Math 594. Homework 1 (due January 15)

1. Let V and W be finite-dimensional vector spaces over a field F. Let $G = \mathrm{GL}(V)$ and $H = \mathrm{GL}(W)$ be the associated general linear groups. Let X denote the vector space $\mathrm{Hom}_F(V, W)$ of linear maps from V to W, but viewed only as a set (i.e., we ignore that X has a natural structure of F-vector space via pointwise operations). Recall that X has a natural left H-action and right G-action through composition and inner composition respectively (i.e., $h.x = h \circ x$ while $x.g = x \circ g$).

(i) Prove that $x, x' \in X$ lie in the same G-orbit if and only if they have the same image in W (when viewed as linear maps from V to W).

(ii) Give a criterion of similar flavor for two elements of X to lie in the same H-orbit, and prove your criterion is correct.

(iii) In the special case $W = F$, how many G-orbits are there (don't ignore the zero map!)? What does this tell you about how $\mathrm{GL}(V)$ acts on the set of hyperplanes (i.e., codimension 1 subspaces) in V?

2. Let F be a field, and define $S^1(F) = \{(a, b) \in F^2 \mid a^2 + b^2 = 1\}$.

(i) By thinking about the case $F = \mathbf{R}$, naturally endow $S^1(F)$ with a group structure for any F.

(ii) If there exists $i \in F$ with $i^2 = -1$ (e.g., $F = \mathbf{C}$) and $2 \neq 0$ in F, use such an element to construct an isomorphism of groups $\phi_i : S^1(F) \simeq F^\times$. this isomorphism is not intrinsic to F in the sense that there's another square root choice, namely $-i$, so we could use ϕ_{-i} instead. What is the resulting automorphism $\phi_{-i} \circ \phi_i^{-1}$ of $F^\times$ which carries ϕ_i into ϕ_{-i} (and vice-versa)? Meanwhile, if $2 = 0$ in F (F need not be $\mathbf{F}_2$!!), then show $S^1(F) \simeq F$ as groups (using addition on F).

(iii) This is a purely philosophical question to think about on your own: can the field $\mathbf{C}$ intrinsically distinguish between its two square roots of -1?

3. Let $F = \mathbf{F}_p$ denote the "field with p elements" for a prime p (i.e., the integers mod p). Let V be an n-dimensional vector space over F, and $G = \mathrm{GL}(V)$. Note that V has size p^n (as one sees by choosing a basis). Assume $n > 0$.

(i) Using the fact that the group $F^\times$ acts on $V - \{0\}$ (through scalar multiplication) and the orbits of this action are precisely the lines, conclude without any use of bases or coordinates that V contains $(p^n - 1)/(p - 1)$ lines. Applying this formula to the dual space V^*, how many hyperplanes are in V?

(ii) By Exercise 1(iii), you know G acts transitively on the set X of hyperplanes in V. If we choose one hyperplane x_0, conclude that $|G| = |X||\mathrm{Stab}_G(x_0)|$. Now elements of $\mathrm{Stab}_G(x_0)$ induce linear automorphisms of x_0. Use general principles from linear algebra to show that the resulting map of groups $\mathrm{Stab}_G(x_0) \to \mathrm{GL}(x_0)$ is surjective, and deduce $|\mathrm{Stab}_G(x_0)| = |\mathrm{GL}(x_0)||\mathrm{Fix}_G(x_0)|$ where $\mathrm{Fix}_G(x_0)$ denotes the subgroup of elements of G which fix everything in the hyperplane x_0 (i.e., act as the identity on x_0 viewed as hyperplane in V).

(iii) Putting together everything from (ii), we get the formula $|G| = |X||\mathrm{Fix}_G(x_0)||\mathrm{GL}(x_0)|$. You know $|X|$ from (i). By considering a complementary vector to x_0 in V, find a simple formula for $|\mathrm{Fix}_G(x_0)|$ in terms of $p = |F|$ and n, and use induction ($\dim x_0 = n - 1$!) to get a formula for $|G|$ in terms of $p = |F|$ and n.

(iv) Here's "another" way to compute $|G|$: think in terms of matrices. How many ways can you specify the first column of an invertible $n \times n$ matric over F? Once this is chosen, how many options are there for the second column? And so on. Deduce a formula for the number of such invertible matrices, and compare with (iii). More importantly: show this is the *same* method in disguise!

4. Consider the action of $G = \mathrm{GL}_2(\mathbf{F}_3)$ on the set X of all 4 lines in $V = \mathbf{F}_3^2$. Let $\rho : G \to \mathrm{Aut}(X)$ be the action map for the natural left action of G on X.

(i) Choose an ordering on X so as to identify $\mathrm{Aut}(X)$ with $\mathfrak{S}_4$, and for your favorite choice of 6 elements $g \in G$ (no two being scalar multiples of each other) write down $\rho(g) \in \mathfrak{S}_4$ in terms of its cycle decomposition.

(ii) Show that $\rho(g) = 1$ if and only if g is a scalar multiplication (this argument should work for $\mathrm{GL}(V)$ acting on the set X of lines in V for V of finite dimension over any field whatsoever: don't use matrices!!), and conclude in our situation that $\rho(g) = \rho(g')$ if and only if $g = \pm g'$.

(*iii*) By counting the size of source and target, use (*iii*) to deduce that ρ is surjective.

(*iv*) Extra credit: Prove that for a 2-dimensional vector space over any field at all, $\mathrm{GL}(V)$ acts transitively on the set of *triples* of lines in V (so if V has only 4 lines, then ...).

5. Let G be a group.

(*i*) If $g \in G$ satisfies $g^n = 1$ for some $n > 0$, show that if we take n *minimal* with this property then for any $m \in \mathbf{Z}$ (allowing $m \leq 0$) we have $g^m = 1$ if and only if $n|m$ (hint: write $m = nq + r$ with $0 \leq r < n$). We call this least n the *order* of g (and say g has *finite order*; otherwise we say g has *infinite order*). If $d|n$, what is the order of g^d?

(*ii*) Give an example of a group G with two elements $g, g' \in G$ of finite order such that gg' has infinite order (hint: matrices).

(*iii*) We say G is (finite) *cyclic* if there exists $g_0 \in G$ of finite order such that every element of G is a power of g_0 (with possibly negative exponent). When this happens, with g_0 of order n, show that G is abelian with $|G| = n$ and that there is a *well-defined* group homomorphism $\mathbf{Z}/n \to G$ sending $i \bmod n$ to g_0^i, and that this is an isomorphism. Conclude that (up to non-unique isomorphism) there is "only one" cyclic group of order n for each positive integer n (there's no "natural" isomorphism between two of the same size).

(*iv*) If G is cyclic of order n and $i \in \mathbf{Z}$, show that the map $g \mapsto g^i$ is a group homomorphism which is an isomorphism if and only if multiplication by i on $\mathbf{Z}/n$ is injective, in which case $i \bmod n \in (\mathbf{Z}/n)$ has a multiplicative inverse. Deduce a natural isomorphism of groups $\mathrm{Aut}_{\mathrm{group}}(G) \simeq (\mathbf{Z}/n)^\times$ which does *not* depend on the specification of a generator of G.

6. Fix $n > 1$. For $\sigma \in \mathfrak{S}_n$ and a pair $\{i, j\}$ of distinct integers between 1 and n (inclusive), note that $(\sigma(i) - \sigma(j))/(i - j) = (\sigma(j) - \sigma(i))/(j - i)$, so this ratio does not depend on the ordering among i and j. Define

$$\varepsilon_n(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j},$$

where the product is taken over unordered pairs of distinct integers between 1 and n.

(*i*) Compute $\varepsilon_3(\sigma)$ for all $\sigma \in \mathfrak{S}_3$, and show in general that $\varepsilon_n(\sigma) = \pm 1$ for all $\sigma \in \mathfrak{S}_n$.

(*ii*) Prove that $\varepsilon_n : \mathfrak{S}_n \to \{\pm 1\}$ is a surjective group homomorphism. Its kernel, A_n, is called the *alternating group* on n letters.

7. Let A be an abelian group, $a, a' \in A$ elements with respective finite orders n and n'.

(*i*) If $n = \prod p_i^{e_i}$ and $n' = \prod q_j^{f_j}$ are the prime factorizations, show that there exist elements in A of order $p_i^{e_i}$ and $q_j^{f_j}$ for all i and j.

(*ii*) If n and n' are relatively prime, show aa' has order nn'. In general, construct an element of order $\mathrm{lcm}(n, n')$ (consider $n = 6$, $n' = 10$ to see what's happening).

(*iii*) Taking for granted that the equation $X^m = 1$ has no more than m solutions in a field F (a *false* statement in non-commutative fields: there are infinitely many soltuons to $X^2 = -1$ in the quaternions), a result we'll prove later in the course, use (*ii*) to show that when F is *finite* then an element of maximal order in the finite abelian group $F^\times$ must be a generator. Conclude (by pure thought!) that $F^\times$ is cyclic. Find generators of $\mathbf{F}_{17}^\times$ and $\mathbf{F}_{31}^\times$.