18.755 eleventh problem solutions, due Wednesday, April 29, 2020

1. Find all root data living on the lattices $X_* = \mathbb{Z}^2$, $X^* = \mathbb{Z}^2$ with the property that $R$ contains the two roots

$$\alpha = (1, 0), \quad \beta = (0, 1).$$

**Hint:** this is NOT the same problem you solved last week.

The pairing between $X_*$ and $X^*$ is

$$\langle (a, b), (c, d) \rangle = ac + bd.$$

Therefore the requirement $\langle \alpha, \alpha^\vee \rangle = 2$ means

$$\alpha^\vee = (2, a), \quad \beta^\vee = (b, 2).$$

We compute

$$s_\alpha(x, y) = (x, y) - \langle (x, y), \alpha^\vee \rangle \alpha = (x, y) - (2x + ay)(1, 0) = (-x - ay, y)$$

$$s_\alpha = \begin{pmatrix} -1 & -a \\ 0 & 1 \end{pmatrix}$$

and similarly

$$s_\beta = \begin{pmatrix} 1 & 0 \\ -b & -1 \end{pmatrix}.$$ 

Therefore

$$T = \text{def} \ s_\alpha s_\beta = \begin{pmatrix} -1 + ab & a \\ -b & -1 \end{pmatrix}.$$ 

By the root system axioms, the group $W$ generated by $s_\alpha$ and $s_\beta$ must permute the finite set of roots. The kernel of the homomorphism from $W$ to permutations must fix the roots $(1, 0)$ and $(0, 1)$, so must be the identity. The conclusion is that $W$ is *finite*. In particular, $T^N = I$ for some large enough integer $N$. So the eigenvalues of $T$ are roots of unity. It follows that

$$-2 \leq \text{tr} T \leq 2;$$

that $\text{tr} T = 2$ only if $T = I$; and that $\text{tr} T = -2$ only if $T = -I$.

Our $T$ is clearly not the identity (because of the entry $-1$ in the lower right); so

$$-2 \leq \text{tr} T < 2.$$ 

Since $\text{tr} T = ab - 2$,

$$0 \leq ab < 4.$$
If $ab = 0$, so that $\text{tr} T = -2$, then $T = -I$, so $a = b = 0$. In this case the sets

$$R_0 = \{\pm(1,0), \pm(0,1)\}, \quad R_0^\vee = \{\pm(2,0), \pm(0,2)\}$$

must be in our root datum; and these sets by themselves make a root datum. The possible additional (root, coroot) pairs that could be added you enumerated in Problem Set 10; no need to repeat that here.

In the remaining cases, $ab$ is 1, 2, or 3; so the possibilities are

$$(a,b) = (\pm 1, \pm 1); \quad (a,b) = (\pm 1, \pm 2) \text{ or } (\pm 2, \pm 1); \quad (a,b) = (\pm 1, \pm 3) \text{ or } (\pm 3, \pm 1).$$

To reduce the number of cases, we may replace $\beta$ by $-\beta$ (changing the sign of the second coordinate on $\mathbb{Z}^2$) and assume $a < 0, \quad b < 0$. Furthermore we may interchange $\alpha$ and $\beta$ (interchanging the coordinates on $\mathbb{Z}^2$) and assume

$$a = -1, \quad b = -1 \text{ or } -2 \text{ or } -3.$$ 

The matrices computed earlier are now

$$s_\alpha = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad s_\beta = \begin{pmatrix} 1 & 0 \\ -b & -1 \end{pmatrix}.$$ 

Applying these matrices repeatedly to our given roots, and their transposes to our given calculated coroots, produces when $b = -1$

$$R_1 = \{\pm(1,0), \pm(0,1), \pm(1,1)\}, \quad R_1^\vee = \{\pm(2,-1), \pm(-1,2), \pm(1,1)\}.$$

By mildly painful calculation (or see the Proposition below), these sets constitute a root datum. Because we might have gotten to this calculation by first interchanging the coordinates or changing the sign on one, there is one more possibility

$$R_1' = \{\pm(1,0), \pm(0,1), \pm(1,-1)\}, \quad (R_1')^\vee = \{\pm(2,1), \pm(1,2), \pm(1,-1)\}.$$

When $b = -2$, applying $s_\alpha$ and $s_\beta$ repeatedly produces

$$R_2 = \{\pm(1,0), \pm(0,1), \pm(1,1), \pm(1,2)\}, \quad R_2^\vee = \{\pm(2,-1), \pm(-2,2) \pm (2,0), \pm(0,1)\}.$$

Again these sets satisfy the axioms for a root datum by direct computation, or by the proposition below. Because we might have gotten to this calculation by first interchanging the coordinates or changing the sign on one, there are three more possibilities

$$R_2^a = \{\pm(1,0), \pm(0,1), \pm(1,-1), \pm(-1,2)\}, \quad (R_2^a)^\vee = \{\pm(2,1), \pm(2,2), \pm(2,0), \pm(0,1)\}.$$ 

$$R_2^b = \{\pm(1,0), \pm(0,1), \pm(1,1), \pm(2,1)\}, \quad (R_2^b)^\vee = \{\pm(2,2), \pm(2,1), \pm(0,2), \pm(1,0)\}.$$ 

$$R_2^c = \{\pm(1,0), \pm(0,1), \pm(-1,1), \pm(2,-1)\}, \quad (R_2^c)^\vee = \{\pm(2,-2), \pm(2,-1), \pm(0,2), \pm(1,0)\}.$$
When $b = -3$, we get
\[
R_3 = \{\pm (1, 0), \pm (0, 1), \pm (1, 1), \pm (1, 2), \pm (1, 3), \pm (2, 3)\},
\]
\[
R_2^\vee = \{\pm (2, -1), \pm (-3, 2) \pm (3, -1), \pm (0, 1), \pm (-1, 1), \pm (1, 0)\}.
\]

Again these twelve pairs $(\gamma, \gamma^\vee)$ constitute a root datum. I won’t write the other three systems obtained by interchanging coordinates or changing the sign of one coordinate.

This is the calculation I intended for you to make. The problem actually asks also about the possibility of enlarging the root datum further. To see what candidates there are for enlarging the root datum is a bit of a pain. You need to look for candidate (root, coroot) pairs $(\gamma, \gamma^\vee)$ to add so that all the pairs $(\gamma, r\alpha + s\beta)$ satisfy the requirements in the following proposition. (Here $r\alpha + s\beta$ are the roots calculated above.) I have not written how this leads to the following answers . . .

For $R_0$, the only possible enlargement to a reduced root datum is adding four pairs
\[
S_0 = \{(\epsilon_1, \epsilon_2) \mid \epsilon_j = \pm 1\}, \quad S_0^\vee = \{(\epsilon_1, \epsilon_2) \mid \epsilon_j = \pm 1\}.
\]

This was the solution to last week’s

For $R_1$, the only possibility is adding the six pairs
\[
S_1 = \{\pm (2, 1), \pm (1, 2), \pm (1, -1)\}, \quad S_1^\vee = \{\pm (1, 0), \pm (0, 1), \pm (1, -1)\}.
\]

The root data for $R_2$ and $R_3$ cannot be enlarged.

Here is the general fact needed to check all these things.

**Proposition.** If $\alpha$ and $\beta$ are linearly independent roots in a root datum, then the two integers $b = \langle \alpha, \beta^\vee \rangle$ and $a = \langle \beta, \alpha^\vee \rangle$ are both zero or both nonzero. In the latter case they have the same sign; one is $\pm 1$ and the other is $\pm 2$ or $\pm 3$.

The coroots $\alpha^\vee$ and $\beta^\vee$ are in particular linearly independent.

The action of $T = s_\alpha s_\beta$ on the span of $\alpha$ and $\beta$ has order $m = 2$ if $ab = 0$, $m = 3$ if $ab = 1$, $m = 4$ if $ab = 2$, and $m = 6$ if $ab = 3$. The group $W = \langle s_\alpha, s_\beta \rangle$ is a dihedral group of order $2m$, consisting of the elements
\[
T^j, \ T^j s_\alpha \quad (0 \leq j < m).
\]

The last $m$ elements listed are precisely the reflections in $W$. The roots in $W \cdot \{\alpha, \beta\}$ are
\[
R_{\alpha,\beta} = \{\pm T^j \alpha, \pm T^j s_\alpha \beta \mid 0 \leq j < m\}.
\]

(In fact the $\pm$ signs are not needed: there are exactly $2m$ distinct roots.) The elements
\[
(X_*, X^*, R^\vee_{\alpha,\beta}, R_{\alpha,\beta})
\]
are a root system.
Proof. We consider the action of \( s_\alpha, s_\beta, \) and \( T \) on the span of \( \alpha \) and \( \beta \). Because \( \alpha \) and \( \beta \) are assumed to be linearly independent, this span is isomorphic to \( \mathbb{Z}^2 \), with basis \( \alpha \) and \( \beta \). The argument above now gives the restrictions on \( a \) and \( b \).

The linear functionals \( \alpha^\vee \) and \( \beta^\vee \) restrict to \( \mathbb{Z}^2 \) as \( (2, a) \) and \( (b, 2) \) respectively; and these are linearly independent for the allowed values of \( a \) and \( b \).

The \( 2 \times 2 \) matrix \( T \) has determinant 1 and trace \( t = ab - 2 \), which is \(-2, -1, 0, \) or \( 1 \). Therefore the characteristic polynomial of \( T \) is \( x^2 - tx + 1 \). This polynomial is \( (x + 1)^2 \) if \( t = -2 \) (so that \( m = 0 \)). In the other three cases, it is the cyclotomic polynomial whose roots are the primitive \( m \)th roots of unity where \( m = 3, m = 4, \) and \( m = 6 \). Consequently \( T \) has order exactly \( m \). (When \( m = 2 \), we need also the fact that both \( a \) and \( b \) must be zero when \( ab = 0 \).)

Since \( s_\alpha^2 = s_\beta^2 = 1 \), any element of \( W \) is an alternating product of \( s_\alpha \)s and \( s_\beta \)s. A product of \( 2k \) terms starting with \( s_\alpha \) is \( T^k \). A product of \( 2k \) terms starting with \( s_\beta \) is \( T^{-k} = T^{m-k} \). A product of \( 2k + 1 \) terms starting with \( s_\alpha \) is \( T^k s_\alpha \). A product of \( 2k + 1 \) terms starting with \( s_\beta \) is \( T^{-k} s_\beta = T^{4-k} \).

Using these facts, we see easily that every element of \( W \) is on our list. That there are no duplications is also easy; I’ll skip that.

That \( W \cdot \{ \alpha, \beta \} \) consists of the indicated elements is easy. (Getting rid of the \( \pm \) is not hard, but I won’t worry about it.) To see that \( R_{\alpha, \beta} \) is the roots in a root datum, the only difficult point is to verify that each \( s_\gamma \) permutes the roots.

The first part of the reason is that if \( s(\alpha, \alpha^\vee) \) is the reflection defined by a pair \( r \in X^* \) and \( r^\vee \in X_* \) (required to satisfy \( \langle r, r^\vee \rangle = 2 \)), and \( A \) is any invertible endomorphism of \( X^* \), then

\[
s(Ar, (A^t)^{-1}(r^\vee)) = As(r, r^\vee)A^{-1}.
\]

That is, the reflection \( s_\gamma \) is obtained from \( s_\alpha \) (or \( s_\beta \)) by conjugation by some element \( w \in W \). If \( B \) is another endomorphism of \( X_* \), then

\[
s(Ar, (A^t)^{-1}(r^\vee)(Bx)) = As(r, r^\vee)(A^{-1}Bx).
\]

That says that \( s_\gamma \) preserves any \( W \) orbit, and so in particular preserves \( R_{\alpha, \beta} \). QED

2. Let

\[
X_* = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \mid x_1 + x_2 + x_3 + x_4 \in 2\mathbb{Z}\},
\]

a lattice of rank four. You may assume that the dual lattice is

\[
X^* = \{(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \mid \text{(all } \lambda_j \in \mathbb{Z}) \text{ or (all } \lambda_j \in \mathbb{Z} + 1/2)\}.
\]

There is a root datum living on these lattices with

\[
R^\vee_0 = \{\pm e_i \pm e_j \mid 1 \leq i \neq j \leq 4\} = R_0.
\]
the bijection between roots and coroots being the “obvious” one. You may assume that
\[(X_\ast, R_0^\vee, X^\ast, R_0)\]
is actually a root datum. Find all root data living on \(X_\ast\) and \(X^\ast\) with the property that
\[R_0^\vee \subset R^\vee, \quad R_0 \subset R.\]

First useful thing is to compute the group
\[W_0 = \text{group generated by all reflections in } R_0 \subset \text{Aut}(X^\ast).\]

We computed in class certainly that
\[s_{e_i - e_j} =_{\text{def}} \sigma_{ij} = \text{interchange } i \text{ and } j \text{ coords.}\]
I think we computed, and in any case it’s the same idea
\[s_{e_i + e_j} =_{\text{def}} \tau_{ij} = \text{interchange } i \text{ and } j \text{ coords and change their signs.}\]

As an easy consequence
\[W_0 = \text{permutation and even number of sign changes of four coords,}\]
\[|W_0| = 4! \cdot 2^3 = 192.\]

It’s more or less clear that in each orbit of \(W_0\) on \(X^\ast\) there is exactly one element \(\lambda_0\) such that
\[\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq |\lambda_4|.\] \((DOM)\)

Such an element is called dominant. The condition of being dominant can be expressed as
\[\langle \lambda, \beta^\vee \rangle \geq 0, \quad \beta \in \{e_1 - e_2, e_2 - e_3, e_3 - e_4, e_3 + e_4\}.\] \((DOM')\)

Similarly, in each orbit of \(W_0\) on \(X_\ast\) there is exactly one element \(x_0\) such that
\[x_1 \geq x_2 \geq x_3 \geq x_4|.\] \((DOM)\)

Such an element is called dominant. The condition of being dominant can be expressed as
\[\langle \alpha, x \rangle \geq 0, \quad \alpha \in \{e_1 - e_2, e_2 - e_3, e_3 - e_4, e_3 + e_4\}.\] \((DOM')\)

We want to investigate the possibilities for strictly larger root data. Suppose therefore that
\[\gamma \in R - R_0 \subset X^\ast\]
is a new root, and that
\[ \gamma^\vee \in R^\vee - R_0^\vee \subset X_* \]
is the corresponding coroot. Write \( \gamma^0 \) for the corresponding dominant root. Because dominance for \( \gamma^0 \) is a condition on coroots, and dominance for \( (\gamma^0)^\vee \) is a condition on the corresponding roots, the proposition above (saying that \( \langle \alpha, \beta^\vee \rangle \) and \( \langle \beta, \alpha^\vee \rangle \) have the same sign) guarantees that \( \gamma^\vee \) is also dominant.

Applying the proposition to the roots \( e_1 + e_2 \) and \( \gamma^0 \), we find that
\[ \langle e_1 + e_2, (\gamma^0)^\vee \rangle = (\gamma^0)^\vee_1 + (\gamma^0)^\vee_2 \]
is an integer between \(-3\) and 3. The integers \( (\gamma^0)^\vee \) are decreasing, have even sum, and all but perhaps the last are nonnegative; so the only candidates for \( (\gamma^0)^\vee \) are
\[
(2, 1, 1, 0), \quad (2, 0, 0, 0), \quad (1, 1, 1, 1), \quad (1, 1, 1, -1), \quad (1, 1, 0, 0).
\]
The last is ruled out by our assumption that \( (\gamma^0)^\vee \) does not belong to \( R_0^\vee \), leaving us with
\[
(2, 1, 1, 0), \quad (2, 0, 0, 0), \quad (1, 1, 1, 1), \quad (1, 1, 1, -1). \quad (Coroots)
\]
In every case, we find \( \langle e_1 + e_2, (\gamma^0)^\vee \rangle = 2 \) or 3. Again by the proposition, we conclude that
\[ \langle \gamma^0, e_1 + e_2 \rangle = 1. \]
The dominant elements of \( X^\ast \) satisfying this condition are
\[
(1, 0, 0, 0), \quad (1/2, 1/2, 1/2, 1/2), \quad (1/2, 1/2, 1/2, -1/2). \quad (Roots)
\]
If we add the condition \( \langle \gamma^0, (\gamma^0)^\vee \rangle = 2 \), we find four candidate dominant (root, coroot) pairs. Consider first the candidates
\[ (\gamma^0)^\vee = (2, 1, 1, 0), \quad \gamma^0 = (1, 0, 0, 0). \]
Here we find
\[ \langle e_2 + e_3, (\gamma^0)^\vee \rangle = 2, \quad \langle \gamma^0, (e_2 + e_3)^\vee \rangle = 0, \]
contradicting the proposition that these must be zero or nonzero together. The remaining three candidate pairs are
\[ (\gamma_A^0)^\vee = (2, 0, 0, 0), \quad \gamma_A^0 = (1, 0, 0, 0); \]
\[ (\gamma_B^0)^\vee = (1, 1, 1, 1), \quad \gamma_B^0 = (1/2, 1/2, 1/2, 1/2); \]
\[ (\gamma_C^0)^\vee = (1, 1, 1, -1), \quad \gamma_C^0 = (1/2, 1/2, 1/2, -1/2); \]
What is added to \( R_0^\vee \) and \( R_0 \) must be a union of \( W_0 \) orbits. The candidates are
\[ S_A^\vee = \{ \pm 2e_i \}, \quad S_A = \{ \pm e_i \} \]
\[ S^\vee_B = \{(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) \mid \prod \epsilon_i = 1\}, \quad S_B = \{(\epsilon_1/2, \epsilon_2/2, \epsilon_3/2, \epsilon_4/2) \mid \prod \epsilon_i = 1\}. \]
\[ S^\vee_C = \{(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) \mid \prod \epsilon_i = -1\}, \quad S_B = \{(\epsilon_1/2, \epsilon_2/2, \epsilon_3/2, \epsilon_4/2) \mid \prod \epsilon_i = -1\}. \]

The reflection in \(2\epsilon_i\) changes the sign of the \(i\)th coordinate; so the group

\[ W_A = \text{group generated by reflections in } R_0 \text{ and } S_A \]

consists of all permutations and sign changes of the coordinates. This clearly permutes

\[ R_A = R_0 \cup S_A, \quad R_A^\vee = R_0^\vee \cup S_A^\vee. \]

The conclusion is that

\[ (X^*, R_A^\vee, X^*, R_A) \]

is in fact a root datum.

It is equally true that if we define

\[ R_B = R_0 \cup S_B, \quad R_B^\vee = R_0^\vee \cup S_B^\vee, \quad R_C = R_0 \cup S_C, \quad R_C^\vee = R_0^\vee \cup S_C^\vee \]

then

\[ (X^*, R_B^\vee, X^*, R_B), \quad (X^*, R_C^\vee, X^*, R_C) \]

are both root data. I am not sure of the simplest way to see these facts. The sets \( S = S_B \) or \( S_C \) each consist of four mutually “orthogonal” pairs

\[ \pm(\gamma_1^\vee, \gamma_1), \pm(\gamma_2^\vee, \gamma_2), \pm(\gamma_3^\vee, \gamma_3), \pm(\gamma_4^\vee, \gamma_4) \]

satisfying

\[ \langle \gamma_i^\vee, \gamma_j^\vee \rangle = 0 \quad (i \neq j). \]

Consequently each reflection \( s_{\gamma_i} \) permutes \( S \) (exchanging \( \pm \gamma_i \) and fixing the other six roots in \( S \)). We chose \( S \) to be permuted by the reflections from \( R_0 \). That each reflection in \( S \) permutes \( R_0 \) is an easy calculation. These facts prove that we get root datum with \( B \) and \( C \).

It is clear that a reflection from \( S_A \) (a sign change in one coordinate) interchanges \( S_B \) and \( S_C \). It is also true, if not quite as obvious, that a reflection from \( S_B \) interchanges \( S_A \) and \( S_C \), and similarly with \( B \) and \( C \) reversed. These facts prove that the last possible root datum is

\[ R_{ABC} = R_0 \cup S_A \cup S_B \cup S_C, \quad R_{ABC}^\vee = R_0^\vee \cup S_A^\vee \cup S_B^\vee \cup S_C^\vee. \]

and that it is indeed a root datum. The group \( W_{ABC} \) generated by all reflections can be described as

\[ W_{ABC} \simeq W_0 \rtimes S_3; \]

the \( S_3 \) factor permutes \( S_A, S_B, \) and \( S_C \). Therefore

\[ |W_{ABC}| = 2^3 \cdot 4! \cdot 3! = 192 \cdot 6 = 1152. \]