Problem (Problem 1)**:** Let F be a finite field with q elements.

(a) Find the order of the general linear group

$$GL_n(F) = \{A \in \mathrm{Mat}_n(F) \mid \det(A) \neq 0\}.$$

(b) Find the order of the special linear group

$$SL_n(F) = \{A \in \mathrm{Mat}_n(F) \mid \det(A) = 1\}.$$

Solution:

(a) In order to find the order of the general linear group, we let $A \in GL_n(F)$ be an arbitrary matrix. The first column of A can consist $q^n - 1$ nonzero vectors in F^n.

To determine the second column, we observe that it cannot be a nonzero element element of the 1-dimensional linear subspace spanned by the first column of A. In particular, this means that there are $q^n - 1 - (q-1)$ such possible elements, or $q^n - q$. Inductively, we see that if we have determined the first $k-1$ columns, then the choices of column k consist of all nonzero vectors in F^n that are not of the form

$$v = c_1 v_1 + \cdots + c_{k-1} v_{k-1}$$

for $c_1, \dots, c_{k-1} \in F$; there are $q^{k-1} - 1$ such nonzero elements of the linear subspace spanned by $v_1, \dots, v_{k-1}$, so that

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

(b) By using the determinant homomorphism $\det\colon GL_n(F) \to F$, we find that

$$GL_n(F)/SL_n(F) \cong F^{\times},$$

whence

$$|GL_n(F)| = (q-1)|SL_n(F)|,$$

or

$$|SL_n(F)| = \frac{1}{q-1} \prod_{i=0}^{n-1} (q^n - q^i).$$

Problem (Problem 2)**:** Let F be a field with q elements, $V = F^n$ an n-dimensional F-vector space, and $m \leqslant n$. The purpose of this problem is to determine the cardinality of the set $T(m)$, the set of all m-dimensional subspaces W of V.

(a) Show that the standard action of $G = GL_n(F)$ on V induces a natural action of G on $T(m)$. Furthermore, show that this action is transitive.

(b) Let $W \in T(m)$ be the subspace spanned by the first m elements of the standard basis $\{e_1, \dots, e_n\}$ of V. Identify explicitly the stabilizer $\mathrm{stab}_G(W)$.

(c) Combine these facts with the formulas from Problem 1 (a) to determine $|T(m)|$.

Solution:

(a) We observe that G acts on V by mapping $0 \neq v \mapsto Av \neq 0$ for $A \in G$. We can extend this to an action on a m-dimensional subspace with ordered basis $(v_1, \dots, v_m)$ by mapping

$$S \cdot (v_1, \dots, v_m) = (Sv_1, \dots, Sv_m).$$

We observe that $\mathrm{id} \cdot (v_1, \dots, v_m) = (v_1, \dots, v_m)$, and

$$\begin{aligned} S \cdot (T \cdot (v_1, \dots, v_m)) &= S \cdot (Tv_1, \dots, Tv_m) \\ &= (STv_1, \dots, STv_m) \\ &= ST \cdot (v_1, \dots, v_m). \end{aligned}$$

Finally, to see that this action is transitive, we observe that for any two ordered bases $(v_1, \dots, v_m)$ and $(w_1, \dots, w_m)$ that define elements of $T(m)$, each can be extended to bases for V, $(v_1, \dots, v_m, v_{m+1}, \dots, v_n)$ and $(w_1, \dots, w_m, w_{m+1}, \dots, w_n)$, and we can specify a linear map $T\colon V \to V$ taking $v_i \mapsto w_i$ for each i. This specifies an element of $GL_n(F)$ by taking the matrix representation of this linear map. Therefore, the action is transitive.

(b) We observe that if $(e_1, \dots, e_m)$ is the basis for W, and $T \in GL_n(F)$, then

$$Te_i = c_1 e_1 + \cdots + c_m e_m + c_{m+1} e_{m+1} + \cdots + c_n e_n$$

for some constants $c_1, \dots, c_n$. In order for T to stabilize W, then we must have

$$Te_i = c_1 e_1 + \cdots + c_m e_m$$

for each $i = 1, \dots, m$. In particular, T is an invertible block matrix of the form

$$T = \begin{pmatrix} A & * \\ 0 & C \end{pmatrix},$$

where $A \in GL_m(F)$, $*$ is an arbitrary $m \times (n-m)$ matrix, and $C \in GL_{n-m}(F)$.

(c) By the orbit-stabilizer theorem, and since the action of $GL_n(F)$ on $T(m)$ is transitive, we know that

$$\begin{aligned} |T(m)| &= [GL_n(F) : \mathrm{stab}_G(W)] \\ &= \frac{|GL_n(F)|}{|\mathrm{stab}_G(W)|}. \end{aligned}$$

Our task now is to compute the order of the stabilizer. We observe that any element T of $\mathrm{stab}_G(W)$ consists of

- an arbitrary $m \times (n-m)$ matrix over F;
- an element of $GL_m(F)$;
- and an element of $GL_{n-m}(F)$.

Therefore, we find that

$$|\mathrm{stab}_G(W)| = \left(\prod_{i=0}^{m} (q^m - q^i)\right)\left(\prod_{i=0}^{n-m} (q^{n-m} - q^i)\right) q^{n(m-n)}.$$

Thus,

$$|T(m)| = \frac{\prod_{i=0}^{n-1} (q^n - q^i)}{\left(\prod_{i=0}^{m-1} (q^m - q^i)\right)\left(\prod_{i=0}^{n-m-1} (q^{n-m} - q^i)\right)\left(q^{m(n-m)}\right)}.$$

Problem (Problem 6)**:** Suppose a finite group G acts on a finite set X. For $g \in G$, let X^g be the set of all $x \in X$ that are fixed by g. Prove that

$$|G \cdot X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

That is, the number of orbits equals the "average" number of fixed points of elements of G.

Solution: We start by showing that

$$|G \cdot X| = \frac{1}{|G|} \sum_{x \in X} |\text{stab}_G(x)|.$$

From the orbit-stabilizer theorem, we know that

$$|\text{stab}_G(x)| = \frac{|G|}{|G \cdot x|}$$

for each $x \in X$. Therefore, we observe that

$$\sum_{x \in X} |\text{stab}_G(x)| = |G| \sum_{x \in X} \frac{1}{|G \cdot x|}.$$

Since the orbits partition X, we observe that we may split

$$\sum_{x \in X} \frac{1}{|G \cdot x|} = \sum_{i=1}^{r} |G \cdot x_i| \frac{1}{|G \cdot x_i|},$$

since for any $x \in X$ with $x \in G \cdot x_i$, there are $|G \cdot x_i|$ total elements in the same orbit, whence

$$\begin{aligned} \sum_{x \in X} |\text{stab}_G(x)| &= |G| \sum_{i=1}^{r} 1 \\ &= |G||G \cdot X|. \end{aligned}$$

Now, let $Y = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Letting π_1 and π_2 be the projections on the first and second coordinate, we observe that for a specific g_0 and x_0, we have

$$\begin{aligned} \pi_1^{-1}(\{g_0\}) &= \{(g_0, x) \in Y \mid g_0 \cdot x = x\} \\ \pi_2^{-2}(\{x_0\}) &= \{(g, x_0) \in Y \mid g \cdot x_0 = x_0\}. \end{aligned}$$

In particular, we have

$$\begin{aligned} \left|\pi_1^{-1}(\{g_0\})\right| &= |X^{g_0}| \\ \left|\pi_2^{-1}(\{x_0\})\right| &= |\text{stab}_G(x_0)|, \end{aligned}$$

and

$$\begin{aligned} Y &= \bigsqcup_{g \in G} \pi_1^{-1}(\{g\}) \\ &= \bigsqcup_{x \in X} \pi_2^{-1}(\{x\}), \end{aligned}$$

whence

$$|Y| = \sum_{g \in G} |X^g|$$

$$\begin{aligned} &= \sum_{x \in X} |\mathrm{stab}_G(x)| \\ &= |G||G \cdot X|. \end{aligned}$$

Thus,

$$|G \cdot X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Problem (Problem 8)**:** Recall that the symmetric group S_3 consists of the following permutations: e, the transpositions $(1, 2)$, $(1, 3)$, and $(2, 3)$, and the two 3-cycles $(1, 2, 3)$ and $(1, 3, 2)$. Also, recall that every $\sigma \in S_3$ can be written as a product of transpositions.

(a) Show that the center of S_3 is trivial, and hence $\mathrm{inn}(S_3) \cong S_3$.

(b) Show that $\mathrm{aut}(S_3) \cong S_3$, and hence every automorphism of S_3 is inner.

Solution:

(a) To start, we observe that the transpositions do not commute with each other. Letting a, b, c be arbitrary letters, then upon rearrangement we observe that, without loss of generality, $(a, b)(a, c) = (a, c, b)$, while $(a, c)(a, b) = (a, b, c)$.

Similarly, a cycle does not commute with any transposition. This can be seen, again without loss of generality, by computing $(a, b, c)(a, b) = (a, c)$, while $(a, b)(a, b, c) = (b, c)$.

Since the center of S_3 is trivial, it follows that conjugation is always a nontrivial automorphism on S^3, so the inner automorphisms $\iota_g(k) = gkg^{-1}$ are in one-to-one correspondence with the elements of S_3 by mapping $g \mapsto \iota_g$, or that $\mathrm{inn}(S_3) \cong S_3$.

(b) Let $T = \{\tau_1, \tau_2, \tau_3\} \subseteq S_3$ denote the transpositions, and let $\mathrm{aut}(S_3)$ act on T by permutation. We claim that for any $\sigma \in \mathrm{aut}(S_3)$, the action of σ on S_3 is entirely determined by its action on T. This follows from the fact $\sigma(e) = e$ by definition, and that the two 3-cycles in S_3 are built from 2-cycles,

$$\begin{aligned} (1, 2, 3) &= (1, 3)(1, 2) \\ (1, 3, 2) &= (1, 2)(1, 3). \end{aligned}$$

The orbit of τ_1 is the entirety of T, since we may select σ to be the automorphism that exchanges τ_1 with either τ_2 or τ_3 respectively. Since the permutations $\mathrm{Sym}(T)$ are in one-to-one correspondence with permutations in S_3 (take the permutation in S_3 to be that of the indices in T), it follows that the permutation representation $\pi\colon \mathrm{aut}(S_3) \to \mathrm{Sym}(T)$ is faithful, since the only way for $\sigma \cdot \tau_i = \tau_i$ for each τ_i to hold is if $\sigma = \mathrm{id}$.

Using the identification $\mathrm{Sym}(T) \cong S_3$, we thus get an injective map $\pi\colon \mathrm{aut}(S_3) \to S_3$. Yet, since $\mathrm{inn}(S_3) \subseteq \mathrm{aut}(S_3)$ is isomorphic to S_3, it follows that π is necessarily a surjection, so that $\mathrm{inn}(S_3) \cong \mathrm{aut}(S_3)$.