ag = B$. Does this define an equivalence relation on the set S of all subgroups of G? Clearly, $A \sim A$ as $e^{-1}Ae = A$. And if $g^{-1}Ag = B$, we must have $(g')^{-1}Bg' = A$, where $g' = g^{-1}$; proving $B \sim A$. Lastly, $a^{-1}Aa = B$ and $b^{-1}Bb = C$ implies that

$$C = b^{-1}a^{-1}Aab = (ab)^{-1}Aab,$$

showing that $A \sim C$. It follows now from what we know about equivalence relations that

$$|S| = \sum |\mathrm{Cl}(A)|,$$

where here, the sum is taken over all equivalence class of S, and therefore, each A is just one of the possible representatives of each such class.

Let's consider for a moment a subgroup A of G for which $|\mathrm{Cl}(A)| = 1$. It is clear that if A is normal in G, then $|\mathrm{Cl}(A)| = 1$. What about the converse? If $|\mathrm{Cl}(A)| = 1$, then there does not exist an element $g \in G$ such that $g^{-1}Ag$ is some subgroup of G other than A. It follows, then, that $g^{-1}Ag = A$ for all $g \in G$, and therefore, A is normal in G. We can now say that if N is the number of subgroups normal in G, then

$$|S| = N + \sum |\mathrm{Cl}(A)|,$$

where here, each A is not normal in G. We return to this equation later.

Let's now consider, for any subgroup A of G, the normalizer of A; namely,

$$N(A) = \{g \in G | gAg^{-1} = A\}.$$

(This is the largest subgroup of G in which A is normal. See section 2.6, problem 10.) Notice that its right cosets take the form

$$N(A)a = \{g \in G | (ga^{-1})A(ga^{-1})^{-1} = A\} = \{g \in G | g(a^{-1}Aa)g^{-1} = A\}.$$

This makes it clear that the number of such cosets is precisely the number of conjugates of A. We can now say that

$$|\mathrm{Cl}(A)| = \frac{|G|}{|N(A)|}.$$

Now suppose G is a group of prime power order. Specifically, $|G| = p^n$. We then have

$$|S| = \sum \frac{|G|}{|N(A)|} = \sum \frac{p^n}{p^{n_A}} = N + \sum_{n_A < n} \frac{p^n}{p^{n_A}},$$

where for each arbitrarily chosen representative A of each conjugacy class, $p^{n_A} = |N(A)|$. (Notice that if A is not normal in G, then $|N(A)| < |G|$.) Interestingly, this shows that

$$|S| \equiv N \pmod{p}.$$

Looking ahead to Lemma 2.12.6, let's consider the number of p-Sylow subgroups of G. If P is a p-Sylow subgroup of G, then by Sylow's Second Theorem, $|Cl(P)|$ accounts for all p-Sylow subgroups in G. It follows immediately that the number of such groups in G is $|G|/|N(P)|$, where P is any such group.

Problem 11

Using Theorem 2.11.2 as a tool, prove that if $|G| = p^n$, p a prime number, then G has a subgroup of order p^α for all $0 \leq \alpha \leq n$.

We proceed by strong induction on n. The cases $n = 0$ and $n = 1$ are trivial. Assuming all cases $n-1, n-2, \ldots, 1, 0$, we must prove case $n \geq 2$. For our proof to work, we need only find any non-trivial, normal subgroup N of G. If G is non-abelian, we may let $N = Z(G)$ by Theorem 2.11.2. If G is abelian, then...ugh, think about it. In any case, let N be a non-trivial, normal subgroup of G of order p^m with $0 < m < n$. It then follows by our inductive hypothesis, that G has subgroups of orders p^i for $0 \leq i \leq m$. Now consider the factor group G/H. By a problem in Gallian's book (cite it here), for every subgroup K of G/N, there exists a subgroup H of G containing N such that $K = H/N$. And now since N is non-trivial, we know, again by our inductive hypothesis, that there exist subgroups of K of every possible order. These are the orders p^i with $0 \leq i \leq n-m$. It now follows that there exist subgroups H of G of orders p^i with $m \leq i \leq n$. And this completes the proof!

Problem 12

If $|G| = p^n$, p a prime number, prove that there exist subgroups N_i, $i = 0, 1, \ldots, r$ (for some r) such that $G = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_r = \{e\}$ where N_i is a normal subgroup of N_{i-1} and where N_{i-1}/N_i is abelian.

By problems 11 and 14, G has a normal subgroup H of order p^{n-1}. Now since $|G/H| = |G|/|H| = p^n/p^{n-1} = p$, we see that G/H must be a cyclic group, and therefore abelian. Now, of course, we can apply this same reasoning to H in finding a normal subgroup K of H of order p^{n-2}, and so on. Since G is of finite order, this nesting of subgroups must terminate at $\{e\}$.

I believe a group G, not necessarily of prime order, but having the above properties otherwise, is considered to be a solvable group. It's interesting to consider the solvability of any group. By Caylay's theorem, any group G is isomorphic to a subgroup of $A(S)$ for an appropriate set S. Now if $|S| = n$, let $\emptyset = S_0 \subset S_1 \subset \cdots \subset S_n = S$ be a sequence of n properly nested subsets of S, and define $H_i = \{\phi \in G | \text{for all } x \in S_i, \phi(x) = x\}$. It is not hard to see that each H_i is a normal subgroup of G. Further, for any $0 \leq i < j \leq n$, notice that $H_j \leq H_i$, and H_j is normal in H_i. So what's to keep any group from being solvable? The only remaining criteria would appear to be the requirement that each H_j/H_i be abelian. In this general situation, I'm not sure what we can say, if anything, about how abelian the fractor group H_j/H_i is. A measure of that has something to do with its commutator subgroup, I think.

Problem 14

Prove that any subgroup of order p^{n-1} in a group G of order p^n, p a prime number, is normal in G.

If H was such a subgroup of G, then it would have p right (or left) cosets in G. Hmmm...