Math 744, Fall 2014
Jeffrey Adams
Homework III SOLUTIONS

(1) Let $\mathbb{F}_q$ be the field with q elements.

(a) Show that $GL(2,\mathbb{F}_q)$ acts transitively on the projective space of lines in $\mathbb{F}_q^2$. Use this to compute the order of $GL(2,\mathbb{F}_q)$.

(b) Compute the order of $PGL(2,\mathbb{F}_q) = GL(2,\mathbb{F}_q)/\{xI\}$, $SL(2,\mathbb{F}_q) = \{g \in GL(2,\mathbb{F}_q)| \mid \det(g) = 1\}$, and $PSL(2,\mathbb{F}_q) = SL(2,\mathbb{F}_q)/\pm I$.

(c) Show that $PSL(2,2) \simeq S_3, PSL(2,3) \simeq A_4$, and $PSL(2,5) \simeq A_5$.

Solution:

(a) It is easy to see $GL(n,F)$ acts transitively on $F^n - \{0\}$ for any field and any n. So $GL(2,\mathbb{F}_q)$ clearly acts transitively on lines in $\mathbb{F}_q^2$. The stabilizer of the line through $(1,0)$, i.e. $\{(x,0) \mid x \in \mathbb{F}_q\}$, is $P := \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. This group is isomorphic as a set to $\mathbb{F}_q \times (\mathbb{F}_q^*)^2$, and has order $q(q-1)^2$. So G/P is isomorphic to the projective space X of lines, which has order $q+1$. So $|G|/|P| = q+1$, and

$$|GL(2,\mathbb{F}_q)| = (q+1)q(q-1)^2.$$

(b) There is an exact sequence

$$1 \to \mathbb{F}_q^* \to GL(2,\mathbb{F}_q) \to PGL(2,\mathbb{F}_q) \to 1,$$

which implies

$$|PGL(2,\mathbb{F}_q)| = (q+1)q(q-1)^2/(q-1) = (q+1)q(q-1)$$

On the other hand $SL(2,\mathbb{F}_q)$ is the kernel of the determinant map, which is surjective onto $\mathbb{F}_q^*$. So this time the exact sequence is

$$1 \to SL(2,\mathbb{F}_q)* \to GL(2,\mathbb{F}_q) \to \mathbb{F}_q^* \to 1.$$

This gives the same order:

$$|SL(2,\mathbb{F}_q)| = (q+1)q(q-1)$$

Finally there is an exact sequence

$$1 \to \pm I \to SL(2, \mathbb{F}_q) \to PSL(2, \mathbb{F}_q) \to 1$$

which gives

$$|PSL(2, \mathbb{F}_q)| = \begin{cases} (q+1)q(q-1)/2 & q \neq 2^k \\ (q+1)q(q-1) & q = 2^k \end{cases}$$

(c)

$G = PSL(2, 2)$ acts on X of order 3. The map $G \to \mathrm{Aut}(X)$ is injective, so $G \hookrightarrow S_3$. Since $|G| = 3(2)1 = 6$ $G \simeq S_3$.

$G = PSL(2, 3)$ acts on X of order 4. The map $G \to \mathrm{Aut}(X)$ is injecgtive, so $G \hookrightarrow S_4$. The order of G is $4 * 3 * 2/2 = 12$. The only subgroup of S_4 of order 12 is A_4 (why is this?), so $G \simeq A_4$.

$G = PSL(2, 5)$ acts on X of order 6. The map $G \to \mathrm{Aut}(X) \simeq S_6$ is injective, and G has order $6 * 5 * 4/2 = 60$. Why is it isomorphic to A_5?

As I mentioned in class, this is related to a famous result about symmetric groups: the outer automorphism group of S_n (i.e. $\mathrm{Aut}(S_n)/S_n$) is trivial, unless $n = 6$, in which case it is $\mathbb{Z}/2\mathbb{Z}$. Let H be the stabilizer of 6 in $S_6 = \mathrm{Aut}\{1, 2, 3, 4, 5, 6\}$, so $H \simeq S_5$. If τ is an outer automorphism of S_6 then $\tau(H)$ gives a copy of S_5 which does not fix any of $\{1, 2, 3, 4, 5, 6\}$. This can be visualized in various ways, including using the icosahedron. In any event, our copy of A_5 is τ of $A_5 \subset H$.

Alternatively, A_5 is given by generators and relations

$$A_5 = \langle x, y \mid x^2 = y^3 = 1, (xy)^5 = 1 \rangle.$$

So we just need to find elements of $PGL(2, 5)$ satisfying these conditions.

It is easy to find elements of order 5: $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Also order 2: $\begin{pmatrix} 0 & 1 \\ \pm 1 & 0 \end{pmatrix}$ (remember we're in $PSL(2)$ so $-I = I$). Also conjugates of these, of course. For order 3, embed F_{25} in $GL(2)$ as

$$a + \sqrt{2} \to \begin{pmatrix} a & b \\ 2b & a \end{pmatrix};$$

some of these elements have order 6 in $GL(2)$, or 3 in $PGL(2)$.

After some trial and error here is a set of generators satisfying the given relations:

$$x = \begin{pmatrix} 3 & 0 \\ 1 & 2 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 2 \\ 4 & 2 \end{pmatrix}, \quad xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(2) Suppose $\mathfrak{g}$ is a semisimple Lie algebra, let $(\ ,\ )$ be the Killing form, let $\{X_i\}$ be a basis of $\mathfrak{g}$, and let $\{Y_i\}$ be the dual basis with respect to $(,)$ (i.e. $(X_i, Y_j) = \delta_{i,j}$. Finally let (π, V) be a representation of $\mathfrak{g}$, and let

$$C = \sum_i \pi(X_i)\pi(Y_i) \in \mathrm{End}(V)$$

(a) Show that C is independent of the choice of basis $\{X_i\}$.

Solution:

This comes down to the following fact. Suppose V is a vector space equipped with a symmetric bilinear form. Then the element $\sum_i v_i \otimes w_i$, where $\{v_i\}$ is a basis and $\{w_i\}$ is the dual basis with respect to the form, is independent of the choice of basis.

To see this, use the *canonical* isomorphism

$$V \otimes V^* \simeq \mathrm{Hom}(V, V)$$

given by $v \otimes \lambda \to f_{v,\lambda}$, where $f_{v,\lambda}(w) = \lambda(w)v$. Then the identity element of $\mathrm{Hom}(V, V)$ corresponds to a canonical element of $V \otimes V^*$. Identifying V with its dual using the form gives the element $\sum_i v_i \otimes w_i$, which being canonical is independent of the choice of basis.

(b) Show that $C\pi(X) = \pi(X)C$ for all $X \in \mathfrak{g}$.

C is called the Casimir element of π.

This is a standard calculation. See any of the basic references, for example Humphreys.

(4) Show that the only three-dimensional simple complex Lie algebra is $\mathfrak{sl}(2, \mathbb{C})$ (up to isomorphism).

Solution: As I mentioned in class this is easy if you assume too much. A reasonable place to start is to use the Killing form $(,)$. The radical is an ideal, so it must be nondegenerate. Then the adjoint representation takes $\mathfrak{g}$ to $\mathfrak{so}(\mathfrak{g}, (,))$.

Since $\mathfrak{so}(\mathfrak{g},(,))$ is three dimensional this is an isomorphism. Over $\mathbb{C}$ there is only one symmetric bilinear form up to equivalence.

(5) Compute the root system of $\mathfrak{sO}(2n+1,\mathbb{C})$. Describe a choice of a set of positive roots. What is the order of the Weyl group?

Solution: Take the form to be $\begin{pmatrix} 0 & I_n & 7 \\ I_n & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Then

$$\mathfrak{h} = \mathrm{diag}(z_1, \ldots, z_n, -z_1, \ldots, -z_n, 0),$$

write this as $(z_1, \ldots, z_n)$. Then the roots are $\pm e_i \pm e_j$ (coming from $SO(2n)$) and $\pm e_i$ (the root vectors are entries in the last row and column.

The Weyl group is all permutations and sign changes: $W \simeq S^n \ltimes \mathbb{Z}/2\mathbb{Z}^n$.

(6) Do the same for $\mathfrak{sp}(2n,\mathbb{C})$.

Solution With the usual form the Cartan subalgebra is $\mathrm{diag}(z_1, \ldots, z_n, -z_1, \ldots, -z_n)$. Write this as $(z_1, \ldots, z_n)$. Coming from $mathfrakgl(n)$ embedded as $\mathrm{diag}(A, -{}^tA)$ we find the roots $e_i - e_j$. For any symmetric A the matrix $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$ is in $\mathfrak{g}$, this gives the roots $e_i + e_j$ and $2e_i$ (from A diagonal). The lower left hand-corner gives the negatives of these. So the roots are: $\pm e_i \pm e_j$ and $\pm 2e_i$.

The Weyl group is isomorphic to $S^n \ltimes \mathbb{Z}/2\mathbb{Z}^n$ just as in Problem 5.

(7) We defined a root system to have the property: if $\alpha \in R$, then $-\alpha \in R$, and no other multiple of α is in R. (This is actually a *reduced* root system). Assume only that $\alpha \in R$ implies $-\alpha \in R$. Show that if $\alpha \in R$ at there are at most 4 multiples of α contained in R. Give an example of a root system where this holds.

Suppose α and $c\alpha$ are roots. Then $2(\alpha, c\alpha)/(c\alpha, c\alpha)$ has to be an integer. This is equal to $2c(\alpha,\alpha)/c^2(\alpha,\alpha) = 2/c$. So $c = \pm 1, \pm 2$.

The only irreducible, non-reduced root system is type BC_n. This is $B_n \cup C_n$. The roots are $\pm e_i \pm e_j, \pm e_i$ and $\pm e_j$. A degenerate case is $BC_1 = \{\pm e_i, \pm 2e_i\}$.

(8) Calculate the Cartan matrices in types A_n, B_n, C_n, D_n. By induction, calculate their determinants.

See any standard reference. The determinants are:

1. A_n: $n+1$
2. B_n, C_n: 2
3. D_n: 4
4. E_6: 3
5. E_7: 2
6. E_8, F_4, G_2: 1

As I mentioned in class, these are the orders of the centers of the corresponding simply connected complex groups. Also they are the orders of P/R or $P^\vee/R^\vee$ in each case. In particular E_8, F_4 and G_2 are both simply connected and adjoint.