18.755 twelfth problem solutions

1. Fix an integer \( n \geq 2 \), and consider the two lattices of rank \( n \)

\[
X = \{ x \in \mathbb{Z}^n \mid \sum_{i=1}^{n} x_i \in 2\mathbb{Z} \}
\]

\[
Y = \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n.
\]

We saw in class that these lattices are dual to each other. You may assume that the coroots and roots of Spin\((2n)\) are

\[
R^\vee = \{ \pm e_i \pm e_j \mid 1 \leq i \neq j \leq n \} \subset X,
\]

\[
R = \{ \pm e_i \pm e_j \mid 1 \leq i \neq j \leq n \} \subset Y.
\]

Write

\[
\mathcal{R} = (X, R^\vee, Y, R)
\]

for the root datum of Spin\((2n)\).

(1) Prove that \( \mathcal{R} \) has no coverings except itself.

The shortest argument is using the claim above relating root datum coverings to group coverings. We know that Spin\((2n)\) is simply connected (because \(2n \geq 4 \geq 3\)) so it has no proper coverings.

Here is a direct argument. According to the definition of coverings, we are seeking sublattices \(X' \subset X\) that contain \(R^\vee\). We claim that \(R^\vee\) spans \(X\), so the only such sublattice is \(X\) itself (which is what we want to prove).

We proceed by induction on \(n\). The base case is \(n = 2\); what we wish to prove is that if \(x_1 + x_2\) is even, then we can find integers \(a\) and \(b\) so that

\[
(x_1, x_2) = a(1, 1) + b(1, -1).
\]

This is a system of two equations for the unknowns \(a\) and \(b\)

\[
a + b = x_1, \quad a - b = x_2.
\]

The solution in rational numbers is unique:

\[
a = (x_1 + x_2)/2, \quad b = (x_1 - x_2)/2.
\]

Here \(a\) is an integer because \(x_1 + x_2\) is assumed to be even; and \(b\) is an integer because \(b = a - x_2\). This completes the base case.

So assume that \(n > 2\), and that the result is known for \(n - 1\). Suppose \(x \in \mathbb{Z}^n\) has \(\sum x_i\) even. Define

\[
y = x - x_n(e_{n-1} - e_n) = (x_1, x_2, \cdots, x_{n-2}, x_{n-1} - x_n, 0).
\]
By inductive hypothesis we can write

\[ y = \sum_{1 \leq i < j \leq n-1} a_{ij}(e_i + e_j) + b_{ij}(e_i - e_j) \]

with \(a_{ij}\) and \(b_{ij}\) integers. The definition of \(y\) gives an expression for \(x\) as an integer combination of coroots as well. This completes the induction.

Being slightly more careful shows that any \(x\) in \(X\) has a unique expression

\[ x = b_1(e_1 + e_2) + b_2(e_1 - e_2) + b_3(e_2 - e_3) + \cdots + b_n(e_{n-1} - e_n) \]

with \(b_j \in \mathbb{Z}\).

(2) **Find all the quotients of \(\mathcal{R}\).** *(Hint: the number of possibilities is odd, and it isn’t one.)*

According to the definition of quotients, we are looking for sublattices \(Y' \subset Y\) that contain all the roots. Since the roots look exactly like the coroots, the conclusion from part (1) is that we are looking for sublattices

\[ X \subset Y' \subset Y. \]

According to a standard theorem about subgroups, this is exactly the same problem as looking for subgroups of the finite group

\[ S = \text{def } Y/X. \]

It is easy to see that there are exactly four elements in \(S\), represented by

\[ s_0 = 0, \quad s_1 = (1, 0, \cdots, 0), \quad s_+ = (1/2, \cdots, 1/2), \quad s_- = s_+ - s_1. \]

Here \([s_0]\) is the class of elements in \(\mathbb{Z}^n\) with even coordinate sum; \([s_1]\) is elements in \(\mathbb{Z}^n\) with odd coordinate sum; \([s_+]\) is elements of \((\mathbb{Z} + 1/2)^n\) with coordinate sum congruent to \(n/2\) (mod 2); and \([s_-]\) is elements of \((\mathbb{Z} + 1/2)^n\) with coordinate sum congruent to \(1 + n/2\) (mod 2).

We need to know the group structure of \(S\). We calculate

\[ [s_+] + [s_] = (1, \cdots, 1) = \begin{cases} \ [s_0] & \text{if } n \text{ is even} \\ \ [s_1] & \text{if } n \text{ is odd}. \end{cases} \]

With this relation in hand, it is very easy to conclude that

\[ S \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & n \text{ even} \\ \mathbb{Z}/4\mathbb{Z} & n \text{ odd}. \end{cases} \]
The $n$ even case is the Klein 4-group, which has five subgroups: $0$, $S$, and the three two-element subgroups
\[\{[s_0], [s_1]\}, \{[s_0], [s_+]\}, \{[s_0], [s_-]\}.\]

The $n$ odd case has three subgroups: $0$, $S$, and $\{[s_0], [s_1]\}$.

To give a complete answer (and to address part (3)) we should write the two lattices explicitly. If we shrink $Y$ to $Y'$, we must expand $X$ to $X' = (Y')^*$. It’s a bit tricky to think about where to look for this expansion. Any rank $n$ lattice $X$ sits naturally in an $n$-dimensional $\mathbb{Q}$-vector space
\[V = X \otimes \mathbb{Z} \mathbb{Q}.\]

The lattice duality between $X$ and $Y$ identifies
\[V^* \simeq Y \otimes \mathbb{Z} \mathbb{Q}.\]

The larger $X'$ we are looking for are all contained in the vector space $V$. The definition is
\[X' = \{v \in V \mid \langle v, \lambda' \rangle \in \mathbb{Z} (\lambda' \in Y')\}.\]

In our case the coordinates in the definition of $X$ and $Y$ show that $V$ and $V^*$ may be identified with $\mathbb{Q}^n$. If $n$ is odd, the sublattices $Y'$ are
\[Y_0 = X = \{\lambda \in \mathbb{Z}^n \mid \sum \lambda_i \in 2\mathbb{Z}\}\]
(corresponding to the subgroup $0$),
\[Y_S = Y = \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n\]
(corresponding to the subgroup $S$), and
\[Y_1 = \mathbb{Z}^n\]
(corresponding to the subgroup $\{[s_0], [s_1]\}$). Their dual lattices are
\[X_0 = Y = \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n,\]
\[X_S = X = \{\lambda \in \mathbb{Z}^n \mid \sum \lambda_i \in 2\mathbb{Z}\},\]
\[X_1 = \mathbb{Z}^n.\]

The group corresponding to $(X_S, Y_S)$ is Spin$(2n)$. The group corresponding to $(X_1, Y_1)$ is SO$(2n)$. The group corresponding to $(X_0, Y_0)$ is
\[PSO(2n) = \text{det} SO(2n)/\{\pm I\}.\]
If \( n \) is even, we have these same three lattice pairs (corresponding to the same compact groups) and two more:

\[
Y_+ = \{ \lambda \in \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n \mid \sum \lambda_i \equiv n/2 \pmod{2} \},
\]
\[
Y_- = \{ \lambda \in \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n \mid \sum \lambda_i \equiv 1 + n/2 \pmod{2} \}.
\]

Their dual lattices are

\[
X_+ = \{ x \in \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n \mid \sum x_i \in 2\mathbb{Z} \},
\]
\[
X_- = \{ x \in \mathbb{Z}^n \cup (\mathbb{Z} + 1/2)^n \mid \sum x_i \in 2\mathbb{Z} + 1 \}.
\]

The condition of belonging to \( X_0 \) means that \( x \) takes integer values on the root lattice \( Y_0 \). To get into \( X_\pm \), we must impose one more condition: taking an integer value on \( s_\pm \). That is the condition written in each case.

The groups corresponding to \((X_\pm, Y_\pm)\) are called half spin groups \( \text{Spin}_\pm(2n) \). They are quotients of \( \text{Spin}(2n) \) (always with \( n \) even!) by one of the two central elements not equal to \( \pm 1 \) in the Clifford algebra.

(3) I talked in class about the operation of “Langlands duality” on root data, interchanging the lattice with the dual lattice (and roots with coroots). What is the operation of Langlands duality on the various quotients of \( \mathcal{R} \)?

Since the roots and coroots look the same, the question is just what happens to the lattice pairs when they are exchanged. The explicit calculations in (2) make this clear:

\[
(X_0, Y_0) \leftrightarrow (X_S, Y_S), \quad PSO(2n) \leftrightarrow \text{Spin}(2n),
\]
\[
(X_1, Y_1) \leftrightarrow (X_1, Y_1), \quad SO(2n) \leftrightarrow SO(2n).
\]

If \( n \equiv 0 \pmod{4} \), (so that \( n/2 \) is even) then

\[
(X_+, Y_+) \leftrightarrow (X_+, Y_+), \quad \text{Spin}_+(2n) \leftrightarrow \text{Spin}_+(2n),
\]
\[
(X_-, Y_-) \leftrightarrow (X_-, Y_-), \quad \text{Spin}_-(2n) \leftrightarrow \text{Spin}_-(2n):
\]

both of the half spin groups, like \( SO(2n) \), are Langlands self-dual. If \( n \equiv 2 \pmod{4} \) (so that \( n/2 \) is odd), then

\[
(X_+, Y_+) \leftrightarrow (X_-, Y_-), \quad \text{Spin}_+(2n) \leftrightarrow \text{Spin}_-(2n):
\]

the two half-spin groups are interchanged by Langlands duality.
2. For this problem we again fix an integer \( n \geq 2 \), and consider the two lattices of rank \( n - 1 \)
\[
X = \{x \in \mathbb{Z}^n \mid \sum x_i = 0\},
\]
\[
Y = \mathbb{Z}^n / [\mathbb{Z}(1, \ldots, 1)].
\]
We computed in class that these are the lattices for the root datum of \( SU(n) \), with roots and coroots
\[
R^\vee = \{e_i - e_j \mid 1 \leq i \neq j \leq n\} \subset X,
\]
\[
R = \text{images of } \{e_i - e_j \mid 1 \leq i \neq j \leq n\} \subset Y.
\]
Answer the same questions as for \( \text{Spin}(n) \) above. (One change is that the hint is no longer correct. What is the number of finite quotients of \( SU(n) \)?)

Again we know that \( SU(n) \) is simply connected, so it follows from the claim made before the problems that the root datum has no coverings. The more direct proof is to show that the coroots span the lattice \( X \); that is, that every integer vector with coordinates summing to zero is an integer combination of various \( e_i - e_j \). This is an easy version of what’s in the solution to the first problem.

For the quotients of \( R \), we need to understand the sublattices of \( Y \) that contain all the roots. If \( \lambda \) in \( Y \) is represented by \((\lambda_1, \ldots, \lambda_n)\), then
\[
\rho(\lambda) = [\sum \lambda_i] \in \mathbb{Z}/n\mathbb{Z}
\]
(the “residue” of \( \lambda \)) is well-defined. More or less the argument of the first paragraph shows that the span of the roots is
\[
Y_0 = \{\lambda \in Y \mid \rho(\lambda) = 0\}.
\]
Quotients of \( R \) correspond to lattices \( Y' \) such that
\[
Y_0 \subset Y' \subset Y.
\]
Just as in the first problem, these correspond to subgroups of the finite group
\[
S = \text{def } Y/Y_0.
\]
Clearly the homomorphism \( \rho \) identifies
\[
S \cong \mathbb{Z}/n\mathbb{Z},
\]
the cyclic group of order \( n \). Its subgroups are the various
\[
S_d = (n/d + n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}
\]
for \(d\) a divisor of \(n\). The corresponding sublattice is

\[
Y_d = \{ \lambda \in \mathbb{Z}^n \mid \sum \lambda_i \in (n/d)\mathbb{Z} \}/\mathbb{Z}(1, \ldots, 1).
\]

Thus

\[
Y = Y_n, \quad \langle R \rangle = Y_1.
\]

are the largest and smallest possibilities. The dual lattices are

\[
X_d = \{ x \in \left[ \frac{1}{n} \mathbb{Z} \right]^n \mid \sum x_i = 0, \quad nx_i \equiv ad \pmod{n} \}.
\]

Here each \(nx_i\) is meant to be congruent to the same integer multiple \(ad\) of \(d\). Thus for example

\[
X_1 = \{ x \in \mathbb{Q}^n \mid \sum x_i = 0, \quad x_i - x_j \in \mathbb{Z} \}.
\]

\[
X_n = \{ x \in \mathbb{Z}^n \mid \sum x_i = 0 \} = X = (R^\vee).
\]

The group corresponding to \((X_n, Y_n)\) is \(SU(n)\), and the group corresponding to \((X_1, Y_1)\) is \(PSU(n)\). If \(\zeta\) is a primitive \(n\)th root of unity, then the group corresponding to \((X_d, Y_d)\) is

\[
SU(n)_d = SU(n)/\langle \zeta^d I \rangle,
\]

the quotient of \(SU(n)\) by scalar matrices of \((n/d)\)th roots of unity. (This is not standard notation; I introduce it just to talk about the next part of the problem.)

For the third part, it isn’t entirely clear that Langlands duality operates on these root data, since it isn’t clear in these coordinates how to identify lattices around \(Y\) with lattices around \(X\). The two rational vector spaces where these lattices live are

\[
V = \mathbb{Q}^n/\mathbb{Q}(1, \ldots, 1)
\]

and

\[
V^* = \{ x \in \mathbb{Q}^n \mid \sum x_i = 0 \}.
\]

But there is a unique isomorphism from \(V\) to \(V^*\) sending each root to the corresponding coroot: it is

\[
j: V^* \to V, \quad j([\lambda]) = \lambda - \frac{1}{n}\lambda_n(1, \ldots, 1).
\]

It is fairly easy to see that

\[
j(Y_d) = X_{n/d}
\]

for any divisor \(d\) of \(n\); so the Langlands dual operation is

\[
(X_d, Y_d) \leftrightarrow (X_{n/d}, Y_{n/d}), \quad SU(n)_d \leftrightarrow SU(n)_{n/d}.
\]
So nothing is fixed by Langlands duality unless \( n = m^2 \) is a perfect square; in that case the group
\[
SU(m^2)_m = SU(m^2)/(\text{\((m\text{th roots of unity})\cdot I\))}
\]
is fixed by Langlands duality.

The total number of finite quotients of \( SU(n) \) is
\[
d(n) = \text{number of divisors of } n.
\]

If the prime factorization of \( n \) is
\[
n = \prod_j p_j^{m_j},
\]
then
\[
d(n) = \prod_j (m_j + 1).
\]

For example,
\[
d(12) = d(2^2 \cdot 3) = (2 + 1) \cdot (1 + 1) = 6;
\]
the six divisors are 1, 2, 3, 4, 6, 12.

Do you see why we have proven (even before the formula for \( d(n) \)) that \( d(n) \) is odd if and only if \( n \) is a perfect square?