Groups and Rings

Unseen Problem Sheet 3 Solutions

October 28, 2021

A1. $\mathbb{Z}_{p^2}$ has precisely one subgroup of order p, whereas $\mathbb{Z}_p \times \mathbb{Z}_p$ has at least two: $\mathbb{Z}_p \times 0$ and $0 \times \mathbb{Z}_p$. The two groups are therefore non-isomorphic. Assume G has order p^2 and is not isomorphic to $\mathbb{Z}_{p^2}$. This means G is not cyclic. By Cauchy's Theorem, there is $a \in G$ with ord $a = p$. For $b \notin < a >$, we have ord $b = p$ or $= p^2$; the latter is impossible since this would imply G is cyclic. So ord $b = p$ and $| < b > | = p$. Note that, since $b \notin < a >$ and any group of prime order cannot have nontrivial subgroups, we have $< a > \cap < b >= e$. Clearly $| < a >< b > | = | < a > || < b > | = p^2 = |G|$ and thus $G =< a >< b >$. Since G is abelian, hence $< a >$ and $< b >$ are normal subgroups, and so we have $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

A2. Proof by induction : Suppose $|G| = n$. For $n = p$, we know that this must be cyclic, and every element except identity has order p. Thus, $N_p = p - 1$, so we are done. Now suppose $n = p^k * m$ for $k \geq 1$ and $gcd(m, p) = 1$. Then, by Cauchy's theorem, there exists an element, say x of G whose order is p. Let C_x denote the subgroup of G generated by x. Suppose $G' = G/C_x$. Then, if p does not divide $|G'|$, we have that there is no element of order p in G'. So, this implies $k = 1$, and all elements of order p in G arise from C_x, thus $N_p = p - 1$. If p divides $|G'| = p^{k-1} * m$, then by our induction hypothesis, the number of elements of order p in G', say N'_p satisfies $p|N'_p + 1$. Moreover, every order p element of G' gives rise to p order p elements of G, so we have $N_p = N'_p(p + 1)$ (the 1 is for the elements from C_x). Hence the result follows.

A3. Let H be a subgroup of index p. Then G acts on the set of left cosets of H by left multiplication. This action induces a homomorphism from $\phi : G \to S_p$, whose kernel, say K, is contained in H. Then G/K is isomorphic to a subgroup of S_p. Thus, the order of G/K divides $p!$; however, it must also divide $|G|$. Since p is the smallest prime dividing $|G|$, it follows that $|G/K| = p$. Since $|G/K| = [G : K] = [G : H][H : K] = p[H : K]$, it follows that $[H : K] = 1$, hence we conclude $K = H$. Since K is normal, so is H.

A4. (1) Every product of g_j's will be contained in H_i. Moreover, each of these products must be distinct, since otherwise we obtain a relation between the g_j's, which would imply $H_i = H_{i+1}$ for some i, leading to a contradiction.
(2) $H_k = G$ for some k. This gives, $n \geq 2^k$, giving us the desired result.

In order to construct a group of order n, we must make a choice of at most $log_2 n$ elements coming from S_n, whose cardinality is $n!$. The result follows from a simple counting argument.