Math 6000, Fall 2017 (Prof. Kinser), Midterm

Nicholas Camacho

October 20, 2017

Problem 1. Suppose that G is a finite group and acts doubly transitively on a set with n elements. Prove that $n(n-1)$ divides $|G|$. Can you generalize this? (Just give the statement of a generalization.)

Solution:

We state and prove the general case:

Definition 1. Let G be a group and suppose G acts on a set X. We say that the action of G on X is *k-transitive* if for every

$$(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in X^{\oplus k} \setminus \Delta,$$

there exists $g \in G$ so that

$$(g \cdot x_1, \ldots, g \cdot x_k) = (y_1, \ldots, y_k),$$

where

$$\Delta = \{(x_1, \ldots, x_k) \in X^{\oplus k} \ \mid x_i \neq x_j \ \forall \ i \neq j\}.$$

Lemma 1 (General Orbit-Stabilizer Lemma)**.** *Let G be a group that acts on a set X, let $(x_1, \ldots, x_k)$ be in $X^{\oplus k}$, let $\mathcal{O}_{x_1,\cdots,x_k}$ denote the orbit of $(x_1, \ldots, x_k) \in X^{\oplus k}$, and let $G_{x_1,\ldots,x_k}$ denote the stabilizer subgroup of $(x_1, \ldots, x_k)$. Then*

$$|\mathcal{O}_{x_1,\ldots,x_k}| = [G : G_{x_1,\ldots,x_k}].$$

Proof. First, we show $G_{x_1,\ldots,x_k} \leq G$: Certainly $1_G \in G_{x_1,\ldots,x_k}$, and if $g, h \in G_{x_1,\ldots,x_k}$, then so is gh^{-1}:

$$(gh^{-1}x_1, \ldots, gh^{-1}x_k) = (gh^{-1}(hx_1), \ldots, gh^{-1}(hx_k)) = (gx_1, \ldots, gx_k) = (x_1, \ldots, x_k).$$

Let $\mathcal{C} = \{gG_{x_1,\ldots,x_k} : g \in G\}$ be the set of left cosets of $G_{x_1,\ldots,x_k}$ in G, and define a map

$$\begin{aligned} \mathcal{C} &\longrightarrow \mathcal{O}_{x_1,\cdots,x_k} \\ gG_{x_1,\ldots,x_k} &\longmapsto (gx_1, \ldots, gx_k). \end{aligned}$$

This map is well-defined and injective:

$$\begin{aligned} gG_{x_1,\ldots,x_k} = hG_{x_1,\ldots,x_k} \iff h^{-1}g \in G_{x_1,\ldots,x_k} &\iff (h^{-1}gx_1, \ldots, h^{-1}gx_k) = (x_1, \ldots, x_k) \\ &\iff (gx_1, \ldots, gx_k) = (hx_1, \ldots, hx_k). \end{aligned}$$

The map is clearly surjective. Hence $[G : G_{x_1,\ldots,x_k}] = |\mathcal{C}| = |\mathcal{O}_{x_1,\ldots,x_n}|$. ☕

Proposition 1 (Generalization of Problem 1)**.** *Let G be a finite group that acts k-transitively on a set X, $|X| = n < \infty$, (so $k \leq n$). Then $n(n-1)(n-2)\cdots(n-k+1)$ divides the order of G.*

Proof. Take $(x_1, \cdots, x_k) \in X^{\oplus k} \setminus \Delta$ in the lemma. Since G acts k-transitively on X, then it follows directly from the definition of k-transitive that $\mathcal{O}_{x_1,\ldots,x_n} = X^{\oplus k} \setminus \Delta$, and so

$$|\mathcal{O}_{x_1,\ldots,x_n}| = |X^{\oplus k} \setminus \Delta| = n(n-1)\cdots(n-k+1).$$

Hence by the lemma,

$$|G| = |\mathcal{O}_{x_1,\ldots,x_n}| \cdot |G_{x_1,\ldots,x_k}| = n(n-1)\cdots(n-k+1) \cdot |G_{x_1,\ldots,x_k}|.$$

☕

Problem 2. Recall that a *maximal subgroup* of a group G is a proper subgroup which is not contained in any proper subgroup but itself. Let $\Phi(G)$ be the intersection of all maximal subgroups of G, if it has any, and $\Phi(G) = G$ otherwise.

(a) Compute $\Phi(G)$ for each of $G = S_3,\ A_4,\ S_4,\ A_5,\ S_5$. In each case, your answer should be a description of the subgroup $\Phi(G)$ and a *brief* argument, not solely a list of computations.

Solution:

- $\boldsymbol{S_3}$: Any nontrivial proper subgroup of S_3 is maximal, by an order argument. So we intersect at least two subgroups of relatively prime order, giving $\Phi(S_3) = \{()\}$.
- $\boldsymbol{A_4}$: First notice that A_4 does not contain a subgroup of order 6: The only groups of order 6 are $\mathbb{Z}_6$ and S_3, but no element of A_4 has order 6, and A_4 does not contain the odd permutations (which do lie in S_3). Hence the only proper nontrivial subgroups of A_4 are of orders 3 and 4, which must all be maximal by an order argument. So again, we intersect at least two subgroups of relatively prime order, giving $\Phi(A_4) = \{()\}$.
- $\boldsymbol{S_4}$: Since 12 is the only multiple of 12 that is a proper divisor of $|S_4| = 24$, then A_4 is maximal. Similarly, since 8 is the only multiple of 8 that is a proper divisor of 24, any subgroup of S_4 of order 8 is maximal. We saw in Homework 1 that S_4 has 3 Sylow 2-subgroups,:

$$\begin{aligned}
H &= \langle (1234), (24) \rangle = \{(), (1234), (24), (13)(24), (1432), (12)(34), (13), (14)(23)\}, \\
K &= \langle (1342), (14) \rangle = \{(), (1342), (14), (14)(23), (1243), (12)(34), (23), (13)(24)\}, \\
L &= \langle (1423), (12) \rangle = \{(), (1423), (12), (12)(34), (1324), (13)(24), (34), (14)(23)\}.
\end{aligned}$$

Any subgroup of S_4 of order 2 or 4 lies in one of these. Also, $S_3 \leq S_4$ (viewed as all permutations that fix 4). Now S_3 is maximal since it has order 6 and hence could only possible lie in a subgroup of S_4 of order 12, which does not happen since $A_4 \leq S_4$ is the only subgroup of order 12, and A_4 does not contain S_3. So

$$\Phi(S_4) \leq A_4 \cap H \cap K \cap L \cap S_3 = \{()\}.$$

Lemma 2. *$\Phi(G)$ is characteristic in G.*

Proof. Let $M \lneq G$ be maximal and $\alpha \in \mathrm{Aut}(G)$. If $\alpha(M) \leq N \lneq G$, then

$$(M \leq \alpha^{-1}(N) \lneq G) \implies M = \alpha^{-1}(N) \implies \alpha(M) = N.$$

So $\alpha(M)$ is maximal. Let $\{M_i\}_{i \in I}$ be the collection of maximal subgroups of G. The injectivity of α gives $\alpha(M_i) \neq \alpha(M_j)$ for all $i \neq j$ and so $\{M_i\}_{i \in I} = \{\alpha(M_i)\}_{i \in I}$. Therefore

$$\alpha(\Phi(G)) = \alpha\left(\bigcap_{i \in I} M_i\right) = \bigcap_{i \in I} \alpha(M_i) = \bigcap_{i \in I} M_i = \Phi(G).$$

☕

- $\boldsymbol{A_5}$: First notice that since $[A_5 : A_4] = 5$ is prime, then A_4 is maximal in A_5. So $\Phi(A_5) \lneq A_5$. Since A_5 is simple and $\Phi(A_5)$ is characteristic in A_5, then $\Phi(A_5) = \{()\}$.
- $\boldsymbol{S_5}$: Since $\Phi(S_5)$ is characteristic in S_5 and $\{()\}, A_5$ are the only proper normal subgroups of S_5, then $\Phi(S_5) \in \{\{()\}, A_5\}$. Since $[S_5 : S_4] = 5$ is prime, then S_4 is maximal in S_5. But $A_5 \not\leq S_4$, so we must have $\Phi(S_5) = \{()\}$.

(b) Say an element $x \in G$ is a *nongenerator* of G if for every proper subgroup $H \leq G$, also $\langle x, H\rangle$ is a proper subgroup of G. (Equivalently, x can be removed from any set of generators of G and the remaining set will still generate G.) Prove that if $|G| > 1$, then $\Phi(G)$ is exactly the set of nongenerators of G.

Proof. Let X be the set of nongenerators of G. If $x \in X$ and $M \lneq G$ is maximal, then $M \leq \langle x, M\rangle \lneq G$ implies $M = \langle x, M\rangle$ and so $x \in M$. Hence $x \in \Phi(G)$, and so $X \subseteq \Phi(G)$.

Conversely, let $x \in \Phi(G)$ and $H \lneq G$ be a proper subgroup. If $x \in H$, then $\langle x, H\rangle = H \lneq G$ implies $x \in X$, and we are done. If $x \notin H$, then in particular H is not maximal. So there exists a proper subgroup $K \lneq G$ which properly contains H, i.e., $H \lneq K \lneq G$. If $x \in K$, then

$$\langle x, H\rangle \leq \langle x, K\rangle = K \lneq G,$$

which implies $x \in X$, and we are done. If $x \notin K$, then the set

$$\mathcal{S} = \{L \lneq G \mid H \lneq L \text{ and } x \notin K\}$$

is nonempty. $\mathcal{S}$ has a partial ordering by set inclusion. If $\mathcal{C}$ is a chain in $\mathcal{S}$, then

$$U := \bigcup_{K \in \mathcal{C}} L$$

is a subgroup of G, an upper bound for $\mathcal{C}$, and does not contain x (otherwise $x \in L$ for some $L \in \mathcal{C}$, a contradiction). To see that $U \in \mathcal{S}$, suppose for contradiction $U = G$. Then $x \in U$, which means $x \in L$ for some $L \in \mathcal{C}$, a contradiction. So $U \in \mathcal{S}$, and so by Zorn's Lemma, $\mathcal{S}$ contains a maximal element M.

Now, if M is a maximal subgroup of G, then $x \in M$, a contradiction since $M \in \mathcal{S}$. So M is not a maximal subgroup of G, which means there exists L so that $M \lneq L \lneq G$. If $x \notin L$, then we have a contradiction to the maximality of M as an element of $\mathcal{S}$. So $x \in L$. Therefore,

$$H \lneq \langle x, H\rangle \leq \langle x, M\rangle \leq \langle x, L\rangle = L \lneq G,$$

and so $x \in X$, giving $X = \Phi(G)$. ☕

Problem 3. In this problem, you learn how to view some properties of module categories without referring to modules or elements. Use the category of modules over an arbitrary ring as intuition. Let $\mathcal{C}$ be a category. Given a collection of objects $A_1, \dots, A_n \in \mathcal{C}$, the *biproduct* of this collection is an object $A_1 \oplus \cdots \oplus A_n$ along with morphisms:

- $p_k \colon A_1 \oplus \cdots \oplus A_n \to A_k$ in $\mathcal{C}$ called *projections*, and
- $i_k \colon A_k \to A_1 \oplus \cdots \oplus A_n$ in $\mathcal{C}$ called *embeddings*,

such that $A_1 \oplus \cdots \oplus A_n$ along with the set $\{p_k\}_{k=1}^n$ is a product in $\mathcal{C}$, and $A_1 \oplus \cdots \oplus A_n$ along with the set $\{i_k\}_{k=1}^n$ is a coproduct in $\mathcal{C}$. As usual, biproducts need not exist in an arbitrary category. *Note that we are defining our use of the $\oplus$ symbol by objects with universal properties in a category, not as list of elements, since we don't have a way of taking elements from objects in $\mathcal{C}$.*

1. Unpacking the definitions, find a simple category theoretic description of the biproduct of an empty collection, if it exists. If such an object does exist, it's called a *zero object* of $\mathcal{C}$. Use this to define a "zero morphism" $0\colon A \to B$ between any two objects of $\mathcal{C}$.

   Solution:

   Since we cannot have maps from or to an empty collection, the zero object 0 of $\mathcal{C}$ must satisfy that for any $A \in Ob(\mathcal{C})$, there exist unique morphisms $0 \to A$ and $A \to 0$. Hence the zero object of $\mathcal{C}$, if it exists, is both an initial and terminal object in $\mathcal{C}$.

   Given any two objects A and B in $\mathcal{C}$, we have unique maps $A \xrightarrow{f} 0$ and $0 \xrightarrow{g} B$. So define a zero morphism $\mathbf{0}$ in $\mathcal{C}$ between A and B by $\mathbf{0} = g \circ f : A \to 0 \to B$.

2. Suppose that $\mathcal{C}$ is a category in which the biproduct of any finite set of objects exists. Use this to define an "addition" operation which takes $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and returns a morphism $f + g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. *Hint: try to create a sequence of morphisms of the form $A \to A \oplus A \to B \oplus B \to B$.*

   Solution:

   From the definition of the product $A \oplus A$, $\pi_1, \pi_2 : A \oplus A \to A$, there exists a unique morphism α such that $1_A = \pi_1 \circ \alpha$ and $1_A = \pi_2 \circ \alpha$. (We choose $1_A \in \mathrm{Hom}(A, A)$ since it is the only morphism we know is in $\mathrm{Hom}(A, A)$).

   Similarly, from the definition of the coproduct $B \oplus B$, $i_1, i_2 : B \to B \oplus B$, there exists a unique morphism $\beta : B \oplus B \to B$ such that $1_B = \beta \circ i_1$ and $1_B = \beta \circ i_2$.

   Again, from the definition of the product $B \oplus B$, $\tilde{\pi}_1, \tilde{\pi}_2 : B \oplus B \to B$, there exists a unique morphism $\gamma : A \oplus A \to B \oplus B$ such that $f \circ \pi_1 = \tilde{\pi}_1 \circ \gamma$ and $g \circ \pi_2 = \tilde{\pi}_2 \circ \gamma$. So we define $f + g := \beta \circ \gamma \circ \alpha$.

$$\begin{tikzcd}
 & A \arrow[r, "f"] & B \arrow[d, bend right, "i_1"'] \arrow[dr, "1_B"] & \\
A \arrow[ur, "1_A"] \arrow[r, "\exists!\alpha"] \arrow[dr, "1_A"'] & A \oplus A \arrow[u, "\pi_1"'] \arrow[d, "\pi_2"] \arrow[ur, "f\circ\pi_1"] \arrow[r, "\exists!\gamma"] \arrow[dr, "g\circ\pi_2"'] & B \oplus B \arrow[u, bend right, "\tilde{\pi}_1"'] \arrow[d, bend left, "\tilde{\pi}_2"] \arrow[r, "\exists!\beta"] & B \\
 & A \arrow[r, "g"'] & B \arrow[u, bend left, "i_2"] \arrow[ur, "1_B"'] &
\end{tikzcd}$$

3. **Optional:** Show that for any two objects A, B, the addition law from (b) satisfies:
   - $f + g = g + f$ for all $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$,
   - $f + 0 = f$ for all $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$,
   - the addition law is associative.

   That is, $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is an abelian monoid