D-MATH Algebra I HS 2013
Prof. Brent Doran

Solution 7

The class equation, Symmetric group, Sylow theorems

1. (a) Prove that if $G/Z(G)$ is cyclic then G is abelian, in particular $Z(G) = G$.
Solution Let us fix a generator $\overline{g}$ of $Z(G)$ and let $g \in G$ be an element such that $\overline{g} = gZ(G)$. Let x_1, x_2 be elements of G, there exist element z_i in $Z(G)$ and integers a_i such that $x_i = z^{a_i} g_i$. This implies that $x_1 x_2 = z^{a_1} g_1 z^{a^2} g_2 = z^{a_1+a_2} g_1 g_2 = z^{a_1+a_2} g_2 g_1 = x_2 x_1$.

   (b) Prove that a group G of order p^4 has an abelian subgroup of order p^3.
Solution Since the center of a p-group is always non trivial, $Z(G)$ has cardinality p^4, p^2 or p. If the cardinality is p^4 then G is abelian and has abelian subgroups of cardinality p^3.

   Let us now assume that the cardinality of $Z(G)$ is p^2, and let x be an element that doesn't belong to $Z(G)$. Then the cardinality of $H = Z(x)$ is p^3: H contains $Z(G)$ and x, in particular its cardinality divides p^4, is not p^4 since x is not in the center, and is bigger than p^2. Moreover $Z(H) = H$ since both x and $Z(G)$ are contained in $Z(H)$.

   Let us now assume that $|Z(G)| = p$. The class equation gives $p^4 = p + \sum C(x)$. This implies that there exist a conjugacy class of cardinality p (otherwise the righthand side would not be divisible by p^2). Hence there exists an elemente x with $|Z(x)| = p^3$. Such a group is abelian since its center has cardinality at least p^2, since it contains x and $Z(G)$ but if it had cardinality exactly p^2 the quotient would be cyclic.

2. Compute the centralizer in S_6 and in A_6 of the permutation $(1,2,3)(4,5,6)$.
SolutionThe conjugacy class of σ in S_6 consists of all the permutations whose cycle decomposition has two 3-cycles. This implies that $C(\sigma)$ has cardinality

$$|C_\sigma| = \frac{6!}{18}$$

and hence the cardinality of $Z(\sigma)$ is 18. Clearly the group $H = \langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$ is a subgroup of $Z(\sigma)$ of cardinality 9, hence of index 2 in $Z(\sigma)$. The permutation $\tau = (1,4)(2,5)(3,6)$ that exchanges the two factors is in $Z(\sigma)$ but not in H, hence $Z_{S_6}(\sigma) = \langle H, \tau\rangle$.

   The permutation σ belongs to A_6 and the centralizer of σ in A_6 is the intersection $A_6 \cap Z_{S_6}(\sigma)$ and consists of the group H.

3. (a) Let p and q be permutations. Prove that the products pq and qp have cycles of equal length.
Solution The permutations pq and qp are conjugate: $pq = p(qp)p^{-1}$ in particular they have cycles of equal length.

   (b) Prove that the transpositions $(1,2),(2,3),\dots(n-1,n)$ generate the symmetric group S_n.
Solution Let us consider the group G generated by the transpositions $(k,k+1)$. Any transposition is contained in G: the transposition $(m,m+l)$ can be written as the product

$$(m+l-1,m+l)\dots(m+1,m+2)(m,m+1)(m+1,m+2)\dots(m+l-1,m+l).$$

In order to finish the proof it is enough to prove that any permutation can be written as a product of transpositions. We will prove this by induction on n, where n is the number of elements that are not fixed by the permutation τ. If $n = 2$ then τ is a transposition and hence we are done. Let us now assume that any permutation that moves at most k elements is a product of transpositions, and let σ be a permutation that moves $k+1$ elements. Let a be an element in the support of σ, let $b = \sigma^{-1}(a)$ and let us consider the permutation $\rho = \sigma(a,b)$. The support of ρ is contained in the support of σ, moreover a is fixed by ρ. This implies, by inductive hypothesis that ρ can be written as a product of transpositions, hence the same is true for σ.

4. Let $G = GL_n(\mathbb{Z}/p\mathbb{Z})$, p prime, H a Sylow p-subgroup of G.

   (a) Compute the cardinality of G and of H.
Solution Let M be a matrix in $M_{n\times n}(\mathbb{Z}/p\mathbb{Z})$. The matrix is invertible if and only if its k-th column is a vector of $(\mathbb{Z}/p\mathbb{Z})^n$ that doesn't belong to the linear span of the first $k-1$ columns. In particular, since a k-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ has p^k elements we get that the cardinality of $GL_n(\mathbb{Z}/p\mathbb{Z})$ is

$$|GL_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) = p^{\frac{n(n-1)}{2}}d$$

where d is a number that is coprime with p. This implies that, if H is a p-Sylow, the chardinality of H is $p^{\frac{n(n-1)}{2}} = p^k$.

   (b) Let M be an element of H. What are the eigenvalues of M?
Solution In particular this implies that, for every element $M \in H$, we have $M^{p^k} = 1$ that implies that $(\det M)^{p^k} = 1$, in particular the characteristic polynomial of M divides $(x^{p^k}-1) = (x-1)^{p^k}$ modulo p. In particular if a matrix M is in H, all its eigenvalues are 1.

   (c) Describe explicitly a Sylow p-subgroup H. *Hint* Assume that there exists a basis in which all matrices of H are upper triangular.
Solution Since all the eigenvalues of a matrix M in H are 1, if M is in

addition upper triangular, M must have ones on the diagonal. Let us now consider the set U of upper triangular matrices of G having ones on the diagonal. The cardinality of U is p^k and U is a subgroup of G, in particular U is a Sylow p-subgroup of G.

5. Let $G_1 \subseteq G_2$ be groups whose orders are divisible by p and let H_1 be a Sylow p-subgroup of G_1. Prove that there is a Sylow p-subgroup H_2 of G_2 such that $H_1 = H_2 \cap G_1$.
   Solution Indeed the group H_1 is a $p-$group that is a subgroup of G_2, in particular the Second Sylow Theorem implies that there exist a Sylow p-subgroup H_2 of G_2 such that H_1 is contained in H_2. Let us now consider the intersection $H_2 \cap G_1$. It is a $p-$group, since it is a subgroup of H_2 that is a p-group, it is contained in G_1 by definition and contains H_1 since both H_2 and G_1 contain H_1. This implies that $H_1 = H_2 \cap G_1$. And this concludes the proof.

6. (a) Prove that no simple group has order pq where p and q are distinct primes.
   Solution If $pq = 6$ the result is known. We will assume that $pq > 6$. Moreover we will assume, without loss of generality that $p > q$. Let G be a group of order pq and let us denote by s the number of Sylow $p-$subgroups of G. By the third Sylow Theorem we know that s divides q and is congruent to 1 modulo p. Since q is smaller than p, q cannot be congruent to 1 modulo p. This implies that there exists precisely one p-Sylow, that is hence a normal subgroup of G. This implies that G is not simple.

   (b) prove that no simple group has order pq^2 where p and q are disctinct primes.
   Solution Let us first assume that $p > q^2$ and let us consider the number s of Sylow p-subgroups. Since s divides q^2, that is smaller than p and is congruent to 1 modulo p we get that $s = 1$ hence the Sylow p-subgroup is normal.

   Let us now assume that $q^2 > p$ and consider the number s of q-Sylow. If $s = 1$ we are done, let us assume that $s = p$, from the fact that $s = 1$ modulo q we get $p = kq + 1$. Let us now consider the number t of Sylow p-subgroups. Again if $t = 1$ we are done. If $t = q$ we get $q = mp + 1 = m(kq + 1)$ and this gives a contradiction. We are left with the case $t = q^2$ and in this case we get $q^2 = m(kq + 1) + 1 = mkq + m + 1$. This implies that $m + 1 = q$ and hence $k = 1$ which is, again, a contradiction.

   (c) Classify all groups of order 33.
   Solution Let G be a group of order 33. The Sylow 11 subgroup of G is normal (since 3 is not equal to 1 modulo 11), and also the Sylow 3-subgroup is normal (since 11 is not equal to 1 modulo 3). This implies that the unique group of order 33 is the cyclic group that is the product of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z}$.