College of the Holy Cross, Fall Semester, 2018
MATH 351, Midterm 1 Solutions
Thursday, October 4

I. Let $G = \mathrm{SL}(2, \mathbb{Z})$, the set of 2×2 integer matrices with determinant 1, which is a group under the operation of matrix multiplication. Let

$$H = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid b \equiv 0 \bmod 4 \right\}.$$

(A) (15) Is H a subgroup of G? Why or why not?

Solution: H is a subgroup of G. Here's a proof. First, the identity element in G, namely the 2×2 identity matrix:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is in H since the upper right entry is $0 \equiv 0 \bmod 4$. Next if

$$A = \begin{pmatrix} a & 4k \\ c & d \end{pmatrix}, \quad \text{and} \quad B = \begin{pmatrix} e & 4\ell \\ f & g \end{pmatrix}$$

are elements of H, then the product

$$\begin{aligned} A^{-1}B &= \begin{pmatrix} d & -4k \\ -c & a \end{pmatrix} \begin{pmatrix} e & 4\ell \\ f & g \end{pmatrix} \\ &= \begin{pmatrix} de - 4kf & 4ld - 4kg \\ -ce + af & -4\ell c + ag \end{pmatrix}. \end{aligned}$$

The upper right entry in the product is $4(ld - kg)$ and l, d, k, g are all integers, so this element is $\equiv 0 \bmod 4$. Hence $A^{-1}B \in H$ and H is a subgroup of G.

(B) (10) Compute this matrix product, noting that the left and right matrices are inverses of each other and the middle matrix is in H:

$$\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 8 \\ 1 & 9 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

What does the result tell you about the subgroup H?

Solution: All the matrices are in G, since they are all integer matrices with determinant equal to 1. The product is

$$\begin{pmatrix} -69 & 47 \\ -116 & 79 \end{pmatrix}$$

Note that the upper right entry is $47 \equiv 3 \bmod 4$, not $0 \bmod 4$. Hence this product is *not an element of H*. It follows that H is *not a normal subgroup of G*.

II. (A) (15) Let $G = \langle a \rangle$ be a cyclic group. Prove that every subgroup of G is also cyclic.

Solution: Let H be any subgroup of G. If $H = \{e = a^0\}$ then $H = \langle e \rangle$, so H is cyclic. Otherwise, let $a^k \in H$, where k is the smallest strictly positive power of a for which this holds. Since H is a subgroup, this means that every power of a^k is also in H, and hence $\langle a^k \rangle \subseteq H$. Now to show the other containment, every other element of H is in G, so it has the form a^n for some n. Use division in $\mathbb{Z}$ to divide k into n. This means that we can write $n = qk + r$, where $0 \leq r < n$. Since $a^n \in H$ and $a^k \in H$, $a^r = a^n \cdot (a^k)^{-q} \in H$. But by the choice of k, this implies $r = 0$ and $a^r = e$. Hence $a^n = (a^k)^q \in \langle a^k \rangle$. Hence since a^n was an arbitrary element of H, we also have $H \subseteq \langle a^k \rangle$. Therefore, $H = \langle a^k \rangle$ is cyclic. This is what we had to show.

(B) (5) In part (A), suppose that a has order 120. List all the integers that are orders of elements of G.

Solution: The orders are the divisors of 120:

$$1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120.$$

(C) (10) Still assuming a has order 120, how many elements of G have order 24? What are they?

Solution: There are $\phi(24)$ of them. Since $24 = 2^3 \cdot 3$, this number is $\phi(24) = 2^2 \cdot (2 - 1) \cdot (3 - 1) = 8$. To find them, recall that we want the a^i for which $\frac{120}{\gcd(120,i)} = 24$, so $\gcd(120, i) = 5$. The i that work are $i = 5, 25, 35, 55, 65, 85, 95, 115$.

III. (A) (10) Let H be a subgroup of a group G. Show that $aH = bH$ if and only if $a^{-1}b \in H$.

Solution: $\Rightarrow$: Suppose that $aH = bH$. Then for every $h \in H$ there exists $h' \in H$ such that $ah = bh'$. Multiplying by a^{-1} on the left and h'^{-1} on the right we get $a^{-1}b = h(h')^{-1}$. Since H is a subgroup and $h, h' \in H$, $h(h')^{-1} \in H$. Hence $a^{-1}b \in H$.

$\Leftarrow$: Suppose that $a^{-1}b \in H$. Then for all $h \in H$, we have $a^{-1}bh = h' \in H$. Hence $bh = ah'$. This implies $bH \subseteq aH$. Since the left cosets of H in G partition G, this implies that $bH = aH$. (Recall any two left cosets are either identical or disjoint.)

(B) (15) Let $G = S_3$ and let

$$H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\rangle.$$

Find all of the left and right cosets of H in G.

Solution: The generator for H is an element of order 2 in S_3. Hence

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Since $|G| = 6$ and $|H| = 2$, there are 3 left cosets and 3 right cosets. The distinct left cosets are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} H = H$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

The right cosets are computed similarly:

$$H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = H$$
$$H \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$
$$H \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

IV. Let G be a group containing subgroups H and K with $|H| = 28$ and $|K| = 65$.

(A) (10) What is the smallest possible value for $|G|$?

Solution: By Lagrange's Theorem, $|G|$ must be divisible by both $28 = 2^2 \cdot 7$ and $65 = 5 \cdot 13$. Since these two integers are relatively prime, $\operatorname{lcm}(28, 65) = 28 \cdot 65 = 1820$.

(B) (10) Show that $H \cap K = \{e\}$.

Solution: By Lagrange's Theorem again, the intersection $H \cap K$ is a subgroup of both H and K, so its order must divide both 28 and 65. Since $\gcd(28, 65) = 1$, the intersection can contain only the identity element: $H \cap K = \{e\}$.