ALGEBRA HOMEWORK SET III SOLUTIONS

JAMES CUMMINGS

You may collaborate on this homework set, but must write up your solutions by yourself. Please contact me by email if you are puzzled by something, would like a hint or believe that you have found a typo.

(1) Let p be prime and let G be a non-abelian group of order p^3. Show that $Z(G) = [G, G]$ and this is a subgroup of order p.

Since G is a finite p-group, $Z(G)$ is non-trivial. Also $G/Z(G)$ can not be cyclic, so $Z(G)$ does not have order p^2. It follows that $Z(G)$ has order p, and also incidentally that $G/Z(G) \simeq C_p^2$.

Now since G is non-abelian $[G, G]$ is non-trivial. Since $G/Z(G)$ is abelian we have $[G, G] \leq Z(G)$. So the only possibility is that $[G, G] = Z(G)$.

(2) Prove that every group of order 15 is cyclic

The Sylow subgroups of order 3 and 5 are unique hence normal. Call them P and Q. Then $[P, Q] \subseteq P \cap Q = \{e\}$, hence $G \simeq P \times Q$ and is thus cyclic of order 15.

(3) Prove there is no simple group of order pq for distinct primes p, q.

Let $p < q$ and let m be the number of Sylow q-subgroups. Then m divides p and is congruent to 1 mod q. So $m = 1$.

(4) Repeat the previous exercise for groups of order $p^2 q$.

Let m_p, m_q be the numbers of Sylow p and q subgroups. m_p divides q, so either $m_p = 1$ and we are done or $m_p = q$.

Assume that $m_p = q$, so that in particular $q \equiv 1 \mod p$ and $q > p$. m_q divides p^2. If $m_q = 1$ we are done, if $m_q = p$ then $p \equiv q \mod 1$ and $p > q$, but this is impossible. So $m_q = p^2$. But if there are p^2 many q-subgroups, since they have pairwise trivial intersection that gives $1 + p^2(q - 1)$ many elements of order 1 or q. This leaves only $p^2 - 1$ elements which can be of p-power order, so there is only one Sylow p-subgroup and hence $m_p = 1$ after all.

(5) Let G be a simple group of order 60. Determine the numbers of Sylow p-subgroups for $p = 2, 3, 5$ (if you can't determine the exact values give as much information as you can).

n_p is the number of Sylow p-subgroups.

Easy bit: $n_2 = 3, 5, 15$, $n_3 = 4, 10, 20$, $n_5 = 6$.

Harder bit 1: By an argument from the last HW solns there can't be any subgroups of small index (look at the action of G on the left cosets of H by left multn, its kernel must be trivial). So we can eliminate $n_2 = 3$ and $n_3 = 4$.

Harder bit 2: There are 24 elements of order 5 (subgroups of order 5 have trivial intersection). If $n_3 = 20$ there are (similarly) 40 elements of order 3. Contradiction so $n_3 = 10$.

Seriously hard bit: argue that G must be A_5 (ask me if you are interested in how to do this). Then there are 5 Klein 4-groups so $n_2 = 5$. Checking our other answers: there are 20 3-cycles so indeed $n_3 = 10$ and there are 24 5-cycles so indeed $n_5 = 6$.

(6) Let F be a finite field with q elements and let $GL_n(F)$ be the group of invertible linear maps from F^n to F^n. What is the order of G?

We need to count non-singular matrices. Use the fact that a matrix is non-singular iff each column is not in the span of the previous columns (which must then be independent) to show that the order is

$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}).$$

(7) Prove or give a counterexample to the statement "if G is nilpotent, every subgroup of G is also nilpotent".

Let $H \leq G$ and let G_i be a normal series with $[G, G_{i+1}] \subseteq G_i$. Let $H_i = G_i \cap H$ and argue (this is easy) that H_i is a normal series in H and $[H, H_{i+1}] \subseteq H_i$.

(8) Prove that there are (up to isomorphism) only two non-abelian groups of order 8 and describe them.

From the first question such a group G has $Z(G) = [G, G]$ a subgroup of order 2, and also we have $G/Z(G) \simeq C_2^2$. Choose elements a, b, c so that $Z(G) = [G, G] = \langle a \rangle$, and $G/Z(G) = \{Z(G), bZ(G), cZ(G), bcZ(G)\}$. It follows that all elements are of form $a^i b^j c^k$ for $0 \leq i, j, k < 2$. We know that a commutes with everything so we need to ask what are the products bb, bc, cb, cc? Note that no element has order 8 (else the group is cyclic!) so surely $b^4 = c^4 = e$.

Now $[b, c] \in [G, G] = Z(G)$ and we can't have $bc = cb$ (since that would easily make the group abelian). So $bcb^{-1}c^{-1} = a$, that is $abc = cb$.

Finally $(bZ(G))^2 = Z(G)$ so that $b^2 \in Z(G)$, similarly $c^2 \in Z(G)$ and $(bc)^2 \in Z(G)$. If $b^2 = c^2 = e$ then $(bc)^2 = b(cb)c = b(abc)c = ab^2c^2 = a$, so at least one of b, c, bc has order 4. We assume WLOG it is b, so that $b^2 = a$ and G is generated by b, c.

If c has order 2 then G is generated by b, c subject to relations $b^4 = c^2 = e$ and $cbc = abc^2 = ab = b^{-1}$. In this case we have the dihedral group of order 8.

Otherwise c has order 4. In this case G is generated by b, c subject to relations $b^4 = c^4 = e$, $b^2 = c^2$, $cb = b^3c$. This gives another group of order 8, the "quaternion group".

Cultural note (which may make more sense to you later in life): the quaternions are an associative $\mathbb{R}$-algebra consisting of elements $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ and $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ki = j$. The elements $\pm\{1, i, j, k\}$ form a quaternion group.

(9) Recall that if G is a group then $G^{(n)}$ is defined by the induction $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$. Compute this series of groups when $G = S_3$, S_4, S_5.

Commutators are even so $[S_n, S_n] \subseteq A_n$. Conversely $(ab)(ac)(ab)(ac) = (abc)$ so easily $[S_n, S_n] = A_n$ for $n \geq 3$.

Easily for S_3 it goes $S_3, A_3, \{e\}, \dots$.

For A_4 we start S_4, A_4. Now A_4 has a unique Sylow 2-subgroup $V = \{e, (12)(34), (13)(24), (14)(23)\}$, A_4/V is abelian so $[A_4, A_4] \subseteq V$. On the other hand $(123)(124)(132)(142) = (12)(34)$ so easily equality holds. And V is abelian so we get $S_4, A_4, V, \{e\}, \ldots$.

(We will use these series later to solve the cubic and quartic equations)

Since A_5 is nonabelian simple $[A_5, A_5]$ must be A_5. So we get $S_5, A_5, A_5, \ldots$