GU4041: Intro to Modern Algebra I

Professor Michael Harris
Solutions by Noah Olander, Anton Wu, and Iris Rosenblum-Sellers

Practice Final

1) True or False? If false, give a counterexample, if true, provide an explanation. The explanation can be brief, but it is not enough to say that the statement was explained in the course.

a) A group of order 392 has either 1 or 8 Sylow 7-subgroups

Proof. $392 = 2^3 \times 7^2$. Then by Sylow's third theorem, n_7, the number of Sylow 7-subgroups, has an order in $\{1, 2, 4, 8\} \cap 1 + 7\mathbb{Z}$. This intersection is precisely $\{1, 8\}$, so the statement is true. □

b) For any n, let $A(n)$ denote the number of distinct non-isomorphic abelian groups of order n. Then $A(65) > A(64)$

Proof. $65 = 5 \times 13$, each of which are prime, so there's only one abelian group of order 65 up to isomorphism, by the classification of finitely generated abelian groups. Then since there's at least one of order 64, i.e. $\mathbb{Z}_{64}$, this statement is false □

c) Let G be a group of even order. Then it has at least one conjugacy class, not including the identity element, with an odd number of elements

Proof. The order of G is the sum of the orders of its conjugacy classes. Since $\{e\}$ is a conjugacy class, and the sum of the orders of the conjugacy classes is even, and the sum of any number of even numbers and a single odd number is odd, if each other conjugacy class had even order, we would have a contradiction, as the sum of the orders of the conjugacy classes would be odd, while $|G|$ is even. □

d) Let H be a subgroup of the alternating group A_5. Suppose H contains every 3-cycle. Then $H = A_5$.

Proof. We argue by order. There are at least $2\binom{5}{3} + 1$, since for any set of 3 elements, there are two three-cycles including those 3, plus the identity, so there are at least 21 elements. Then the order of this subgroup divides $|A_5|$, so it's either 30 or 60. However, if it were 30, it would be an index 2-subgroup, entailing that it's a nontrivial normal subgroup, violating the simplicity of A_5. Therefore, the statement is true. □

2)

a) Determine the centralizer of the product $(12)(34)(56)(78)$ of four 2-cycles in S_8. Use this to determine the number of all elements of S_8 which can be written as products of four 2-cycles.

Proof. Suppose g is such that $g(12)(34)(56)(78)g^{-1} = g(12)g^{-1}g(34)g^{-1}g(56)g^{-1}g(78)g^{-1} = (12)(34)(56)(78)$ Then $g(12)g^{-1} \in \{(12), (34), (56), (78)\}$, and so on. We recall that $g(12)g^{-1} = (g(1)g(2))$, where $g(1)$ denotes evauation of g as a bijection on $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Then $g(1)$ is some number; it determines $g(2)$ if g is in the centralizer; likewise, $g(3)$ is some number, and so on, so the order of the centralizer is $\binom{8}{1}\binom{6}{1}\binom{4}{1}\binom{2}{1} = 384$, and it consists of precisely the elements following the rule that if $g(k) = l$, then $g(k + j_k) = l + j_l$, where j_n is 1 if n is even, and -1 otherwise, for all n. For example, $(1475)(2386)$ is in the centralizer. The centralizer is also the stabilizer under conjugation action, so it follows that $8!/384 = 105$ is the orbit under conjugation action, which is the number of elements which can be written as the product of four transpositions. □

b) Same question, but with S_{12}.

Proof. An element of the centralizer must have that its restriction to S_8 is a bijection, since it must follow the stronger condition of mapping 2 to $g(1) + j_{g(1)}$, for example. It can do anything on the remaining copy of S_4, so there are 24(384) elements in the centralizer now. In this case, we have that the order of the orbit is $12!/(24(384)) = 51975$. □

3) How many elements of order 5 are there in $S_5 \times \mathbb{Z}_{25}$?

Proof. An element $(\tau, [k])$ of $S_5 \times \mathbb{Z}_{25}$ has order 5 if the order of both τ and $[k]$ is a factor of 5, and they are not both 1. There are 5 elements like that in $\mathbb{Z}_{25}$, and elements like that in S_5 equal to the number of ways to permute 4 numbers plus one; we can see this, since τ must be a 5-cycle or the identity; if it's a 5-cycle, we can write it starting with a 1, and with some permutation of $2, 3, 4$ and 5 after it. There are 4! ways to do that then, so there are 25 elements of order a factor of 5 in S_5. Then there are 125 in $S_5 \times \mathbb{Z}_{25}$ of order 1 or 5; so there are 124 of order 5. □

4)

a) What is the number of conjugacy classes of the dihedral group D_{2n}? Prove your answer and note that it depends on whether n is odd or even.

Proof. Let $r^k s$ be some flip in D_{2n}. It's in the conjugacy class of s iff $j : r^j s r^{-j} = r^k s$; we recall that $r^j s r^{-j} = r^{2j} s$. Then they're all in one conjugacy class iff [2] generates $\mathbb{Z}_n$, since then we can pick j accordingly, which is iff n is odd. Otherwise, there are conjugacy classes of the $r^k s$'s in bijection with the cosets of $< [2] >$ in $\mathbb{Z}_n$; i.e. every even number is in the same conjugacy class as s, and every odd is in the same as rs. As for the powers of r, we recall that $s r^k s^{-1} = r^{-k}$, so each power of r is in a conjugacy class with it's inverse. Also, $r^j r^k r^{-j} = r^k$ obviously, and $r^j s r^k s r^{-j} = r^j r^{-k} r^{-j} = r^{-k}$, so that's the extent of the conjugacy classes of powers of r. Then if n is even, there are $n/2+1$ conjugacy classes of powers of r, since $r^{n/2}$ and r^0 are their own inverses, and there are 2 conjugacy classes of elements of the form $r^k s$, so there are $n/2+3$ total. If n is odd, then there are $(n+1)/2$ conjugacy classes of powers of r, and only one of flips, so there are $(n+1)/2+1$ total. □

b) Write down the class equation for D_{2n} and identify the centralizer of each element.

Proof. If n is even, then $Z(D_{2n}) = 2$, and $2n = 2 + 2(n/2) + (n/2-1)(2)$, where the first 2 is the center, containing the identity and $r^{n/2}$, the two of size $n/2$ are the ones with s and rs respectively, and the final $(n/2-1)$ of order 2 are the conjugacy classes $\{r^k, r^{-k}\}$. The centralizer of each rotation class (except for the central one) must have order n, by the orbit-stabilizer theorem, and it's just the set $< r >$. The centralizer of the central elements is vacuously the whole group, and the centralizer of the $r^k s$'s must each have order 4; for each, it's the center, plus itself, and, since centralizers are closed, $r^{k+n/2}$; i.e. if $gh = hg$, and $gk = kg$, then $g(hk) = hgk = hkg = (hk)g$. If n is odd, the class equation is $2n = 1 + (n-1)/2(2) + n$, where the 1 is the size of the trivial center, the $(n-1)/2$ copies of 2 are the conjugacy classes $\{r^k, r^{-k}\}$, and the n is the number of flips. The centralizer of the identity is the whole element, the centralizer of the rotation classes is once again $< r >$, and the flips commute with just themselves and the identity. □

5) Let G be a group, $N \lhd G$ a normal subgroup, $H = G/N$ the quotient group, and $\pi : G \to H$ the quotient map. Let X be the set of conjugacy classes of the group N. The conjugacy class of $n \in N$ is denoted $[n]$.

a) For $g \in G$ and $n \in N$, let $g([n]) = [gng^{-1}]$. Show that this is a well-defined action of G on X.

Note that $gng^{-1} \in N$ for any $g \in G$, since $N \lhd G$. To show that G acts on X, we verify the following:

- identity: for $1 \in G$, we have $1([n]) = [1n1^{-1}] = [n]$.
- composition: for $g_1, g_2 \in G$, we have $(g_1 g_2)([n]) = [g_1 g_2 n (g_1 g_2)^{-1}] = [g_1 g_2 n g_2^{-1} g_1^{-1}] = g_1([g_2 n g_2^{-1}]) = g_1(g_2([n]))$.

To show that the action is well-defined, we see that if $[n_1] = [n_2]$, then there exists $n \in N$ such that $n n_1 n^{-1} = n_2$, so $g([n_1]) = [g n_1 g^{-1}] = [(gng^{-1}) g n_1 g^{-1} (gng^{-1})^{-1}] = [g n n_1 n^{-1} g^{-1}] = g([n n_1 n^{-1}]) = g([n_2])$.

b) Write down the class equation for this action.

Recall that if G acts on X, then in general the orbit equation is

$$|X| = |X^G| + \sum_A [G : G_A]$$

where X^G is the set of elements of X which are fixed by all $g \in G$, and A runs over the orbits in X, and G_A is the subgroup of G which stabilizes A. Thus, in this case the class equation is $|X| = |X^G| + \sum_A [G : \mathcal{N}_G(A)]$.

c) Suppose N is abelian. Show that there is an action of H on X such that $g([n]) = \pi(g)([n])$ for all $n \in N$, $g \in G$.

Since $\pi : G \to H$ is surjective, the equation $\pi(g)([n]) = g([n])$ specifies an action of H on X. [Since π is a homomorphism, we have $\pi(1)([n]) = 1([n]) = [n]$ and

$$(\pi(g_1)\pi(g_2))([n]) = \pi(g_1 g_2)([n]) = (g_1 g_2)([n]) = g_1(g_2([n])) = g_1(\pi(g_2)([n])) = \pi(g_1)(\pi(g_2)([n]))$$

so this is indeed an action.] We must show that this action is well-defined.
Suppose $\pi(g_1) = \pi(g_2)$; that is, there exists $m \in N$ such that $g_1 = g_2 m$. Then

$$g_1([n]) = [g_1 n g_1^{-1}] = [g_2 m n m^{-1} g_2^{-1}] = g_2([m n m^{-1}]) = g_2([n])$$

so $(\pi(g_1))([n]) = (\pi(g_2))([n])$. Hence this action is well-defined.

6) Construct two non-isomorphic, non-abelian groups of order 168, each of which contains a normal abelian subgroup of order 8.

Consider $G_1 = \mathbb{Z}_8 \times (\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ and $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$.
Since there is an injective homomorphism $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_7)$, with $\varphi_m \in \mathrm{Aut}(\mathbb{Z}_7)$ mapping $n \in \mathbb{Z}_7$ to $2^m n \in \mathbb{Z}_7$, we have $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3) := \{(n, m) : n \in \mathbb{Z}_7, m \in \mathbb{Z}_3\}$, with $(n_1, m_1)(n_2, m_2) = (n_1 \varphi_{m_1}(n_2), m_1 m_2)$. Observe that $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ is non-abelian; e.g., $([1], [1])([1], [0]) = ([3], [1]) \neq ([2], [1]) = ([1], [0])([1], [1])$.
Thus, for G_1, we have:

- The order of G_1 is $|G_1| = |\mathbb{Z}_8 \times (\mathbb{Z}_7 \rtimes \mathbb{Z}_3)| = |\mathbb{Z}_8|\,|\mathbb{Z}_7 \rtimes \mathbb{Z}_3| = 8 \cdot 21 = 168$.
- G_1 is non-abelian, since $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ is isomorphic to a subgroup of G_1, and $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ is non-abelian.
- G_1 contains a normal abelian subgroup of order 8: Define the subgroup $H_1 := \mathbb{Z}_8 \times \{([0], [0])\} \subseteq G_1$; we have $|H_1| = 8$. For any $(a, [n], [m]) \in G_1$ and $(b, [0], [0]) \in H_1$, we have

  $$(a, [n], [m])(b, [0], [0]) = (a + b, [n], [m]) = (b + a, [n], [m]) = (b, [0], [0]) \cdot (a, [n], [m])$$

  that is, the elements of H_1 commute with every element in G_1. This certainly implies that $H_1 \lhd G_1$.

Similarly, for G_2, we have:

- The order of G_2 is $|G_2| = |(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_7 \rtimes \mathbb{Z}_3)| = |\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2|\,|\mathbb{Z}_7 \rtimes \mathbb{Z}_3| = 8 \cdot 21 = 168$.
- G_2 is non-abelian, since $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ is isomorphic to a subgroup of G_1, and $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ is non-abelian.
- G_2 contains a normal abelian subgroup of order 8: Define the subgroup $H_2 := (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \{([0], [0])\} \subseteq G_2$; we have $|H_2| = 8$. By the same reason as above, the elements of H_2 commute with every element of G_2, which implies that $H_2 \lhd G_2$.

Finally, we observe that $([1], [0], [0]) \in G_1$ has order 8. The possible orders in $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$ are 1 and 2, and by Lagrange's theorem the possible orders in $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)$ are 1, 3, 7, 21; so no element in G_2 can have order 8. This shows that G_1 is not isomorphic to G_2.

7) Show that there are no simple groups of order 38 and 40.

In a group of order $38 = 2 \cdot 19$, there must by Sylow's theorems exist a subgroup of order 19; but this is a subgroup of index 2, which must be normal. Hence a group of order 38 cannot be simple.
In a group of order $40 = 2^3 \cdot 5$, the Sylow 5-subgroups are subgroups of order 5; and by Sylow's theorems, the number of Sylow 5-subgroups must be a divisor of $40/5 = 8$ which is congruent to 1 (mod 5). Thus, there is a unique subgroup of order 5, so it must be normal. Hence a group of order 40 cannot be simple.

8) Let p be a prime number and let G be a finite p-group. Write down the steps of the proof that G is solvable.

Say G has order p^n and give a proof by induction on n. For $n = 0$ there is nothing to prove. For the inductive step, it suffices to show that G has non-trivial normal subgroup $1 \neq N \lhd G$, $N \neq G$, since then by induction G/N and N will be solvable, and from this it follows that so is G. To do this, use the class equation to prove that $Z(G) \neq 1$:

$$\#Z(G) = \#G - \sum_{\text{non-trivial orbits} O} \#O$$

and the right hand side is divisible by p hence so is the left. Now we have two cases. Either $Z(G) \neq G$, in which case $Z(G)$ is the sought after normal subgroup, or $Z(G) = G$, in which case G is abelian, hence solvable.

9) Write down the class equation for the groups K_4, Q_8, and S_4.

K_4 is abelian of order 4 so the conjugacy classes are all singletons and $Z(K_4) = K_4$. Thus the class equation reads $4 = \#K_4 = \#Z(K_4) = 4$ here. Q_8 has center $\{\pm 1\}$ and the non-trivial conjugacy classes are $\{\pm i\}, \{\pm j\}, \{\pm k\}$ (use that for all $x, y \in Q_8$, either $xy = yx$ or $xy = -1yx$). Thus equation reads $8 = 2 + 2 + 2 + 2$, where the first 2 is the order of the center and the other three are the orders of the non-trivial conjugacy classes. Finally, the conjugacy classes of S_4 correspond to the partitions of 4. These are

$$4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$$

There are $6 = 4!/4$ 4-cycles, $8 = 4 \cdot 3 \cdot 2/3$ 3-cycles, $3 = 4!/(2 \cdot 2 \cdot 2)$ permutations of type $(2, 2)$, $6 = 4 \cdot 3/2$ transpositions, and only the identity is in the remaining conjugacy class. The center of S_n is trivial for $n \geq 3$, so the class equation reads

$$24 = 4! = 6 + 8 + 3 + 6 + 1$$

Note, the key to counting these is that there are k distinct representations of a k-cycle as for instance $(1 \dots k) = (2 \dots k1) = (3 \dots k12) = \cdots (k1 \dots k-1)$. For a product of two distinct transpositions we have to divide by an extra 2 because e.g. $(12)(34) = (34)(12)$.

10) Let G be a group, let $H \subseteq G, K \trianglelefteq G$ two subgroups, with K normal. Suppose the derived subgroup $D(H) \subset H$ is strictly smaller than H and $H \cap K = \{e\}$.

Prove that HK has a normal subgroup J such that HK/J is abelian and $|HK/J| > 1$.

By the second isomorphism theorem, $HK/K \cong H/H \cap K = H$, thus we know $D(HK/K)$ is strictly smaller than HK/K. Set $J = \pi^{-1}(D(HK/K))$ where $\pi : HK \to HK/K$ is the canonical map. Then $HK/J \cong (HK/K)/(D(HK/K))$ by the third isomorphism theorem, and we know the right hand group is abelian of order > 1.