

Assignment 5 – Solutions

MATH 3175–Group Theory

Problem 1 Let $G = \mathbb{Z}_{32}^\times$ the multiplicative group of invertible elements in \mathbb{Z}_{32} . Then

$$\begin{aligned} G &= \{[a] \mid a \in \mathbb{Z}, 0 < a < 32, \gcd(a, 32) = 1\} \\ &= \{[a] \mid a \in \mathbb{Z}, 0 < a < 32, 2 \nmid a\} \\ &= \{[1], [3], [5], [7], [9], [11], [13], [15], [17], [19], [21], [23], [25], [27], [29], [31]\}, \end{aligned}$$

an abelian group of order 16. The subgroup $H = \langle [31] \rangle = \{[1], [31]\}$ is a cyclic group of order 2, while the subgroup $K = \langle [3] \rangle = \{[1], [3], [9], [27], [17], [19], [25], [11]\}$ is a cyclic group of order 8. Clearly, $H \cap K = \{[1]\}$. Moreover, $HK = G$, since all the remaining elements in G (besides those already in H or K) are of the form $h \cdot k$ with $h \in H$ and $k \in K$:

$$\begin{aligned} [5] &= [31] \cdot [27], & [7] &= [31] \cdot [25], & [13] &= [31] \cdot [19], & [15] &= [31] \cdot [17], \\ [21] &= [31] \cdot [11], & [23] &= [31] \cdot [9], & [29] &= [31] \cdot [3]. \end{aligned}$$

Since the elements of H and K commute, we may apply the Decomposition Theorem and conclude that $G \cong H \times K$. In other words, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_8$.

Problem 2 For a finite group G , and a prime p such that $p \mid |G|$, we write $|G| = mp^k$ with $p \nmid m$, we let $\text{Syl}_p(G)$ be the set of p -Sylow subgroups of G , and we denote by n_p the size of this set. By Sylow I, $n_p > 0$, while by Sylow III, $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$. Finally, by Sylow II, all p -Sylow subgroups are conjugate; thus, if $n_p = 1$, then $\text{Syl}_p(G) = \{P\}$, and P is a normal subgroup of G .

1. Let G be a group of order $20 = 4 \cdot 5$. We then have $n_5 \equiv 1 \pmod{5}$ and $n_5 \mid 4$. Thus, $n_5 = 1$, and there is a unique 5-Sylow subgroup of G , call it P , which must be a normal subgroup. Moreover, $|S| = 5$ is neither 1 nor 20, and so P is a non-trivial, proper, normal subgroup of G , thereby showing that G is not a simple group.
2. Let G be a group of order $10 \cdot 11^5$. We then have $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 10$; thus, $n_{11} = 1$. Arguing as above, we conclude that G is not simple.
3. Let G be a group of order $|G| = pq^r$ with p and q both prime, $p < q$, and $r > 0$. We then have $n_q \equiv 1 \pmod{q}$ and $n_q \mid p$. The last condition gives $n_q = 1$ or $n_q = p$. But since $1 < p < q$, it follows that $p \not\equiv 1 \pmod{q}$; hence, $n_q = 1$. Once again, this implies that G is not simple.

Problem 3 Let G be a group with $|G| = 30 = 2 \cdot 3 \cdot 5$, and denote by t_r the number of elements of G that have order r .

1. We have $n_5 \equiv 1 \pmod{5}$ and $n_5 \mid 6$; thus, $n_5 = 1$ or 6. Moreover, $n_3 \equiv 1 \pmod{3}$ and $n_3 \mid 10$; thus, $n_3 = 1$ or 10.
2. First note that all the p -Sylow subgroups of G are cyclic. Indeed, there is no repeated factor in the prime factorization of $|G|$; thus, if P is a p -Sylow, then $|P| = p$ (and so $P \cong \mathbb{Z}_p$).

Now suppose P_1 and P_2 are two distinct Sylow p -subgroups of G . Then $P_1 \cap P_2$ is a proper subgroup of P_1 (and also P_2), and so $|P_1 \cap P_2|$ divides $|P_1|$, by Lagrange's theorem. But $|P_1| = p$ is a prime, and therefore $|P_1 \cap P_2| = 1$, showing that $|P_1 \cap P_2| = \{e\}$.

The two facts proved above imply that $t_p = (p - 1)n_p$, for every prime $p \mid |G|$. (All we used here is that $|G| = p_1 p_2 \cdots p_n$, with all distinct prime factors p_i .)

3. If $n_5 = 6$, then $t_5 = (5 - 1)6 = 24$. Likewise, if $n_3 = 10$, then $t_5 = (3 - 1)10 = 20$.
4. If both $n_5 = 6$ and $n_3 = 10$, then $30 = |G| > t_5 + t_3 = 24 + 20 = 44$, a contradiction. Thus, we must have either $n_5 = 1$ or $n_3 = 1$. In either case, the argument from the previous problem shows that G contains a non-trivial, proper normal subgroup (or order 5 or 3); hence, G is not simple.

Problem 4 Let p be a prime.

1. The symmetric group S_p has order $p! = (p - 1)! \cdot p$. The prime p divides $p!$, but not $(p - 1)!$. Thus, the Sylow p -subgroups of S_p have order precisely p .
2. One such Sylow p -subgroup is $H = \langle (12 \dots p) \rangle$, the cyclic group of order p generated by the cyclic permutation $(12 \dots p)$ that sends $1 \rightarrow 2 \rightarrow \cdots \rightarrow p \rightarrow 1$.
3. Recall the following: if $\sigma = (a_1 \dots a_k)$ is a k -cycle, and τ is any permutation, then $\tau\sigma\tau^{-1}$ is the k -cycle $(\tau(a_1) \dots \tau(a_k))$.

Now suppose $p > 3$, and let $H \leq S_p$ be the above subgroup. Taking $\tau = (12)$ and $\sigma = (12 \dots p)$ we get $\tau\sigma\tau^{-1} = (213 \dots p)$, which does not belong to H . Thus, H is not normal.

Problem 5 The group $G = \text{GL}_3(\mathbb{Z}_2)$ has order $(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168 = 2^3 \cdot 3 \cdot 7$. A Sylow 2-subgroup of G must have order $2^3 = 8$. We have seen before such a subgroup (on the Midterm exam): it is the Heisenberg group of 3×3 upper-diagonal matrices entries in \mathbb{Z}_2 with 1s along the diagonal. In turn, this group is isomorphic to the dihedral group D_4 of order 8.

Bonus question: By Sylow III, the number n_2 of Sylow 2-subgroups satisfies $n_2 \equiv 1 \pmod{2}$ and $n_2 \mid 21$; thus $n_2 \in \{1, 3, 7, 21\}$. It can be shown that G is actually a simple group: it is isomorphic to $\text{PSL}(2, \mathbb{Z}_7)$, the famous Klein simple group of order 168 (the smallest non-abelian simple group after the alternating group A_5 with 60 elements, which is isomorphic to $\text{PSL}(2, \mathbb{Z}_5)$).¹ This immediately rules out $n_2 = 1$, since otherwise H would be normal, contradicting the fact that G is simple. But it also rules out $n_2 = 3$, since otherwise the corresponding representation, $\varphi: G \rightarrow S_3$, cannot have $\ker(\varphi) = \{1\}$ (since $168 > 3! = 6$), and also cannot have $\ker(\varphi) = G$ (since φ is transitive, by Sylow II), and so $\ker(\varphi)$ is a proper, non-trivial normal subgroup of G , thereby contradicting the fact that G is simple. So this leaves open the question whether $n_2 = 7$ or $n_2 = 21$, since 168 divides both $7!$ and $21!$, so the previous argument(s) are not dispositive. The answer, in fact, is $n_2 = 21$.

Indeed, the group G has 21 elements of order 2, and together they form a conjugacy class, $C = \{z_1, z_2, \dots, z_{21}\}$. The centralizer in G of each such element z_i is a group of order 8, and so must be a Sylow 2-subgroup, call it P_i . For instance, H is the centralizer of the matrix with 0's next to the diagonal, and a 1 in the upper corner; if we call this matrix z_1 , then $P_1 = H$. Moreover, if $z_i = g_i z_1 g_i^{-1}$, then $P_i = g_i H g_i^{-1}$, and so $\text{Syl}_2(G) = \{P_1, P_2, \dots, P_{21}\}$, as claimed.

Problem 6 Let $G = D_6 = \langle r, s \mid r^6 = s^2 = (sr)^2 = 1 \rangle$, and consider the normal subgroups $N_1 = \langle r^3 \rangle$ and $N_2 = \langle r^2 \rangle$. The lattice of subgroups of G , as well as those of its respective factor groups, G/N_1 and G/N_2 , are depicted below.² In each case, the projection map $\pi_i: G \rightarrow G/N_i$

¹See for instance the Wikipedia article on [PSL\(2,7\)](#).

²The figures were drawn with the help of the excellent software package [GroupNames](#) by Tim Dokchitser.

($i = 1, 2$) establishes a 1-to-1 correspondences between the sub-lattice of subgroups of G containing N_i and the lattice of subgroups of G/N_i .

