College of the Holy Cross, Fall Semester, 2018
MATH 351, Final Examination Solutions
Friday, December 14

I. Both parts of this question deal with $SL(2,\mathbb{Z})$, the set of 2×2 integer matrices of determinant 1, a group under matrix multiplication. Let

$$H = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) : c \equiv 0 \bmod 5 \right\}.$$

(A) (*) (15) Is H a subgroup of $SL(2,\mathbb{Z})$? Why or why not?

Solution: The answer is *yes*. First, the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (the identity element in $SL(2,\mathbb{Z})$ is in H since the element in the second row and first column is $0 \equiv 0 \bmod 5$. Next, if $A = \begin{pmatrix} a & b \\ 5k & d \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 5k' & d' \end{pmatrix}$ are elements of H, then the matrix product

$$AB = \begin{pmatrix} a & b \\ 5k & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 5k' & d' \end{pmatrix} = \begin{pmatrix} aa' + 5bk' & ab' + bd' \\ 5(ka' + dk') & 5kb' + dd' \end{pmatrix}$$

has lower left entry divisible by 5. Finally, if $A = \begin{pmatrix} a & b \\ 5k & d \end{pmatrix}$ is in H, then

$$A^{-1} = \begin{pmatrix} d & -b \\ -5k & a \end{pmatrix}$$

since $\det(A) = 1$. This matrix is also in H, so H is a subgroup of $SL(2,\mathbb{Z})$.

(B) (*) (15) Is the cyclic subgroup generated by

$$A = \begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix}$$

in G finite or infinite? Explain.

Solution: It is easy to see, and easy to prove by induction, that

$$A^k = \begin{pmatrix} 1 & 0 \\ 5k & 1 \end{pmatrix}$$

for all $k \in \mathbb{Z}$. Since $A^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ only when $k = 0$, this shows that the matrix A is an element of infinite order, and the cyclic subgroup generated by A is infinite.

II. Let $G = \langle a \rangle$ be a cyclic group of order 100.

(A) (*) (10) How many different generators does G have?

Solution: The number is $\phi(100)$ (the Euler phi-function). Since $100 = 2^2 \cdot 5^2$, $\phi(100) = 2^1 \cdot (2-1) \cdot 5^1 \cdot (5-1) = 40$. The generators themselves are the powers a^i where $\gcd(i, 100) = 1$.

(B) (*) (10) What is the order of the element a^{30} in G?

Solution: The order is

$$|a^{30}| = \frac{100}{\gcd(100, 30)} = \frac{100}{10} = 10.$$

(Alternately, one could compute powers of a^{30} until an exponent divisible by 100 is obtained.)

(C) (*) (10) Suppose you know that a subgroup H of G contains both a^{30} and a^{56}. What can you say about the order of H?

Solution: We see $\gcd(30, 56) = 2$. Moreover, because H is a subgroup of G, repeating the steps of the Euclidean algorithm in the exponents, we find:

$$56 = 1 \cdot 30 + 26 \Rightarrow a^{56} \cdot a^{-30} = a^{26} \in H \tag{1}$$

$$30 = 1 \cdot 26 + 4 \Rightarrow a^{30} \cdot a^{-26} = a^4 \in H \tag{2}$$

$$26 = 4 \cdot 6 + 2 \Rightarrow a^{26} \cdot a^{-24} = a^2 \in H. \tag{3}$$

Hence there are two possibilities: Either H is all of G and $|H| = 100$, or else $H = \langle a^2 \rangle$, which says $|H| = 50$.

III. (A) (10) Let $\alpha : G \to H$ be a group homomorphism. Show that $\alpha(G)$ is a subgroup of H.

Solution: For all group homomorphisms $\alpha(e_G) = e_H$. Hence $e_H \in \alpha(G)$. If $c, d \in \alpha(G)$, then $c = \alpha(a)$ and $d = \alpha(b)$ for some $a, b \in G$. Therefore, since α is a group homomorphism,

$$c \cdot d = \alpha(a) \cdot \alpha(b) = \alpha(a \cdot b).$$

This shows $c \cdot d \in \alpha(G)$. Finally, if $c = \alpha(a)$, then

$$c^{-1} = (\alpha(a))^{-1} = \alpha(a^{-1}).$$

It follows that $c^{-1} \in \alpha(G)$. Therefore $\alpha(G)$ is a subgroup of H.

(B) (20) *State and prove* the First Isomorphism Theorem for groups.

Solution: The First Isomorphism Theorem states that if $\alpha : G \to H$ is a group homomorphism, then the image $\alpha(G)$ is isomorphic as a group to $G/\ker(\alpha)$. To prove this we will simplify the notation by writing $\ker(\alpha) = N$ and consider the mapping

$$\begin{aligned} \phi : G/N &\longrightarrow \alpha(G) \\ gN &\longmapsto \alpha(g) \end{aligned}$$

Since this mapping is defined with domain a factor group, we need to start by showing that it is well-defined. If the cosets gN and $g'N$ are equal, though, $g^{-1}g' \in N$ and this implies $\alpha(g^{-1}g') = (\alpha(g))^{-1}\alpha(g') = e_H$. It follows that $\alpha(g) = \alpha(g')$, so the mapping ϕ is well-defined. Next, we claim that ϕ is a group homomorphism. This follows from the way the coset product is defined in the factor group:

$$\phi(gN \cdot g'N) = \phi((gg')N) = \alpha(gg') = \alpha(g) \cdot \alpha(g') = \phi(gN) \cdot \phi(g'N).$$

This shows ϕ is a gorup homomorphism. Since every element g in G yields some coset of the kernel, every $\alpha(g)$ for $g \in G$ is in the image of ϕ, so the mapping ϕ is surjective. So, it remains to show that ϕ is injective. Suppose

$$\phi(gN) = \alpha(g) = \alpha(g') = \phi(g'N).$$

This shows that

$$(\alpha(g))^{-1} \cdot \alpha(g') = \alpha(g^{-1}g') = e_H,$$

so $g^{-1}g' \in N$, and we know that that implies the cosets of g and g' are equal: $gN = g'N$. Therefore ϕ is also injective, and we have shown that ϕ is an isomorphism of groups, which is what we had to do.

IV. All parts of this question refer to the group G of order 8 whose (corrected!) operation table is given below:

$\cdot$	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_2	g_2	g_5	g_4	g_7	g_6	g_1	g_8	g_3
g_3	g_3	g_8	g_5	g_2	g_7	g_4	g_1	g_6
g_4	g_4	g_3	g_6	g_5	g_8	g_7	g_2	g_1
g_5	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_6	g_6	g_1	g_8	g_3	g_2	g_5	g_4	g_7
g_7	g_7	g_4	g_1	g_6	g_3	g_8	g_5	g_2
g_8	g_8	g_7	g_2	g_1	g_4	g_3	g_6	g_5

(A) (*) (5) What is the inverse of the element g_2?

Solution: By inspection of the table, we see g_1 is the identity element. Since $g_2 \cdot g_6 = g_6 \cdot g_2 = g_1$, the inverse of g_2 is g_6.

(B) (*) (5) What elements are in the subgroup $\langle g_3 \rangle$?

Solution: We see $g_3^2 = g_5$, $g_3 \cdot g_5 = g_7$ and $g_3 \cdot g_7 = g_1$. Therefore, g_3 has order 4 and

$$\langle g_3 \rangle = \{g_1, g_3, g_5, g_7\}.$$

(C) (*) (5) Is the subgroup $\langle g_3 \rangle$ normal in G? Why or why not?

Solution: Since $|\langle g_3 \rangle| = 4 = \frac{1}{2}|G|$, this subgroup is normal in G.

(D) (*) (5) What is the center of G, that is, the subgroup $Z(G)$?

Solution: By inspection of the table, the elements that commute with all elements of G are g_1 and g_5. Therefore

$$Z(G) = \{g_1, g_5\}.$$

(E) (20) Construct the group table for the factor group $G/Z(G)$. To which "standard" group is this isomorphic?

Solution: The distinct left cosets of $N = Z(G)$ are

$$N, g_2N = \{g_2, g_6\}, g_3N = \{g_3, g_7\}, g_4N = \{g_4, g_8\}$$

The group table for the factor group is found using the usual coset product

$\cdot$	N	g_2N	g_3N	g_4N
N	N	g_2N	g_3N	g_4N
g_2N	g_2N	N	g_4N	g_3N
g_3N	g_3N	g_4N	N	g_2N
g_4N	g_4N	g_3N	g_2N	N

This is a non-cyclic group of order 4, hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Note: This group of order 8 is isomorphic to the *quaternion group*, Q, the last of the order 8 groups that we just "met" the last day of class. You didn't need to know that to do any part of this problem, though!

V. (A) (15) Up to isomorphism, how many different *abelian* groups of order 600 are there? List one group from each isomorphism class.

Solution: Since $600 = 2^3 \times 3 \times 5^2$, there are three possible structures for the 2-subgroup, one for the 3-subgroup, and two for the 5-subgroup. By the fundamental theorem of finite abelian groups, the following list includes all the possibilities, up to isomorphism:

$$\begin{aligned}
&\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\
&\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
&\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\
&\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\
&\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5
\end{aligned}$$

(B) (15) Up to isomorphism, how many different groups of order 2018 are there? List one group from each isomorphism class. (Hint: This is *not* a long list!)

Solution: Factoring we find $2018 = 2 \cdot 1009$, and 1009 is an odd prime. (This takes some checking, but it is routine; you just have to check that none of the primes $3, 5, 7, 11, 13, 17, 19, 23, 29, 31$ divides 1009. Those are the primes $\leq \sqrt{1009}$.) In this situation we know that there are only two isomorphism classes of groups of order $2p$, namely, every group of order 2018 is isomorphic to either

$$\mathbb{Z}_{2018} \quad \text{or} \quad D_{2018}$$

(D_{2018} is the dihedral group of rotational and reflection symmetries of a regular 1009-gon, which would be hard to distinguish from a circle if you drew it – unless the edges were made very long, of course!).

VI. (A) (20) Use the Sylow Theorems to show that there are no simple groups of order 100.

Solution: We have $100 = 2^2 \cdot 5^2$. By Sylow III, the number of Sylow 5-subgroups must be congruent to 1 mod 5 and it must divide 4. The only possible number is 1, and Sylow II implies that subgroup must be a normal subgroup of order 25. Hence if $|G| = 100$, then G is not a simple group.

(B) (20) How many different Sylow 5-subgroups does the alternating group A_5 have?

First Solution: The alternating group A_5 has order $\frac{1}{2} \cdot 5! = 60$. This factors as $60 = 2^2 \cdot 3 \cdot 5$. The Sylow 5-subgroups must have order 5, and hence are cyclic since 5 is prime. The only elements of order 5 in A_5 (or S_5) are the 5-cycles $(abcde)$, where $\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}$. There are $\frac{5!}{5} = 24$ distinct 5-cycles, but groups of 4 of them generate the same subgroup since if σ is one of the 5-cycles, $\sigma^2, \sigma^3, \sigma^4$ all generate the same subgroup as σ. Hence the number of distinct Sylow 5-subgroups is $\frac{24}{4} = 6$. Note that this agrees with the statement of Sylow III. The number of Sylow 5-subgroups in a group of order 60 is congruent to 1 mod 5 and divides 12, hence is either 1 or 6.

Second Solution: ("sneaky") By Sylow III, the number of Sylow 5-subgroups in a group of order 60 is congruent to 1 mod 5 and divides 12, hence is either 1 or

6. If there is just one Sylow 5-subgroups, then Sylow II implies that subgroup is normal, of order 5. However, we know that A_5 is a simple, nonabelian group, so it has no normal subgroups other than $\{e\}$ and A_5. Therefore, the number must be 6(!)