

MATH 731, FALL 2008
HOMEWORK SET 7 sample solutions

- A. Suppose A, B, C are subgroups of G with $A \triangleleft B$, $C \triangleleft G$ and suppose $BC = G$. Prove that AC is a normal subgroup of G .

Proof. Since $C \triangleleft G$, we have seen before that AC is a subgroup. To show it is normal, let $x \in C, g \in G$. Then $x = ac$ and $g = bd$ for $a \in A, b \in B, c, d \in C$. Thus $g x g^{-1} = g a g^{-1} g c g^{-1}$. We know $g c g^{-1} \in C$, since C is normal.

We have $g a g^{-1} = b d a d^{-1} b^{-1} = b a b^{-1} b a^{-1} d a d^{-1} b^{-1}$. In this final expression, $b a b^{-1} \in A$ since $A \triangleleft B$ and $a^{-1} d a d^{-1} \in C$ because $d, d^{-1} \in C$ and $C \triangleleft G$. Thus $b(a^{-1} d a d^{-1}) b^{-1} \in C$. This shows $g a g^{-1} \in AC$, from which we conclude $g x g^{-1} \in AC$.

Here's an alternative from Michael. Define $\pi : G \rightarrow G/C$ by $\pi(g) = gC$. It's not hard to see that $\pi(A) = AC/C$ and $\pi(B) = BC/C$, and the latter is G/C since $BC = G$. Since $A \triangleleft B$, we have $\pi(A) \triangleleft \pi(B) = G/C$. The correspondence theorem for [normal] subgroups — Second Isomorphism Theorem — tells us $AC \triangleleft G$.

- B. Suppose G is an Abelian group that acts transitively on the set X .

(1) Show that G acts faithfully if and only if $g.x = x$ only happens when $g = e$ (regardless of what x is).

Proof. If G acts freely, then certainly it acts faithfully. Suppose conversely that G acts faithfully and there are g, x with $g.x = x$. Then for any $y \in X$, the transitivity of the action implies $h.x = y$ for some $h \in G$. Thus $g.y = g.(h.x) = (gh).x = (hg).x = h.(g.x) = h.x = y$. Since the action is faithful, this equality for all $y \in G$ implies $g = e$.

Note that a(n apparently) stronger conclusion is true. If $g, h \in G$ and x is any element of X , then $g.x = h.x$ implies $g = h$. To see this, note $g^{-1}h.x = x$, so $g^{-1}h = e$.

(2) Show that G acts doubly transitively and faithfully on X if and only if $|G| = |X| = 2$ and the non-identity element of G swaps the two elements of X .

Proof. If $|G| = |X| = 2$ and the non-identity element of G swaps the two elements of X , then the action is doubly transitive because there is only one choice of source pair (say x, y) and two choices of target pair (either x, y or y, x) and we can see exactly how to move elements. The action is clearly faithful.

Suppose conversely that G acts doubly transitively and faithfully, and let g_1, g_2 be non-identity elements of G . Pick any $x \in X$ and set $x' = g_1.x, y = g_2.x, y' = x$. By (1), $x \neq y$ and $x' \neq y'$. By double transitivity, there is an $h \in G$ with $h.x = x' = g_1.x$ and $h.g_2.x = h.y = y' = x$. By the stronger conclusion stated at the end of (1), these equalities imply $h = g_1$ and $h.g_2 = e$. Thus $g_1.g_2 = e$. This is true for any non-identity elements of G , so taking $g_1 = g_2 = g$, we see $g^2 = e$ for all g . Thus for all g_1, g_2 not the identity, we have $g_2 = g_1^{-1} = g_1$. This shows $|G| = 2$.

Since G acts faithfully, X must have at least the two elements $x = e.x$ and $g.x$, and since G acts transitively, X can have no more elements. Moreover, $g.(g.x) = g^2.x = x$, so the non-identity g does indeed swap x and $g.x$.

Here's an even better alternative for the main part, used by Andreas and Britta. Take any $g_1, g_2 \in G \setminus \{e\}$, take any $x \in X$ and set $x' = x, y = g_1.x, y' = g_2.x$. By part (1), we have $x \neq y, x' \neq y'$. Thus by double transitivity, there is an $h \in G$ with $h.x = x' = x$ and $(hg_1).x = h.y = y' = g_2.x$. By (1), the first equality implies $h = e$ and the second equality implies $hg_1 = g_2$. Thus $g_1 = g_2$. It follows that $|G| = 2$.

C. (1) Prove that if $n \geq 3$, every element of A_n is a product of 3-cycles.

Proof. This is true for all n if we understand the product of zero 3-cycles to be the identity. In particular, if $n \leq 2$, then $A_n = \{\text{id}\}$.

To demonstrate the claim, it is enough to show any product $(ab)(cd)$ of two 2-cycles (with $a \neq b, c \neq d$) is a product of 3-cycles. If a, b, c, d are all distinct, then this product is $(acb)(cda)$. If exactly three of a, b, c, d are distinct, we can rewrite the transpositions so that a, b, d are distinct and $b = c$. In this case, the product is just (abd) . If only two of a, b, c, d are distinct, then (after re-writing) the product must be $(ab)(ab) = \text{id}$, which is either a product of zero 3-cycles (my preference!) or the product of any 3-cycle with itself three times.

(2) Prove that if $n \geq 5$, every element of A_n is a product of permutations of the form $(ab)(cd)$ where a, b, c, d are distinct.

Proof. By (1), it is enough to show any 3-cycle is a product of two permutations of the above form. Let x, y, z be distinct and let v, w be two more numbers between 1 and n different from x, y, z . (We know v, w exist because $n \geq 5$.) Set $\sigma_1 = (xz)(vw)$ and $\sigma_2 = (vw)(xy)$. Then σ_1, σ_2 are of the appropriate type and $\sigma_1\sigma_2 = (xyz)$. This completes the proof.

We need the assumption $n \geq 5$. In A_4 , $\{\text{id}, (12)(34), (13)(24), (14)(23)\}$ is a proper subgroup containing all possible products of two disjoint transpositions.

D. Suppose F is a finite field with q elements (so $F = \mathbb{F}_q$). Explain the following equalities.

(1) $|\mathbb{P}^{n-1}(F)| = (q^n - 1)/(q - 1)$.

Proof. There are $q^n - 1$ nonzero elements of F^n , and each lies on exactly one line through the origin. Moreover, each such line contains $q - 1$ nonzero elements. Thus there are $(q^n - 1)/(q - 1)$ lines through the origin.

(2) $|GL_n(F)| = \prod_{i=0}^{n-1} (q^n - q^i) = q^{n(n-1)/2} \cdot (q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$.

Proof. An element of $GL_n(F)$ is a collection of n linearly independent columns. To obtain such a collection, we start with any nonzero column: there are $q^n - 1$ choices for this element. We next choose a column that is independent of the first column. To do that, we simply must avoid any of the q multiples of the first column, so we have $q^n - q$ choices for the second column.

Suppose we have chosen the first i columns (linearly independent). They span a subspace of F^n of dimension i ; this subspace has q^i elements. To choose a column $i + 1$ that preserves linear independence, we simply need to choose a column not in this subspace. This gives us $q^n - q^i$ choices for column $i + 1$.

It follows that the total number of possible choices in creating an element of $GL_n(F)$ is $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$. This is the product listed. The second expression is obtained from this by factoring out all possible powers of q .

To obtain $|SL_n(F)|$, note that $GL_n(F)$ contains $q - 1$ cosets of SL_n , so $|SL_n(F)| = |GL_n(F)|/(q - 1) = q^{n(n-1)/2} \cdot (q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)$.

To obtain $|PSL_n(F)|$, we must divide $|SL_n(F)|$ by the order of its center, which is the number of n^{th} roots of unity in F . This number is $\gcd(n, q - 1)$. Thus $|PSL_n(F)| = q^{n(n-1)/2} \cdot (q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)/\gcd(n, q - 1)$.