A coroot calculation

June 7, 2023

Abstract

An informal account of the proof of the lemmas `is_root_system.coroot_symmetry_apply_eq` and `is_root_system.coroot_span_eq_top`.

1 The coroot of the reflection of a root

Recall our definition of the (pre)symmetry associated to a pair:

Definition 1.1. *Let k be a field of characteristic zero and V a vector space over k. Given a vector $x \in V$ and a linear form $f \in V^*$ the* ***pre-symmetry*** *associated to the pair (x, f) is the linear endomorphism of V:*

$$s_{x,f} : y \mapsto y - f(y)x. \tag{1}$$

If the condition $f(x) = 2$ holds then $s_{x,f}$ is invertible, satisfies $s_{x,f}^{-1} = s_{x,f}$, and we call it a ***symmetry****.*

Recall the uniqueness lemma:

Lemma 1.2. *Let k be a field of characteristic zero, V a vector space over k, and $\Phi \subseteq V$ a finite subset which spans V. Given a vector $x \in V$ and two linear forms $f, g \in V^*$ such that:*

- *$f(x) = 2$ and $s_{x,f}(\Phi) \subseteq \Phi$,*
- *$g(x) = 2$ and $s_{x,g}(\Phi) \subseteq \Phi$,*

then $f = g$.

Proof. We consider the automorphism:

$$u = s_{x,f} s_{x,g} : V \to V.$$

Using (1) we note that:

$$u = \mathbb{I} + (f - g) \otimes x,$$

where $\mathbb{I}$ is the identity map and we are using natural identification $V^* \otimes V \simeq \mathrm{End}(V)$. More generally it follows by induction that if $n \in \mathbb{N}$ then:

$$u^n = \mathbb{I} + n(f - g) \otimes x. \tag{2}$$

Now note that since $s_{x,f}$ and $s_{x,g}$ preserve Φ, so does u. However since Φ is a finite spanning set, any automorphism preserving it must have finite order. Thus there exists $n > 0$ such that $u^n = \mathbb{I}$. Using (2) it follows that:

$$n(f - g) \otimes x = 0.$$

Since $n > 0$, $x \neq 0$, and V has characteristic zero it follows that we must have $f - g = 0$ as required. □

Recall the definition of a root system:

Definition 1.3. *Let k be a field of characteristic zero, V and vector space over k, and $\Phi \subseteq V$. Then we say Φ is a **root system** in V over k if:*

- *Φ is finite,*
- *Φ spans V,*
- *for all $\alpha \in \Phi$, there exists $f \in V^*$ such that $f(\alpha) = 2$ and $s_{\alpha,f}(\Phi) \subseteq \Phi$,*
- *for all $\alpha \in \Phi$ and $f \in V^*$ such that $f(\alpha) = 2$ and $s_{\alpha,f}(\Phi) \subseteq \Phi$, we have $f(\Phi) \subseteq \mathbb{Z} \subseteq k$.*

*We call the elements of $\alpha \in \Phi$ **roots**.*

Recall the definition of the coroot and symmetry of a root:

Definition 1.4. *Let Φ be a root system in V over k and let $\alpha \in \Phi$ be a root. We define the **coroot** $\alpha^* \in V^*$ to be the unique linear form such that:*

- *$\alpha^*(\alpha) = 2$,*
- *$s_{\alpha,\alpha^*}(\Phi) \subseteq \Phi$.*

We emphasise that uniqueness follows from lemma 1.2. Furthermore we write:

$$s_\alpha = s_{\alpha,\alpha^*},$$

*and speak of the **symmetry** of a root.*

Now if α and β are two roots of some root system then $s_\alpha(\beta) \in \Phi$ is another root and thus has a coroot $(s_\alpha(\beta))^*$. In order to show that the set of coroots form a root system in V^* we need to calculate this coroot in terms of the coroots α^* and β^*. The following lemma gives the answer:

Lemma 1.5 (`is_root_system.coroot_symmetry_apply_eq`). *Let Φ be a root system for V over k and let $\alpha, \beta \in \Phi$ be a roots, then:*

$$(s_\alpha(\beta))^* = \beta^* - (\beta^*(\alpha))\alpha^*.$$

Proof. Let $\gamma = s_\alpha(\beta)$ and $g = \beta^* - (\beta^*(\alpha))\alpha^*$. By the uniqueness lemma 1.2 it is sufficient to show that:

(i) $g(\gamma) = 2$,

(ii) $s_{\gamma,g}(\Phi) \subseteq \Phi$.

We did the proof of (i) together on Wednesday: you just unfold all definitions, expand brackets, and use $\alpha^*(\alpha) = \beta^*(\beta) = 2$.

To prove (ii), since s_α and s_β both preserve Φ, it is sufficient to show that:

$$s_{\gamma,g} = s_\alpha \circ s_\beta \circ s_\alpha.$$

To prove this we just pick any vector $v \in V$ and unfold the left and right hand sides applied to v and observe that they are equal. $\square$

2 The span of the coroots

Definition 2.1. *Let V a vector space over a field k, G a finite group, and:*

$$\rho : G \to GL(k, V)$$

a group homomorphism (aka a representation of G on V). Given a bilinear form:

$$B : V \times V \to k,$$

we define a new bilinear form B_ρ as follows:

$$\begin{aligned} B_\rho : V \times V &\to k \\ (v, w) &\mapsto \sum_g B(g \cdot v, g \cdot w) \end{aligned} \tag{3}$$

where the notation $g \cdot v$ means $\rho(g)(v)$.

Lemma 2.2. *In the notation of definition 2.1, the form B_ρ is G-invariant, i.e.,*

$$B_\rho(g \cdot v, g \cdot w) = B_\rho(v, w),$$

for all v, w in V and g in G. Furthermore if k is an ordered field and B is symmetric and positive definite, then so is B_ρ.

Proof. These are just calculations using formula (3). □

Corollary 2.1. *Let ρ be a representation of a finite group G on a finite-dimensional vector space V over an ordered field k. There exists a G-invariant symmetric positive definite bilinear form on V.*

Proof. Pick any symmetric positive definite bilinear form[1] and apply lemma 2.2 to obtain an invariant form. □

Corollary 2.2. *Let Φ be a root system in a vector space V over an ordered field k and let:*

$$\rho : W \to GL(k, V)$$

be the corresponding representation of the Weyl group. There exists a W-invariant symmetric positive definite bilinear form on V. Note that the map ρ is an inclusion map because W is a subgroup of $GL(k, V)$.

Proof. This follows from lemma 2.1 because the Weyl group is finite. □

Lemma 2.3 (is_root_system.coroot_span_eq_top)**.** *Let Φ be a root system in a vector space V over an ordered field k. The coroots span V^*.*

Proof. It is sufficient to show that for any v in V:

$$(\alpha^*(v) = 0 \text{ for all } \alpha \in \Phi) \implies v = 0. \tag{4}$$

(Since a non-zero v satisfying (4) would define a non-zero linear form vanishing on the span of the α^*.)

Thus let v be a vector satisfying the hypothesis of (4). Note that we have:

$$s_\alpha(v) = v \text{ for all } \alpha \in \Phi.$$

[1] E.g., choose a basis and define the form to be the dot product of coordinates.

Using corollary 2.2 let B be a Weyl-group-invariant non-singular bilinear form on V. Let $\alpha \in \Phi$ and calculate:

$$\begin{aligned} B(v, \alpha) &= B(s_\alpha(v), s_\alpha(\alpha)) \\ &= B(v, -\alpha) \\ &= -B(v, \alpha). \end{aligned}$$

and so:

$$B(v, \alpha) = 0,$$

for all $\alpha \in \Phi$.

Since the roots span V and B is non-singular, we must have $v = 0$ as required. □

3 Bilinear forms

Definition 3.1. *A root system Φ in a vector space V over a field k, induces a bilinear form on V as follows:*

$$\begin{aligned} B_\Phi &: V \times V \to k, \\ &(v, w) \mapsto \sum_{\alpha \in \Phi} \alpha^*(v)\alpha^*(w). \end{aligned}$$

Lemma 3.2. *Let B_Φ be the bilinear form associated to a root system Φ in a vector space V over an ordered field k. Then B_Φ has the following properties:*

(i) it is symmetric,

(ii) it is positive definite,

(iii) it is invariant under the group of symmetries of the root system,

(iv) given $\alpha \in \Phi$:

$$\langle \alpha \rangle^\perp = \ker \alpha^*,$$

where $\langle \alpha \rangle^\perp$ is the orthogonal complement of α wrt B_Φ.

Proof. Claim (i) is clear.

Claim (ii) follows because the coroots span V^*. More precisely, since they span, given any non-zero v in V, there must exist some $\beta \in \Phi$ such that:

$$\beta^*(v) \neq 0.$$

We then have:

$$\begin{aligned}
0 &< \beta^*(v)^2 \\
&\leq \sum_{\alpha \in \Phi} (\alpha^*(v))^2 \\
&= B_\Phi(v, v)
\end{aligned}$$

as required.

For claim (iii), let $u : V \to V$ be a linear automorphism preserving Φ. Note that for any $\alpha \in \Phi$ we have the following generalisation of lemma 1.5 (this is essentially `is_root_system.coroot_apply_of_mem_symmetries` in the Lean code except with u^{-1} instead of u):

$$u^*(\alpha^*) = (u^{-1}(\alpha))^*,$$

where $u^* : V^* \to V^*$ is the transpose of $u : V \to V$. Given any v, w in V we thus calculate:

$$\begin{aligned}
B_\Phi(u(v), u(w)) &= \sum_{\alpha \in \Phi} \alpha^*(u(v))\alpha^*(u(w)) \\
&= \sum_{\alpha \in \Phi} (u^*(\alpha^*))(v)(u^*(\alpha^*))(w) \\
&= \sum_{\alpha \in \Phi} (u^{-1}(\alpha))^*(v)(u^{-1}(\alpha))^*(w) \\
&= \sum_{\alpha \in u^{-1}(\Phi)} \alpha^*(v)\alpha^*(w) \\
&= \sum_{\alpha \in \Phi} \alpha^*(v)\alpha^*(w) \\
&= B_\Phi(v, w)
\end{aligned}$$

as required.

For claim (iv) note that by taking $u = s_\alpha$ in part (iii), for any v in V we have:

$$\begin{aligned}
B_\Phi(\alpha, v) &= B_\Phi(s_\alpha(\alpha), s_\alpha(v)) \\
&= B_\Phi(-\alpha, v - \alpha^*(v)\alpha) \\
&= -B_\Phi(\alpha, v) + \alpha^*(v)B_\Phi(\alpha, \alpha)
\end{aligned}$$

And thus:

$$\alpha^*(v) = 2\frac{B_\Phi(\alpha, v)}{B_\Phi(\alpha, \alpha)},$$

from which the claim follows. □

4 Serre's construction of an invariant bilinear form

Lemma 4.1. *Let Φ be a root system in a vector space V over an ordered field k. Then there exists a positive-definite, symmetric, Weyl-group-invariant bilinear form on V.*

Proof. If $B'(x, y)$ is **any** positive-definite symmetric bilinear form on V, then the form

$$B(x, y) = \sum_{w \in W} B'(wx, wy)$$

is also positive-definite, symmetric and Weyl-group-invariant.

1. Symmetry: This follows directly from the symmetry of B, because for all $x, y \in V$:

   $(x, y) = \sum_{w \in W} B(wx, wy) = \sum_{w \in W} B(wy, wx) = (y, x)$.

2. Positive-Definiteness: Given a nonzero $x \in V$, $B(wx, wx) > 0$ for all $w \in W$, because B is positive-definite. So,

   $(x, x) = \sum_{w \in W} B(wx, wx) > 0$,

   which establishes the positive-definiteness of (x, y).

3. Invariant under the action of the Weyl group:

   For any $w' \in W$, we need to show that $(w'x, w'y) = (x, y)$ for all $x, y \in V$. As W is a group, for each $w' \in W$ the map $w \mapsto w'w$ permutes W. So, we have:

   $(w'x, w'y) = \sum_{w \in W} B(w(w'x), w(w'y)) = \sum_{w'w \in W} B(w'wx, w'wy)$.

   Now, relabelling $w'w$ as w because $w'w$ runs through all elements of W, we get:

   $(w'x, w'y) = \sum_{w \in W} B(wx, wy) = (x, y)$.

   Hence, (x, y) is invariant under the action of the Weyl group.

□

Definition 4.2 (Orthogonal transformation)**.** *An* orthogonal tranasformation *is a linear map on a Euclidean vector space that preserves the inner* *product. That is, a linear map $T : V \to V$ such that for all $v, w \in V$ we have:*

$$\langle Tv, Tw \rangle = \langle v, w \rangle.$$

where $\langle \cdot, \cdot \rangle$ is the inner product on V. The set of all orthogonal transformations on V is denoted $O(V)$.

The choice of B gives V the structure of a Euclidean vector space, present in most traditional definitions of root systems. With respect to this, the elements of the Weyl group W are *orthogonal transformations* of V because they leave B invariant. In particular, since the Weyl group is generated by the reflections s_α for $\alpha \in \Phi$, the symmetries s_α are orthogonal transformations.

This means that for all $v, w \in V$ and $\alpha \in \Phi$ we have:

$$B(s_\alpha(v), s_\alpha(w)) = B(v, w).$$

The key idea here is to let $w = s_\alpha(\alpha)$. Because s_α is involutive, we have $s_\alpha(w) = \alpha$. Thus:

$$B(s_\alpha(v), \alpha) = B(v, s_\alpha(\alpha)). \quad \forall v \in V$$

Expanding using the formula of $s_\alpha(v)$ gives that $\forall v \in V$:

$$\begin{aligned} B(v - \alpha^*(v)\alpha, \alpha) &= B(v, -\alpha) \\ B(v, \alpha) - \alpha^*(v)B(\alpha, \alpha) &= -B(v, \alpha) \\ 2B(v, \alpha) &= \alpha^*(v)B(\alpha, \alpha) \\ \alpha^*(v) &= 2\frac{B(v, \alpha)}{B(\alpha, \alpha)} \end{aligned}$$

Now, non-degenerate bilinear forms correspond to isomorphisms between a vector space and its dual. Thus, we can define a map $\varphi : \Phi \to V^*$ by $\alpha' \mapsto \alpha^*$, and extend this to a map $V \to V^*$ by linearity.

Hence, by definition

$$B(\alpha', x) = (\varphi(\alpha'))(x) = \alpha^*(x).$$

This gives us the equality

$$B(\alpha', x) = 2\frac{B(x, \alpha)}{B(\alpha, \alpha)}, \quad \forall x \in V.$$

Therefore

$$\alpha' = 2\frac{\alpha}{B(\alpha, \alpha)}.$$