# Math 110B Homework 3

Brendan Connelly

Due Monday, February 4, 2026

## Problem 1

Let $G = \mathrm{GL}_n(\mathbb{F}_p)$ and let $S = \mathbb{F}_p^n$. Let

$$A : G \times S \to S$$

be defined by $A(g, v) = g \cdot v$ (matrix-vector multiplication). Show that $A$ is a group action. Compute all orbits and stabilizers.

We can first check the action by the identity matrix. We see for arbitrary $s \in S$

$$A(I_n, s) = I_n s = s$$

Now, for $X, Y \in G$, we can check via the properties of matrix multiplication

$$A(XY, s) = (XY)s = X(Ys) = A(X, Ys) = A(X, A(Y, s))$$

Hence, $A$ is a group action.

We first calculate the orbits of arbitrary $s \in S$. By definition, $\mathcal{O}(s) := \{\, s' \in S \mid \exists X \in G \text{ such that } s' = A(X, s) \,\}$. Hence, it is the set of all vectors such that the given $s \in S$ can be mapped to via the action. For $s = \vec{0}$, any matrix will simply take it back to itself (i.e., $X\vec{0} = \vec{0}$). Now, for $s \neq \vec{0}$, we want all $s'$ such that $s' = Xs$ for some $X \in \mathrm{GL}_n(\mathbb{F}_p)$. But this is easy as we can simply define the full rank linear transformation that maps $s$ to $s'$ and fill in the rest of the matrix to be full rank. This works for any $s' \neq \vec{0}$ which only fails as the transformation would then not be full rank. Hence, $\mathcal{O}(s) = S \setminus \{\vec{0}\}$.

We now calculate $\mathrm{Stab}_s = \{\, X \in G \mid A(X, s) = s \,\}$. By definition, this is the set of all elements in $G$ that leave $s \in S$ unchanged by left multiplication by any $X$. We know that $\mathrm{Stab}_{\vec{0}} = G$ as multiplication by any matrix in $G$ leaves the zero vector unchanged. For $s \neq 0$, we can use the fact that we prove in the following question. We can first compute the stabilizer of $e_1$. We notice that $Xe_1$ is exactly the first column of $X$. Hence, any $X \in G$ is such that $X \in \mathrm{Stab}_{e_1}$ if $X$ is of the following form:

$$X = \begin{pmatrix} 1 & v \\ 0 & B \end{pmatrix}$$

where $0 \in \mathbb{F}_p^{n-1}$ and $v^T \in \mathbb{F}_p^{n-1}$ and $B \in \mathrm{GL}_{n-1}(\mathbb{F}_p)$. We can see this element spans all possible choices for the matrix while being in $\mathrm{GL}_n(\mathbb{F}_p)$ simply by expanding the determinant on the left column.

Now, we know that since $\mathcal{O}(s) = S \setminus \{\vec{0}\}$ for all $s \neq 0$, we can take a $g \in G$ by question 2a such that

$$\mathrm{Stab}_s = g \cdot \mathrm{Stab}_{e_1} \cdot g^{-1}$$

□

---

## Problem 2

Let $G \curvearrowright_A S$ be a left group action.
**(a)** Suppose $s' \in O(s)$, where $O(s)$ is the orbit of some $s \in S$. Show that

$$\text{Stab}_{s'} = g \cdot \text{Stab}_s \cdot g^{-1}$$

for some $g \in G$.

Since $s' \in \mathcal{O}(s)$, there exists $g \in G$ such that $A(g, s) = s'$. Now, suppose $h \in \text{Stab}_{s'}$, then

$$s' = A(h, s') = A(h, A(g, s)) = A(hg, s)$$

Then,

$$A(g, s) = A(hg, s)$$

If we apply $f_A(g)^{-1}$ to both sides, on the left hand side, we obtain

$$A(g^{-1}, A(g, s)) = A(g^{-1}g, s) = A(e, s) = s$$

And on the right hand side we obtain

$$A(g^{-1}, A(hg, s)) = A(g^{-1}hg, s)$$

Hence, $A(g^{-1}hg, s) = s$. So, $g^{-1}hg \in \text{Stab}_s$. Equivalently, $h \in g \cdot \text{Stab}_s \cdot g^{-1}$, and thus

$$\text{Stab}_{s'} \subset g \cdot \text{Stab}_s \cdot g^{-1}.$$

Conversely, since $A(g^{-1}, s') = s$, we may apply the same argument with the roles of $s$ and $s'$ swapped (and with $g^{-1}$ in place of $g$) to obtain

$$\text{Stab}_s \subset g \cdot \text{Stab}_{s'} \cdot g^{-1}.$$

Therefore,

$$\text{Stab}_{s'} = g \cdot \text{Stab}_s \cdot g^{-1}.$$

□

. . . . . .

**(b)** Suppose now for simplicity that the action $A$ is transitive, recall that this means that $O(s) = S$ for any $s \in S$. Let $f_A : G \to \text{Bij}(S)$ be the corresponding homomorphism from class, defined as

$$g \mapsto f_A(g) = A(g, -) : S \to S.$$

Show that $\ker(f_A)$ is the largest normal subgroup contained in $\text{Stab}_s$, for any $s \in S$.

Since we assume $A$ is transitive, for all $s, s' \in S$, there exists $k \in G$ (dependent on our choice of $s, s'$) such that $A(k, s) = s'$. We showed in class the kernel of a homomorphism is a normal subgroup. Hence, it suffices to show that if $H \leq G$ normal, $H \leq \text{Stab}_s$ for any fixed $s \in S$. We know that $f_A(h)(s) = s$ for our fixed $s$ and for arbitrary $h \in H$ (which also gives us that $\ker(f_A) \subset \text{Stab}_s$). We want to show that $f_A(h)(s') = s'$ for all $s' \in S$. We consider

$$\begin{aligned} f_A(h)(s') &= A(h, s') \\ &= A(h, A(k, s)) \end{aligned}$$

$$
\begin{aligned}
&= A(hk, s) \\
&= A(k(k^{-1}hk), s) \\
&= A(k, A((k^{-1}hk), s)) \\
&= A(k, s) \qquad \text{by normal \& assumption} \\
&= s'
\end{aligned}
$$

Hence, $f_A(h) = \mathrm{Id}_S$ for $h \in H$. Thus, $H \leq \ker(f_A)$.

□

.....

**(c)** Show that $H \leq G$ is a normal subgroup if and only if

$$H = \ker(f_{A_{G/H}}),$$

where $A_{G/H}$ is the natural action of $G$ on $G/H$ defined in class.

($\implies$) Suppose $H \leq G$ normal. We recall $A_{G/H} : G \times G/H \to G/H$ such that $A_{G/H}(g, g'H) = gg'H$ which we showed is a well defined group action. Now, we want to show $H = \ker(f_{A_{G/H}})$.

Suppose first $g \in \ker(f_{A_{G/H}})$. Then, $A(g, g'H) = g'H$. So, $gg'H = g'H$. Take $g' = e$. Then, $gH = H$. Hence, $g \in H$.

Now, suppose $g \in H$. Then, $A(g, g'H) = gg'H$. We want to show then that $gg'H = g'H$ for arbitrary $g' \in G$. So, it suffices to show ${g'}^{-1}gg' \in H$ since $H$ is normal. Thus, $g \in \ker(f_{A_{G/H}})$.

($\impliedby$) Suppose $H = \ker(f_{A_{G/H}})$. But this follows immediately since the kernel of an homomorphism is a normal subgroup. So, $H$ is normal.

□

---

# Problem 3

Let $H, K$ be two normal subgroups of a group $G$ with $H \cap K = \{1_G\}$, show that $H, K$ commute elementwise, e.g. $hk = kh$ for all $k \in K$, $h \in H$.

Consider $k^{-1}hkh^{-1}$. We leverage associativity and the normal assumption. Notice $k^{-1}hk \in H$ since $H$ is normal. Thus, $k^{-1}hkh^{-1} \in H$ by closure of a subgroup. Similarly, $hkh^{-1} \in K$ since $K$ is normal. Hence, $k^{-1}hkh^{-1} \in K$ by closure of a subgroup.

Thus, $k^{-1}hkh^{-1} \in H \cap K$ so $k^{-1}hkh^{-1} = e$. Right and left multiplying gives our desired conclusion, i.e., $hk = kh$. Hence, $H, K$ commute elementwise.

□

---

## Problem 4

Let $G$ be a group, and let $G' \leq G$ denote the subgroup generated by the set

$$S := \{ghg^{-1}h^{-1} \mid g, h \in G\},$$

i.e. $G' = \langle S \rangle$.
**(a)** Show that $G'$ is a normal subgroup of $G$.

We can first check normality on the generator of $G'$. Suppose $k \in G$ and take $ghg^{-1}h^{-1} \in S$. We want to show $kghg^{-1}h^{-1}k^{-1} \in S$. It would suffice to just check that this conjugation lands in $G'$ but we can show this stronger statement to justify just checking on the generators more easily. Now, we can insert $k^{-1}k$ in between our terms to see $kghg^{-1}h^{-1}k^{-1} = (kgk^{-1})(khk^{-1})(kg^{-1}k^{-1})(kh^{-1}k^{-1})$. But, we can see this exactly $\tilde{g}\tilde{h}\tilde{g}^{-1}\tilde{h}^{-1}$ for $\tilde{g} = kgk^{-1}$ and $\tilde{h} = khk^{-1}$. It suffices to check that $(kgk^{-1})^{-1} = (kg^{-1}k^{-1})$ and $(khk^{-1})^{-1} = kh^{-1}k^{-1}$. But, from the properties of taking an inverse of multiple elements, these are both immediately true. Hence, as $kghg^{-1}h^{-1}k^{-1} = \tilde{g}\tilde{h}\tilde{g}^{-1}\tilde{h}^{-1}$, the conjugate of an element in $S$ lands in $S$. This sufficiently checks that $G'$ is normal.

We can justify this easily further though. Any $n \in G'$ is such that

$$n = s_1 \cdots s_m$$

for $s_i \in S$ (as if $s_i \in S$, $s_i^{-1} \in S$ so we can just look at finite products. If we insert $k^{-1}k$ in between elements as above, we see

$$ks_1 \cdots s_n k^{-1} = \prod_{i=1}^{m} ks_i k^{-1}$$

But, we just showed each $ks_ik^{-1} \in S$ so we are done.

□

. . . . . .

**(b)** Let $H$ be an abelian group, and let $f : G \to H$ be a homomorphism, show that $G' \leq \ker(f)$.

Let $g, k \in G$. First, observe $(\star) : f(gk) = f(g)f(k) = f(k)f(g) = f(kg)$ since $H$ is abelian. Then, as above, it suffices to check that every element in $S$ is in the kernel of $f$, as by the definition of a homomorphism, we could just decompose into a finite product of the identity element in $H$. So, take $gkg^{-1}k^{-1} \in S$. We see $f(gkg^{-1}k^{-1}) = f(gk)f((kg)^{-1}) = f(gk)f(kg)^{-1} = f(kg)f(kg)^{-1} = e_H$, where we crucially used $(\star)$. Hence, $S \subset \ker(f)$. So, $G' \leq \ker(f)$.

□

---

## Problem 5

Let $G$ be a group, and let $\mathrm{Aut}(G)$ be the set of self-isomorphisms $\psi : G \to G$.
**(a)** Show that under the operation of composition of functions, $\mathrm{Aut}(G)$ is a group.

This follows from facts we have already shown. First, the composition of self-isomorphisms is a self isomorphism because the composition of self bijections is a self bijection and the composition of homomorphisms is a homomorphism. We also know the identity map is trivially an isomorphism. Associativity follows from

function composition. Lastly, the existence of inverses is exactly my proof in question 9a of the previous homework.

□

.....

**(b)** Show that there exists a homomorphism

$$\mathrm{Ad} : G \to \mathrm{Aut}(G)$$

given by $\mathrm{Ad}(g)(h) = ghg^{-1}$, and identify its kernel.

We don't need to check well-definedness as there is no ambiguity. It suffices to check the given definition satisfies the homomorphism definition. For $g_1, g_2, h \in G$, we see

$$\begin{aligned}
\mathrm{Ad}(g_1g_2)(h) &= g_1g_2hg_2^{-1}g_1^{-1} \\
&= g_1\mathrm{Ad}(g_2)(h)g_1^{-1} \\
&= \mathrm{Ad}(g_1)\left(\mathrm{Ad}(g_2)(h)\right) \\
&= \left(\mathrm{Ad}(g_1) \circ \mathrm{Ad}(g_2)\right)(h)
\end{aligned}$$

Hence, $\mathrm{Ad}(g_1g_2) = \mathrm{Ad}(g_1) \circ \mathrm{Ad}(g_2)$. So, Ad is a homomorphism.

We can easily compute its kernel. We suppose that $g \in \ker(\mathrm{Ad})$. Then, for all $h \in G$, $\mathrm{Ad}(g)(h) = h$. Hence, $ghg^{-1} = h$. So, $gh = hg$. Thus the elements in the kernel are exactly those that commute with every element in $G$. This is exactly the definition of $Z(G)$.

□

.....

**(c)** Show that the image of Ad is a normal subgroup of $\mathrm{Aut}(G)$. We call this normal subgroup the group $\mathrm{Inn}(G)$ of inner automorphisms of $G$. The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called $\mathrm{Out}(G)$, the group of outer automorphisms of $G$.

We first note the image of any homomorphism is a group. Now, suppose $\alpha \in \mathrm{Im}(\mathrm{Ad})$. Then, $\alpha(h) = \mathrm{Ad}(g)(h)$ for some $g \in G$. Consider for $\beta \in \mathrm{Aut}(G)$,

$$\begin{aligned}
\beta \circ \alpha \circ \beta^{-1}(h) &= \beta \circ \mathrm{Ad}(g) \circ \beta^{-1}(h) \\
&= \beta g \beta^{-1}(h) g^{-1} \\
&= \beta\left(g\beta^{-1}(h)g^{-1}\right) \\
&= \beta(g)\beta(\beta^{-1}(h))\beta(g^{-1}) \\
&= \mathrm{Ad}(\beta(g))(h)
\end{aligned}$$

Hence, $\beta \circ \alpha \circ \beta^{-1} \in \mathrm{Im}(\mathrm{Ad})$. Thus, $\mathrm{Im}(\mathrm{Ad})$ is a normal subgroup.

□

---

## Problem 6

Let $G$ be a finite group, and let $H \leq G$ be a subgroup such that $|G/H| = p$ where $p$ is the smallest prime dividing $|G|$. Show that $H$ is normal. (Hint: use exercise 2.)

We can consider our work in exercise 2. First, recall the map $f_{A_{G/H}} : G \to S_{|G/H|}$. We showed in exercise 2 that $\ker(f_{A_{G/H}}) \leq \text{Stab}_s$ for any $s \in S$. We can see $\text{Stab}_H = H$, so $\ker(f_{A_{G/H}}) \leq H$. It suffices to show that $H = \ker(f_{A_{G/H}})$ since we already know $\ker(f_{A_{G/H}})$ is a normal subgroup as by 2c, we know that $H$ must be equal to this kernel for it to be normal.

We then see that by the first isomorphism theorem, $G/\ker(f_{A_{G/H}}) \cong \text{Im}(f_{A_{G/H}}) \leq S_p$. Hence, the order of $G/\ker(f_{A_{G/H}})$ must equal $pk$ for some $k \in \mathbb{N}$. Then, since this is isomorphic to a subgroup of $S_p$, we know $k \mid (p-1)!$. By Lagrange's theorem, we can count cosets and for $K := \ker f_{A_{G/H}}$, we have

$$|G/K| = [G : H] \cdot [H : K]$$

Hence, $pk = p \cdot [H : K]$. So, $[H : K] = k$. Suppose for contradiction that $k > 1$. Then, suppose $q$ is a prime factor of $k$. Then, $q \mid (p-1)!$ by what we derived. Yet, still by Lagrange, $q \mid |G|$. But, this contradicts our assumption that $p$ is the smallest prime dividing $|G|$. So, $k = 1$. So, $H = K$.

□

---

## Problem 7

(See problem 5) Calculate the automorphism group of the group $D_{2n}$, and identify the inner automorphism subgroup. Calculate the group of outer automorphisms.

We can first recall the properties of the group $D_{2n}$ that an automorphism $\phi$ must preserve. First, the order an element must be preserved under $\phi$. It sufficient to do this on generators, i.e., $|\phi(r)| = n$ and $|\phi(s)| = 2$. Automorphisms must also be surjective. Since we are calculating on the generators of the group, we need the relationships between the generators to hold, namely $\phi(sr) = \phi(r^{-1}s)$.

From this, we can see $\phi(r) = r^k$ for any $k \in [n]$ such that $\gcd(k, n) = 1$. In other words, for any $k \in \mathbb{Z}_n^\times$. Now, for $s$, we can take $s \mapsto sr^j$ for any $j \in [n]$. We can first check the relation

$$\phi(sr) = \phi(s)\phi(r) = sr^j r^k = sr^k r^j = r^{-k} sr^j = \phi(r)^{-1}\phi(s)$$

Then, we can also check $\phi(s)^2 = e$ as $sr^j sr^j = sr^j r^{-j} s = s^2 = e$. Hence, our group is characterized by taking $\phi(r) = r^k$ for any $k \in [n]$ and $s \mapsto sr^j$ for any $j \in [n]$. This means the automorphism group is exactly $(k, j) \in \mathbb{Z}_n^\times \times \mathbb{Z}_n$ with the operation:

$$(k, j) \cdot (k', j') = (kk', j + kj')$$

from the composition of our map on $r$ and on $s$.

To calculate the inner automorphism group, we can recall the definition, $\text{Ad} : G \to \text{Aut}(G)$ defined by $\text{Ad}(g)(h) = ghg^{-1}$. Because we are working with a homomorphism, we can say $\text{Inn}(G) = \langle \text{Ad}(r), \text{Ad}(s) \rangle$. Let's then compute the following where $\phi_r, \phi_s$ are conjugation by $r, s$ respectively.

$$\phi_r(r) = r \qquad \phi_r(s) = sr^{-2} \qquad \phi_s(r) = r^{-1} \qquad \phi_s(s) = s$$

So, from our above definition, $\text{Inn}(G) = \langle (1, -2), (-1, 0) \rangle$. By our computed operation that characterizes the group, this generates exactly $\pm 1$ in the left component. In the right component, if $n$ is odd, $-2$ generates every element. If $n$ is even, it only generates the even elements. So, the group is exactly $(\pm 1, j)$ where $j \in \mathbb{Z}_n$ if $n$ is odd, and where $j$ must be even in $\mathbb{Z}_n$ if $n$ is even.

To calculate the outer automorphism group, we mod out by $(\pm 1, j)$. If $n$ is odd, the right component disappears leaving us with exactly $\mathbb{Z}_n^\times/\{\pm 1\}$. If even, the right component doesn't entirely disappear; it only vanishes up to sign. Hence, we have $\mathbb{Z}_n^\times/\{\pm 1\} \times \mathbb{Z}_2$.

□

---

# Problem 8

Determine all subgroups of $D_{2n}$, which subgroups are normal?

The subgroups of $D_{2n}$ are easy to see when we look at the generators. If we consider $r$, they are exactly those generated by $\langle r^k \rangle$ where $k \mid n$ (otherwise all would be isomorphic to that generated by just $r$ or by a multiple). As for $s$, we get $n$ subgroups of order 2 generated by $\langle sr^j \rangle$ for $j \in \mathbb{Z}_n$. Together, we get the subgroups generated by $\langle r^k, sr^j \rangle$ where $k \mid n$ and $j \in \mathbb{Z}_k$ as the choice of $j$ only matters up to our ability to rotate.

As for which ones are normal, the rotations are normal as conjugation by a power of $r$ is trivial and $sr^l s = r^{-l}$ which would be in any subgroup generated by that power of $r$.

We can check those subgroups generated by two elements: $\langle r^k, sr^j \rangle$. If we conjugate by $s$, we obtain $s(sr^j)s = r^j s = sr^{-j} \in \langle r^k, sr^j \rangle$ if and only if $k \mid 2j$ as we need $-j \equiv j \mod k$. Now, if we conjugate by $r$, we obtain $r(sr^j)r^{-1} = sr^{j-2}$. So, $j - 2 \equiv j \mod k$. Hence, again, $k = 1, 2$. The two element subgroups fall into this analysis with $k = n$ and are thus not normal for general $n$. Hence, our normal subgroups are rotations and these combinations generated by $\langle r^k, sr^j \rangle$ with $k = 1, 2$. But, it is worth noting that the the $k = 1$ and $k = 2$ groups are the same if $n$ is not even.

□

---

# Problem 9

Calculate the conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$.

We know that the conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$ simply correspond to a change of basis. We know that the characteristic polynomial is preserved by a change of basis. Hence, we can first partition the conjugacy classes based on the properties of the characteristic polynomial. First, we could assume there is a repeated root in the characteristic polynomial. That gives matrices of the form $\lambda I$ and matrices of the form $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. In the third case, if the characteristic polynomial has two roots, we have a diagonalizable matrix, i.e. of the form $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$. And in the last case, we have that the characteristic polynomial has no roots over the field.

We can then count the conjugacy classes in each of these cases. In the first case, we have $p-1$ conjugacy classes as we can take $\lambda \in \mathbb{F}_p \setminus \{0\}$. In the second case, we have the same choices, another $p-1$ conjugacy classes. In the third case, we have $\binom{p-1}{2}$ choice, accounting for switching $\lambda$ and $\mu$ and that they must be distinct. In all of these cases, the conjugacy classes are again exactly those obtained by taking these matrix representations and performing a change of basis.

As for the last case, we can choose to represent the matrix in some way, and we can count the number of conjugacy classes complementary. We can choose a matrix representation of this class via a choice of

basis. Take $v \in \mathbb{F}_p^2$. Then, since a matrix $A$ in this case has no eigenvalues, $\{v, Av\}$ forms a basis. Suppose $A^2 v = \binom{x}{y}$ in said basis. Hence, we can say $A$ is similar to

$$\begin{pmatrix} 0 & x \\ 1 & y \end{pmatrix}$$

We can also count these classes via complementary counting. We can consider the minimal polynomial (which helps us deal with the scaling matrices vs the Jordan form matrices) $f(\lambda) = a_0 + a_1\lambda + \lambda^2$ for all but the scaling case. In this case, we get $p(p-1)$ choices as $a_0 \neq 0$. For the scaling matrices (the only case where the minimal polynomial will have degree 1 here), $f(\lambda) = \lambda + c$ for $c = 1, \ldots, p-1$, giving another $p-1$ choices. All in, we have $p^2 - 1$ distinct conjugacy classes. Hence, in this last case, we must have $p^2 - 1 - 2(p-1) - \binom{p-1}{2}$. This is exactly $\frac{p^2-p}{2}$.

□