Exam 1 Solutions Math 641 Fall 2014

Instructions: Group theory is rich in definitions and theorems. When using a theorem, make sure to cite the theorem clearly and prove that the hypotheses are met. When you state that a hypothesis is met, make sure to prove that all definitions are satisfied. Unsupported claims will receive no credit. Properties proved in class do not need to be reproved. Keep your solutions brief and to the point. A well-thought-out proof does not need to go on for pages.

1. Let

$$G = \left\{ \begin{bmatrix} \widehat{a} & \widehat{b} \\ \widehat{c} & \widehat{d} \end{bmatrix} : \widehat{a}, \widehat{b}, \widehat{c}, \widehat{d} \in \mathbb{Z}_5 \text{ and } \det \begin{bmatrix} \widehat{a} & \widehat{b} \\ \widehat{c} & \widehat{d} \end{bmatrix} \neq \widehat{0} \right\}$$

and

$$H = \left\{ \begin{bmatrix} \widehat{a} & \widehat{b} \\ \widehat{c} & \widehat{d} \end{bmatrix} \in G : \det \begin{bmatrix} \widehat{a} & \widehat{b} \\ \widehat{c} & \widehat{d} \end{bmatrix} = \widehat{1} \right\}.$$

(a) You can assume that G is a group under matrix multiplication. Prove that G is non-abelian and contains 480 elements.

(b) By Cauchy's theorem, G has an element of order 5. Find one.

(c) Prove that H is a normal subgroup of G.

(d) Prove that for each $m \in G$, $Hm = \{g \in G : \det(g) = \det(m)\}$.

(e) Prove that $G/H \cong \mathbb{Z}_4$ where the group operation in $\mathbb{Z}_4$ is addition.

Solutions:

(a) Let $g_1 = \begin{bmatrix} \widehat{1} & \widehat{1} \\ \widehat{0} & \widehat{1} \end{bmatrix}$, $g_2 = \begin{bmatrix} \widehat{1} & \widehat{1} \\ \widehat{1} & \widehat{0} \end{bmatrix}$. Then $g_1 g_2 = \begin{bmatrix} \widehat{2} & \widehat{1} \\ \widehat{1} & \widehat{0} \end{bmatrix}$ and $g_2 g_1 = \begin{bmatrix} \widehat{1} & \widehat{2} \\ \widehat{1} & \widehat{0} \end{bmatrix}$, hence G is not abelian.

There are $5^4 = 625$ matrices with entries in $\mathbb{Z}_5$. We will count the number that have zero determinant, then subtract from 625. We are really counting all $(a, b, c, d) \in \{0, 1, 2, 3, 4\}^4$ such that $ad \equiv bc \bmod 5$. There are 9 solutions to $xy \equiv 0 \bmod 5$, 4 solutions to $xy \equiv 1 \bmod 5$, 4 solutions to $xy \equiv 2 \bmod 5$, 4 solutions to $xy \equiv 3 \bmod 5$, and 4 solutions to $xy \equiv 4 \bmod 5$. Hence there are $9^2 + 4^2 + 4^2 + 4^2 + 4^2 = 145$ matrices with determinant $\widehat{0}$, leaving $625 - 145 = 180$ matrices with non-zero determinant.

An alternate solution is this: there are $5^2 - 1 = 24$ possible choices for the first column. Given that there are $5^2 - 5 = 20$ possible choices for the second column (cannot be a multiple of the first column), the total number of matrices in G is $24 \cdot 20 = 480$.

(b) If g has order 5 and determinant $\widehat{d}$ then $\widehat{d^5} = \widehat{1}$. This is only possible if $d \equiv 1 \bmod 5$. So a strategy to follow is to look for a determinant $\widehat{1}$ matrix g which satisfies $g^5 = e$. A matrix that works is $g = \begin{bmatrix} \widehat{1} & \widehat{1} \\ \widehat{0} & \widehat{1} \end{bmatrix}$. Since $g^5 = e$, $o(g)|5$. Since $o(g) \neq 1$, $o(g) = 5$.

(c) H is the kernel of the homomorphism $\phi : G \to \mathbb{Z}_5^*$ given by $\phi(g) = \det(g)$. Kernels are normal subgroups.

An alternate solution is this: $h_1, h_2 \in H$ implies $\det(h_1 h_2^{-1}) = \det(h_1)\det(h_2)^{-1} = 1 \cdot (1)^{-1} = 1$ implies $h_1 h_2^{-1} \in H$, hence H is a subgroup of G. Moreover $g \in G$ and $h \in H$ implies $\det(ghg^{-1}) = \det(g)\det(h)\det(g)^{-1} = \det(g) \cdot 1 \cdot \det(g)^{-1} = 1$ implies $ghg^{-1} \in H$, hence H is normal in G.

Note that is not sufficient merely to prove that ghg^{-1} for all $g \in G$, $h \in G$. Example: $G = \mathcal{S}_5$, $H =$ set of all 3-cycles in H. H is not a subgroup of $\mathcal{S}_n$ since it doesn't contain the identity permutation, but $\sigma(a, b, c)\sigma^{-1} = (\sigma(a), \sigma(b), \sigma(c)) \in H$.

(d) We proved in class that $\{g \in G : \phi(g) = \phi(m)\} = Km$ where K is the kernel of ϕ (defined in (c)). Since $K = H$, we have $\{g \in G : \det(g) = \det(m)\} = Hm$.

Alternate solution: Let LHS $= Hm$ and RHS $= \{g \in G : \det(g) = \det(m)\}$. We must show LHS $\subseteq$ RHS and RHS $\subseteq$ LHS.

$hm \in$ LHS implies $\det(hm) = \det(h)\det(m) = \det(m)$, hence $hm \in$ RHS. So we have LHS $\subseteq$ RHS.

$g \in$ RHS implies $\det(g) = \det(m)$ implies $\det(gm^{-1}) = \det(g)\det(m)^{-1} = 1$ implies $gm^{-1} \in H$ implies $g = (gm^{-1})m \in Hm$. So we have RHS $\subseteq$ LHS.

(e) Let $g_a = \begin{bmatrix} \widehat{a} & 0 \\ 0 & 1 \end{bmatrix}$. Then $G/H = \{Hg_1, Hg_2, Hg_3, Hg_4\}$. Since $(g_2, g_2^2, g_2^3, g_2^4) = (g_2, g_4, g_3, g_1)$, we have $G/H = \langle Hg_2 \rangle$. Hence G/H is cyclic of order 4 and is isomorphic to $\mathbb{Z}_4$ under addition.

Alternative solution: define $\psi : \mathbb{Z}_4 \to G/H$ via $\psi([a]_4) = Hg_{2^a}$ where $g_{2^a} = \begin{bmatrix} \widehat{2^a} & 0 \\ 0 & 1 \end{bmatrix}$. Well-defined: $[a]_4 = [b]_4$ implies $a = b + 4k$ implies $2^a = (2^b)(16^k) \equiv$

$2^b \bmod 5$, therefore $g_{2^a} = g_{2^b}$, therefore $Hg_{2^a} = Hg_{2^b}$, therefore $\psi([a]_4) = \psi([b]_4)$. Bijective: $(\psi([0]), \psi([1]), \psi([2]), \psi([3])) = (Hg_1, Hg_2, Hg_4, Hg_8) = (Hg_1, Hg_2, Hg_4, Hg_3)$. Homomorphism: $\psi([a] + [b]) = \psi([a + b]) = Hg_{2^{a+b}} = Hg_{2^a} Hg_{2^b} = \psi([a])\psi([b])$. Hence ψ is an isomorphism between $\mathbb{Z}_4$ and G/H.

2. In the following problems, $\mathcal{S}_n$ is the group of permutations of $\{1, 2, \ldots, n\}$ under function composition.

(a) Prove that if $\sigma \in \mathcal{S}_n$ factors into disjoint cycles as $\sigma_1 \cdots \sigma_k$ then

$$o(\sigma) = \operatorname{lcm}(o(\sigma_1), o(\sigma_2), \ldots, o(\sigma_k)).$$

(b) Let p be a prime. Prove that if $\sigma \in \mathcal{S}_n$ satisfies $o(\sigma) = p$ then σ is a product of disjoint p-cycles.

(c) Find permutations σ and τ satisfying

$$\gcd(o(\sigma\tau), o(\sigma)) = \gcd(o(\sigma\tau), o(\tau)) = 1.$$

Solutions:

(a) Write $o(\sigma) = m$. Since disjoint cycles commute with each other, for any integer a we have

$$\sigma^a = \sigma_1^a \cdots \sigma_k^a.$$

If a is any common multiple of $o(\sigma_1), \ldots, o(\sigma_k)$ then $\sigma^a = e$ since each $\sigma_i^a = e$. Therefore

$$m \leq \operatorname{lcm}(o(\sigma_1), o(\sigma_2), \ldots, o(\sigma_k)).$$

Writing $m = q_i o(\sigma_i) + r_i$ for each i, where $0 \leq r_i < o(\sigma_i)$, we have

$$e = \sigma^m = \sigma_1^{r_1} \cdots \sigma_k^{r_k}.$$

Since the $\sigma_i^{r_i}$ move different elements, we must have $\sigma_i^{r_i} = e$ for each i. This forces $r_1 = \cdots = r_k = 0$. Hence $o(\sigma_i) | m$ for each i and

$$m \geq \operatorname{lcm}(o(\sigma_1), o(\sigma_2), \ldots, o(\sigma_k)).$$

(b) The order of a cycle permutation is equal to the length of the cycle. σ is a disjoint product of cycles of length ≥ 2. If any one of these cycles has

length divisible by q where q is a prime not equal to p, then q is a divisor of the least common multiple of the lengths, hence the orders, of the disjoint cycles in σ. So each disjoint cycle has length p^i for some i. Since the least common multiple of these lengths is p, each disjoint cycle has length p.

(c) $\sigma = (1, 4, 5, 6, 7)$ has order 5, $\tau = (1, 2, 3)$ has order 3, $\sigma\tau = (1, 2, 3, 4, 5, 6, 7)$ has order 7.