Math 110B Homework 6

Brendan Connelly

Due Friday, March 6th, 2026

Problem 1

Assume $n \geq 5$. Show that A_n is generated by products of two disjoint two cycles.

Hint: Show first that A_n can be generated by products of two two cycles (possibly not disjoint), then conclude.

We know S_n is generated by two cycles. These cycles are not necessarily disjoint. Also, because sgn is a homomorphism, if $\sigma \in S_n$ such that $\sigma = (x_1\ x_2)\cdots(x_{n-1}\ x_n)$, then $\operatorname{sgn}(\sigma) = (-1)^{\frac{n-1}{2}}$. So, it is immediately clear we can generate A_n with an even number of not necessarily disjoint two cycles. Now, consider $\sigma \in A_n$ with $\sigma = \prod_{i\in I}(a_i\ b_i)(c_i\ d_i)$. It suffices to show we can take these two cycles to be disjoint. Suppose for some i (we omit the subscript i for brevity and clarity) $a \neq c$, but $b = d$. By definition of a cycle, we also know $a \neq b$ and $c \neq d$. If $a = c$ as well, we can remove the entire element as $(a\ b)(c\ d)$ would then be the identity. When $n \geq 5$, we can take $x, y \in [n] \setminus \{a, b, c\}$. Then, $(a\ b)(x\ y)$ is a disjoint two cycle and $(x\ y)(c\ d)$ and $(a\ b)(x\ y)(x\ y)(c\ d) = (a\ b)(c\ d)$. Thus, any product of two non-disjoint two cycles can just be written as a product of two pairs of two disjoint two cycles.

□

Problem 2

Let $C \subset S_n$ be a conjugacy class of elements of S_n. Show that for all $c \in C \cap A_n$ either $[c] = C$ or $|[c]| = |C|/2$, where $[c]$ is the conjugacy class of c as an element of A_n.

We consider the conjugation actions $S_n \overset{A}{\curvearrowright} S_n$ and $A_n \overset{B}{\curvearrowright} S_n$. We know that for $c \in A_n \cap C$, we know that $\operatorname{Stab}_{A,c} = C_{S_n}(c)$ and $\operatorname{Stab}_{B,c} = C_{A_n}(c)$, the centralizers in each group. By orbit stabilizer, or really the special case we call the class equation, we have that

$$|S_n| = |\operatorname{Cl}(c)| \cdot |C_{s_n}(c)| \qquad |A_n| = |[c]| \cdot |C_{A_n}(c)|$$

We want to look at the sizes of the two centralizers. We know $C_{A_n}(c) = C_{S_n}(c) \cap A_n$. If $C_{A_n}(c) = C_{S_n}(c)$, we see that $2 = \frac{|S_n|}{|A_n|} = \frac{|C|}{|[c]|}$. Now, suppose $C_{A_n}(c) \subsetneq C_{S_n}(c)$. Then, take $\tau \in C_{S_n}(c)$ such that $\tau \notin A_n$. Then, consider $\operatorname{sgn} : C_{S_n}(c) \to \{\pm 1\}$. This is a homomorphism so by the First Isomorphism Theorem, $|C_{S_n}(c)/\ker(\operatorname{sgn})| = 2$ since the map is surjective by assumption since $\operatorname{sgn}(\tau) = -1$. We know $\ker(\operatorname{sgn}) = C_{S_n}(c) \cap A_n$. Hence, $|C_{S_n}(c)| = 2|C_{A_n}(c)|$. Substituting into our class equations and dividing out gives

$$2 = \frac{|C|}{|[c]|} \cdot 2 \qquad \Longrightarrow \qquad [c] = C$$

Hence, for all $c \in C \cap A_n$ either $[c] = C$ or $|[c]| = |C|/2$, where $[c]$ is the conjugacy class of c as an element of A_n.

□

Problem 3

Show that a C as above splits into two conjugacy classes in A_n if and only if for any $\sigma \in C$, $C_{S_n}(\sigma) \subset A_n$.

From the previous question, we can consider the two cases. In the reverse direction, if we are in the case such that $\sigma \in C$, $C_{S_n}(\sigma) \subset A_n$, we showed this exactly corresponds to the case when $\frac{|C|}{|[c]|} = 2$. Hence, $|[c]| = \frac{|C|}{2}$, which implies C splits into two conjugacy classes in A_n.

If we are not in this case, we are in the case $C_{A_n}(c) \subsetneq C_{S_n}(c)$. As we showed, this corresponds to $[c] = C$, which means C does not split into two conjugacy classes in A_n. Hence, we have showed both implications. Overall, this follows immediately from our previous proof.

□

Problem 4

We showed in class that if an action of a finite group G on a set X is primitive, then the stabilizer of any $x \in X$ is a maximal subgroup of G. Show the partial converse that if G acts transitively on a set X, and for some $x \in X$ the stabilizer subgroup Stab_x is maximal in G, then the action is primitive.

Suppose for contradiction that $B \subset X$ is a non-trivial block. Then, without loss of generality, we can assume the $x \in X$ such that Stab_x is maximal in G is in the block. If it weren't, hB is a block for some $h \in G$, so, since the action is transitive, we can take $B \mapsto h^{-1}B$ and consider that block where h is such that takes x into B.

Now, we then assume that $\mathrm{Stab}_x = \{g \in G \mid gx = x\}$ is maximal. Let's define the set $H := \{g \in G \mid gx \in B\}$. This is a subgroup of G. First, it is clear $e \in G$ since $ex = x \in B$. Then, for $h, k \in H$, we want to show $hk \in H$. By definition, $kx \in B$. . Since B is a block, $B = hB$ or $B \cap hB = \varnothing$. But, we know $hx \in B$ as $x \in B$, meaning $hx \in B \cap hB$, so $B = hB$. This implies $hkx \in B$. So, $hk \in H$. Now, consider h^{-1}. We know $hB = B$ by the same intersection logic. So then $B = h^{-1}B$. Again, $x \in B$, so $h^{-1}x \in h^{-1}B = B$.

Now, we leverage the maximality. Clearly, $\mathrm{Stab}_x \leq H \leq G$. But, take $y \notin B$ and $z \in B \setminus \{x\}$ which exists by our assumption B non-trivial. By transitivity, there exists $g', g'' \in G$ such that $g'x = y$ but also $g''x = z$. So, Stab_x is a strict subset of H which is a strict subset G. This contradicts maximality, meaning B must actually be trivial, which completes the proof.

□

Problem 5

Consider the action of A_n on the set of subsets of $\{1, \ldots, n\}$ of size 3. Show that this action is primitive.

Hint: Assume to contradiction that $M = \text{Stab}\{1,2,3\}$ is contained in $M' = \langle M, g\rangle$, first show [breaking into $n = 7$, $n > 7$ as separate cases], that the orbit under M' of $\{1,2,3\}$ contains $\{1,2,4\}$. Then show that one can obtain $(1\ 2\ k) \in M'$ for any k, thus $M' = A_n$.

We can first see the action is transitive. We can simply count the size of the orbit of $\{1,2,3\}$ via the stabilizer. By definition, $M := \{\sigma \in A_n \mid \sigma(\{1,2,3\}) = \{1,2,3\}\}$. Each element in M can then permute the first three elements in any order and then the last $n-3$ elements. Thus, $|M| = \frac{3!}{2}(n-3)!$. Then, $\frac{|G|}{|M|} = \binom{n}{3}$, which is exactly the size of $X :=$ set of subsets of $\{1, \ldots, n\}$ of size 3. So, by orbit stabilizer, the orbit is the full set X, which implies transitivity.

We assume to contradiction that $M = \text{Stab}\{1,2,3\}$ is contained in $M' = \langle M, g\rangle$ where $g \in A_n$ is any element not in M.

Now, let's define $x := \{1,2,3\}$. It suffices to produce some element of the form $\{i,j,k\}$ with $\{i,j\} \subset \{1,2,3\}$ and $k \geq 4$. This is true because if we can do this, we can shift this to $\{1,2,4\}$ via an element in M. This is true because S_3 is three transitive (so two transitive) and we can take our outside element (element in $\{4,5,\ldots,n\}$ to 4 and fix our parity issue to make sure this element is in A_n.

Now, define $y := g(x)$. If $|y \cap x| = 2$, we have $\{1,2,4\}$ as discussed. So, assume $|y \cap x| \leq 1$. Without loss of generality, let $1, 2 \notin y$. We also assumed in this case $ab \in y$ where those are two elements outside $\{1,2,3\}$.

Now, we consider the case $n > 7$. By two transitivity of A_k for $k \geq 5$, we can choose $m \in M$ such that $m(a) = g^{-1}(1)$ and $m(b) = g^{-1}(2)$. So, $g^{-1}(1), g^{-1}(2) \in m(y)$. Then, $\{1,2\} \in g(m(y))$. Hence, $\{1,2,4\} \in \mathcal{O}_{M'}(x)$. Then, by transitivity, $\{1,2,k\} \in \mathcal{O}_{M'}(x)$ is as well.

We now consider the case $n = 7$, here, the outside action on M is not two transitive as A_4 is not two transitive. We then break into more cases, first $|y \cap x| = 1$. And then, $|y \cap x| = 0$. In the second case, we can relabel as in the $n \geq 7$ case. In the first case, we can use that A_4 is just transitive to map one outside element, map the inside element, and match parity.

In both cases, we have thus recovered $\{1,2,k\} \in \mathcal{O}_{M'}(x)$. Then, $i, j \geq 3$ with $i \neq j$,

$$(2\ i\ j) = (1\ 2\ i)(1\ 2\ j)(1\ 2\ i)^{-1}.$$

For $i, j, k \geq 3$ distinct,

$$(i\ j\ k) = (2\ i\ j)(2\ j\ k).$$

Thus every 3-cycle lies in M' which we showed generates A_n, hence $M' = A_n$. By question 4, we are done.

□

Problem 6

Calculate a p-Sylow subgroup of $\text{GL}_n(\mathbb{F}_p)$.

I claim a p-Sylow subgroup of $\text{GL}_n(\mathbb{F}_p)$ will have order $\binom{n}{2}$. This is clear as we know the order of $|\text{Gl}_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$. The lowest degree of p in this expression is $1 \cdot p \cdot p^2 \cdots p^{n-1} = p^{\binom{n}{2}}$. We then simply need to construct a subgroup of this order. I claim for U upper triangular matrices with ones on the diagonal are such a subgroup. We know upper triangular matrices are a subgroup. Multiplication will preserves the ones on the diagonal as well. Also, they are invertible since the determinant of each is

one. To calculate the order of U, we can see that we have p choices for the second column, p^2 for the third, all the way up to p^{n-1} for the n-th column. We don't have to worry about linear independence as that is handled by the determinant condition. Taking the product of these powers of p again gives us $p^{\binom{n}{2}}$. Hence, U is a p-Sylow subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

□

Problem 7

Show that any group of order $p^a \cdot q$ with $p \neq q$ distinct primes cannot be simple.

Suppose $q < p$. Then, there exists an $H \leq G$ such that $|H| = p^a$. By the relevant homework question, $|G/H| = q$ is the minimal prime, showing that H is normal, which completes this case.

Suppose $p < q$. Then, we know $n_p = q$ as $n_p = 1$ implies the one p-sylow subgroup is normal and by the third sylow theorem, if G is simple for contradiction, $n_p \mid q$ and $q \equiv 1 \mod p$.

We next show if there exists two distinct p-sylow subgroups, they don't all intersect trivially. We define $D := P_1 \cap P_2$ where without loss of generality we assume P_1 and P_2 to be the p-sylow subgroups that have the maximal size intersection. We know we can do this as we can assume for contradiction all p-sylows intersect trivially. This forces $(p^a - 1)q + 1$ distinct elements to be inside p-sylow subgroups. This leaves exactly $q - 1$ elements not equal to the identity, i.e, it leaves exactly one q-sylow subgroup. This means the q-sylow subgroup is normal in G which is a contradiction. Hence, all p-sylows cannot intersect trivially. So, we can choose the maximal D knowing $|D| > 1$.

We then leverage the fact that every proper subgroup H of a group $\tilde{G}$ of order p^b must have the property that H is a proper subgroup of its normalizer. By Lagrange, $|H| = p^c$ for $c < b$. We can consider the natural action we have used before $A : H \times P/H \to P/H$ defined by $A(h, xH) = (hx)H$ for all $h \in H$ and $xH \in P/H$. By the fixed point theorem and since $H \in P/H$ will be fixed by H, $|X^H| \geq p$. Hence, there exists some $xH \neq H$ such that $hxH = xH$. Then, $x^{-1}hx \in H$ so $x^{-1} \in N_{\tilde{G}}(H)$ but $x^{-1} \notin H$, proving this subgroup containment is strict.

Now that we have this fact, we know $D < N_{P_1}(D)$ and $D < N_{P_2}(D)$. We can show $N_G(D)$ is not a p group. Assume for contradiction it were. Then, $N_G(D)$ sits inside of some p-sylow subgroup P_3. Furthermore, $N_{P_1}(D) = P_1 \cap N_G(D) \subset P_1 \cap P_3$. So, by our maximality assumption of D, $P_3 = P_1$. By symmetry $P_2 = P_3$, which is a contradiction as $P_1 \neq P_2$. Hence, $q \mid N_G(D)$.

So, $N_G(D)$ has a q-sylow subgroup. From the order, we can also say $P_1 N_G(D) = G$. Hence, every $g \in G$ is such that $g = yh$ with $h \in P_1$ and $y \in N_G(D)$. Then, we observe $gP_1g^{-1} = (yh)P_1(yh)^{-1} = yP_1y^{-1}$ since h is in P_1. Building on this, $D = yDy^{-1} \subset yP_1y^{-1} = gP_1g^{-1}$ for arbitrary D. Hence, D is contained in the intersection of all p-sylow subgroups since all such subgroups are conjugate by the second theorem. Define, $A := \cap_{g \in G} gP_1g^{-1}$. We know $|A| > 1$ as $D \leq A$. It then suffices to show A is normal to produce our contradiction. It suffices to show that if $y \in A$, $zyz^{-1} \in A$ for $z \in G$. Then, by construction, for every $g \in G$, $y \in gP_1g^{-1}$. Then, $zyz^{-1} \in zgP_1g^{-1}z^{-1} = (zg)P_1(zg)^{-1}$. Since we are running over all $g \in G$, it is equivalent to run over all $gz \in G$. Hence, $zyz^{-1} \in gP_1g^{-1}$ for all $g \in G$, thus, $zyz^{-1} \in A$. So, A is a non-trivial normal proper subgroup of G, which is a contradiction of simplicity. This completes the proof for both cases.

□

Problem 8

Use the Sylow theorems to show that groups of order 30, 36, 42 can never be simple. Deduce that there is no nonabelian simple group of order $n < 60$.

We can start with groups of order $42 = 2 \cdot 3 \cdot 7$. We see $n_7 \mid 6$ and $n_7 \equiv 1 \mod 7$. Hence, $n_7 = 1$ so the corresponding p-Sylow subgroup is normal, and thus groups of order 42 are not simple.

Then, for a group of order $30 = 2 \cdot 3 \cdot 5$, we see by the same token, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 6$. Hence, $n_5 \in \{1, 6\}$. Then, $n_5 = 6$ or we are done. Then, each 5-group must clearly have trivial intersection as they are of prime order. So, we have $30 - 24$ elements available for another group. We can then consider n_3. By the same second Sylow theorem, $n_3 \in \{1, 10\}$. Then, if $n_3 = 10$, we have 20 additional elements of order 3, which is a contradiction. Thus, any group of order 30 must not be simple.

Lastly, for a group of order $36 = 2^2 3^2$. By the Sylow theorems, we can see $n_3 = 1, 4$. If $n_3 = 1$, we are done. So, assume $n_3 = 4$. Then, take P to be such a 3-Sylow subgroup, so of order 9. Then, we take the natural action on the cosets $G \overset{A}{\curvearrowright} G/P$. This gives the homomorphism $f_A : G \to S_4$. Then, define $K := \ker(f_A)$. K is a normal subgroup. If K is the whole group G, every subgroup is fixed, which means P is normal. Hence, we can assume the action is non-trivial. K must also then be non-trivial for size reasons. So, in our last chain of eventualities, K is a proper normal subgroup, which is our final contradiction. This demonstrates that there does not exist a simple group of order 36.

We can finally consider all groups of order less than or equal to 60. Every number below 60 other than $30, 36, 42$ is of the form $p^a q$ for a possibly 0. We can see of groups that are the product of three elements, the smallest choice other than the three we have is $2 \cdot 5 \cdot 7 = 70$. Hence, every group of order less than 60 is the product of up to two primes, possibly to some power. The only exception is $36 = 2^2 3^2$. The next possible smallest choice of a group of order this type is $2^2 5^2 = 100$. So, each case except for the outlined exceptions is of the form $p^a q$ for a possibly 0. This falls into the case in problem 7. For $a = 0$, which technically doesn't fall into this case, we have a group of prime order, which are the trivial abelian groups. Hence, there is no nonabelian simple group of order $n < 60$.

□