Math 322 Homework 11

Xander Naumenko

05/12/23

Herstein 2.13.2a. Consider the map $\phi : G \to D$ defined by $\phi(g) = (g, g)$. ϕ is a homomorphism since $\phi(g_1g_2) = (g_1g_2, g_1g_2) = (g_1, g_2)(g_1, g_2) = \phi(g_1)\phi(g_2)$. Also $\ker\phi = \phi^{-1}((1, 1)) = 1$ and ϕ is clearly surjective, so ϕ shows that G and D are isomorphic.

Question Herstein 2.13.4b. Both directions:

($\implies$) Suppose D is normal in T, and let $g_1, g_2 \in G$. Since D is normal we have $(g_2^{-1}, g_2^{-1})(g_1, g_1)(g_2, g_2) = (g_1, g_1) \implies g_2^{-1}g_1g_2 = g_1 \implies g_1g_2 = g_2g_1$. Since g_1, g_2 were arbitrary thus every element of G commutes, so it is abelian.

($\impliedby$) Suppose G is abelian, and let $(g_1, g_2) \in T, (g, g) \in D$. Then $(g^{-1}, g^{-1})(g_1, g_2)(g, g) = (g^{-1}g_1g, g^{-1}g_2g) = (g_1, g_2)$. Thus D is normal in T.

Question Herstein 2.13.5. Let $|G| = \prod_{i=1}^n p_i^{\alpha_i}$ and let P_i be a arbitrary Sylow p_i-subgroups. Each element in a P_i has order one of $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$, so other than the identity each of the P_i are pairwise disjoint. Also each P_i is normal since G is abelian. I claim that $G = P_1P_2\cdots P_n$ is the internal direct product of these groups. There are $p_i^{\alpha_i}$ choices for each group, so there are $\prod_{i=1}^n p_i^{\alpha_i} = |G|$ elements of the form $g = g_1g_2, \cdots g_n, g_i \in P_i$, I claim that each of these is unique. Suppose $g_1g_2\cdots g_n = g_1'g_2'\cdots g_n' \implies (g_1g_1'^{-1})^{|G|/p_1^{\alpha_1}} = (g_2'g_2^{-1}\cdots g_n'g_n^{-1})^{|G|/p_1^{\alpha_1}} = 1 \implies g_1 = g_1'$. Repeating this for $2, 3, \ldots, n$ gives that this representation of g is unique. Since there are exactly $|G|$ unique elements generated this way, by the definition given on the top of page 106 we have that G is the internal direct product of P_i. Then by theorem 2.13.1 it is isomorphic to $P_1 \times \ldots \times P_n$.

Question Herstein 2.13.6. Both directions:

($\implies$) Suppose $A \times B = \langle(a, b)\rangle$ is cyclic. By contradiction assume that $\gcd(m, n) = k > 1$, then we have $(a, b)^{\frac{mn}{k}} = \left((a^m)^{n/k}, (b^n)^{m/k}\right) = (1^{n/k}, 1^{m/k}) = (1, 1)$. However this contradicts the assumption that (a, b) was of order mn, so it must be that $\gcd(m, n) = 1$.

($\impliedby$) Assume that m and n are relatively prime, and let $A = \langle a\rangle$ and $B = \langle b\rangle$. I claim $A \times B = \langle(a, b)\rangle$. Let $k \in \mathbb{N}$ with $(a, b)^k = (a^k, b^k) = (1, 1)$. Since $a^k = 1$ we have $m|k$ and similarly since $b^k = 1$ we have $n|k$. m and n are relatively prime so it must be that $mn|k$, implying that the order of $(a, b) = mn$ and thus $A \times B$ is cyclic.

Question 8. Consider $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ using additive notation, let $N_1 = \langle(0, 1)\rangle$, $N_2 = \langle(1, 0)\rangle$ and $N_3 = (1, 1)$. G is abelian so each of these groups is normal, and they each only contain the identity 0 and their generator so they're clearly disjoint except the identity. Also clearly $G = \{(0, 0), (0, 1), (1, 0), (1, 1)\} = N_1N_2N_3$. However $(1, 1)$ can be represented either as $(0, 1)+(1, 0)$ or $(1, 1)$, so not every element in G can be uniquely expressed by a product of elements of N_1, N_2 and N_3. Thus G is not the internal direct product of N_1, N_2 and N_3.

Question 11. Let $h \in H_0$ with $h \neq 1$. If $|G|$ has two prime factors p, q then h belongs to both a Sylow p-subgroup and Sylow q-subgroup, but this is impossible since elements of those groups must have powers that are purely powers of p and q respectively and h can't be both. Thus the order G is p^k for some prime p and $k \in \mathbb{N}$.

By Cauchy's theorem there is a subgroup of order p and H_0 is contained in it, so we can write $H_0 = \langle h \rangle$ where the order of h is p. For any $g \in G$ with order p we have $\langle h \rangle \subseteq \langle g \rangle \implies \langle h \rangle = \langle g \rangle$, so this subgroup is unique. Next, I claim that for every $m = 1, 2, \ldots, k$, there are at most p^m elements of order p^m. Suppose $g_1, g_2 \in G$ both have order m, then $\langle h \rangle \subseteq \langle g_1 \rangle$ and $\langle h \rangle \subseteq \langle g_2 \rangle$. Cyclic groups of the same order only intersect nontrivially if they're equal, so $\langle g_1 \rangle = \langle g_2 \rangle$. A group of order p^m by definition has exactly p^m elements, so the maximum possible number of elements of order p^m is p^m.

Now consider counting the number of elements of each order. The number of elements of order strictly less than p^k is, using the above claim (this is, to be clear, a very weak bound but it is sufficient. It ignores the fact that each of these subgroups intersect with all smaller ones),

$$1 + p + p^2 + \ldots + p^{k-1} = \sum_{i=0}^{k-1} p^i = \frac{p^k - 1}{p - 1} \leq p^k - 1.$$

However there are p^k elements in G so this couldn't have accounted for all of them. Thus there is an element of order p^k, which implies that G is cyclic.