Rational approximation in compact Lie groups and their Lie algebras II*

Patrick Eberlein (pbe@math.unc.edu)
Department of Mathematics, CB # 3250
University of North Carolina
Chapel Hill, NC 27599
December 1999

Introduction

Let G_o denote a compact, connected semisimple Lie group, U a finite dimensional real vector space and $\rho : G_o \to GL(U)$ a representation of G_o on U; that is, a Lie group homomorphism. The Lie algebra $\mathfrak{G}_o$ of G_o admits a (real Chevalley) basis $\mathfrak{C}_o$ whose structure constants are integers. Choosing a basis $\mathfrak{B}$ of U defines an associated homomorphism $\rho_{\mathfrak{B}} : H \to GL(n,\mathbb{R})$. Define $B(\mathbb{Z}, \mathfrak{C}_o)$ (respectively $B(\mathbb{Q}, \mathfrak{C}_o)$) to be the set of bases of U such that $d\rho(\mathfrak{C}_o)$ leaves invariant $\mathbb{Z}$ - span ($\mathfrak{B}$) (respectively $\mathbb{Q}$ - span ($\mathfrak{B}$)). For $\mathfrak{B} \in B(\mathbb{Q}, \mathfrak{C}_o)$, we define $G_{o,\mathfrak{B},\mathbb{Q}} = \{g \in G_o : \rho(g)$ leaves invariant $\mathbb{Q}$-span $(\mathfrak{B})\} = \{g \in G_o : \rho_{\mathfrak{B}}(g) \in GL(n,\mathbb{Q})\}$ and $G_{o,\mathbb{Q}} = \{g \in G_o : Ad(g)$ leaves invariant $\mathbb{Q}$ -span $(\mathfrak{C}_o)\}$. In [E] we showed 1) $B(\mathbb{Z}, \mathfrak{C}_o)$ is nonempty. 2) If $\mathfrak{B} \in B(\mathbb{Q}, \mathfrak{C}_o)$, then $\rho_{\mathfrak{B}}(G_o)$ is an affine algebraic group defined over $\mathbb{Q}$. 3) If $\mathfrak{B} \in B(\mathbb{Q}, \mathfrak{C}_o)$, then $G_{o,\mathfrak{B},\mathbb{Q}}$ is dense in G_o in the Lie group topology. In the present article we investigate the structure of the set $B(\mathbb{Q}, \mathfrak{C}_o)$ under a natural equivalence relation. In addition, for a basis $\mathfrak{B}$ in $B(\mathbb{Q}, \mathfrak{C}_o)$ we compare the group $G_{o,\mathfrak{B},\mathbb{Q}}$ for an arbitrary representation $\rho : G_o \to GL(U)$ to the corresponding group $G_{o,\mathbb{Q}}$ for the adjoint representation. Note that $G_{o,\mathbb{Q}} = G_{o,\mathfrak{B},\mathbb{Q}}$ in the case that $\rho = Ad$, $U = \mathfrak{G}_o$ and $\mathfrak{B} = \mathfrak{C}_o$.

---

* Supported in part by NSF grant DMS-9625452

AMS Subject Classification : 22E46

Define two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for U to be <u>$\mathbb{Q}$ - equivalent</u> if $\mathbb{Q}$ - span ($\mathcal{B}_1$) = $\mathbb{Q}$ - span ($\mathcal{B}_2$). In the first main result of this article, Theorem A in section 2, we show that every basis $\mathcal{B}'$ in B($\mathbb{Q}$, $\mathcal{C}_o$) is $\mathbb{Q}$-equivalent to a basis $\mathcal{B} \in$ B($\mathbb{Z}$, $\mathcal{C}_o$).

Let Z($\mathfrak{G}_o$) = {T $\in$ GL(U) : T commutes with every element of $\mathfrak{G}_o$}. Let T $\in$ Z($\mathfrak{G}_o$), X $\in$ $\mathfrak{G}_o$ and $\mathcal{B} \in$ B($\mathbb{Q}$, $\mathcal{C}_o$) be arbitrary elements. It is evident that the matrices of X with respect to $\mathcal{B}$ and T($\mathcal{B}$) are the same, and hence Z($\mathfrak{G}_o$) acts on B($\mathbb{Q}$, $\mathcal{C}_o$). The action of Z($\mathfrak{G}_o$) clearly descends to the quotient space B($\mathbb{Q}$, $\mathcal{C}_o$) / ~, where ~ denotes the $\mathbb{Q}$-equivalence relation. The second main result , Theorem B in section 2, is that if ρ : $G_o \rightarrow$ GL(U) is an irreducible representation, then Z($\mathfrak{G}_o$) acts transitively on B($\mathbb{Q}$, $\mathcal{C}_o$) / ~, or equivalently, if $\mathcal{B}_1$ and $\mathcal{B}_2$ are any two bases in B($\mathbb{Q}$, $\mathcal{C}_o$), then there exists T $\in$ Z($\mathfrak{G}_o$) such that T($\mathcal{B}_1$) and $\mathcal{B}_2$ are $\mathbb{Q}$-equivalent.

We do not know if Z($\mathfrak{G}_o$) acts transitively on B($\mathbb{Q}$, $\mathcal{C}_o$) / ~ in the case that U is reducible. However, the complex analogue for reducible $\mathfrak{G}$-modules is true, where $\mathfrak{G}$ denotes a complex, semisimple Lie algebra. See Lemma C2 in section 3 for a precise statement.

The third main result, Theorem C in section 3, states that the group $G_{o,\mathcal{B},\mathbb{Q}}$ is independent of the basis $\mathcal{B}$ in B($\mathbb{Q}$, $\mathcal{C}_o$). Moreover, if ρ : $G_o \rightarrow$ GL(U) has finite kernel, then $G_{o,\mathcal{B},\mathbb{Q}}$ is a normal subgroup of $G_{o,\mathbb{Q}}$ and the quotient group $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}}$ is an abelian group in which every element has finite order.

The group $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}}$ is a strange invariant that depends only on the representation ρ: $G_o \rightarrow$ GL(U) and the orbit under Ad(G_o) of the real Chevalley basis $\mathcal{C}_o$ in the Lie algebra $\mathfrak{G}_o$ of G_o. If G_o = SU(2) and $\mathcal{C}_o$ is the "natural" real Chevalley basis in $\mathfrak{G}_o$, then for half of the real irreducible representations of SU(2) (those of real type) the group $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}}$ is the identity and for the other half (those of quaternionic type) it is an infinite abelian group in which every element has order two. See the appendix for details and a more precise description of $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}}$ in the second case.

We wish to thank Yves Benoist, Tom Brylawski, Marc Burger, Gopal Prasad and Shrawan Kumar for helpful conversations.

Section 1 Notation and preliminaries

We shall use the notation, definitions and results of [E] in this article. For the convenience of the reader we repeat the table of notation from [E]. All vector spaces, Lie groups and Lie algebras are finite dimensional.

α, β	arbitrary elements of the finite set Φ of roots in $\mathfrak{A}^*$
$\mathfrak{A}$	a Cartan subalgebra of $\mathfrak{G}$
$\mathfrak{A}_o$	$\mathbb{R}$-span $\{i H_\beta : \beta \in \Delta\}$, a maximal abelian subalgebra of $\mathfrak{G}_o$
A_α	the vector $\xi_\alpha - \xi_{-\alpha}$, an element of a real Chevalley basis $\mathcal{C}_o$ for $\mathfrak{G}_o$
$\mathcal{B}^*$	a basis for a finite dimensional complex vector space V
$\mathcal{B}$	a basis for a finite dimensional real vector space U
B_α	the vector $i\,\xi_\alpha + i\,\xi_{-\alpha}$, an element of a real Chevalley basis $\mathcal{C}_o$ for $\mathfrak{G}_o$
B	the Killing form of $\mathfrak{G}$
B_o	the Killing form of $\mathfrak{G}_o$
$\mathcal{C}$	a (complex) Chevalley basis for $\mathfrak{G}$ whose structure constants lie in $\mathbb{Z}$, $\mathcal{C} = \{H_\beta : \beta \in \Delta ; \xi_\alpha : \alpha \in \Phi\}$
$\mathcal{C}_o$	a real Chevalley basis whose structure constants lie in $\mathbb{Z}$ for a compact real form $\mathfrak{G}_o$ of $\mathfrak{G}$, $\mathcal{C}_o = \{i H_\beta : \beta \in \Delta ; A_\alpha, B_\alpha : \alpha \in \Phi^+\}$
Δ	a $\mathbb{Z}$ - base for Φ
Φ	the finite set of roots in $\mathfrak{A}^* = \mathrm{Hom}(\mathfrak{A}, \mathbb{C})$
Φ^+, Φ^-	the positive, negative roots of Φ as determined by Δ
F	$\mathbb{Q}(i) = \mathbb{Q} + i\mathbb{Q} = \{a + ib \in \mathbb{C} : a \in \mathbb{Q} \text{ and } b \in \mathbb{Q}\}$.
$\mathfrak{G}$	a complex semisimple Lie algebra

$\mathfrak{G}_\alpha$	the 1-dimensional eigenspace of $\mathfrak{G}$ on which ad A = α(A) Id for all A in $\mathfrak{A}$
$\mathfrak{G}_o$	a compact, real, semisimple Lie algebra ; the Lie algebra of G_o
$\mathfrak{G}_o{}^{\mathbb{C}}$	the complexification of $\mathfrak{G}_o$
G_o	a compact, connected semisimple Lie group
$G_{o,\mathbb{Q}}$	$\{g \in G_o$: Ad(g) leaves invariant $\mathbb{Q}$-span -$\mathcal{C}_o\}$
$G_{o,\mathcal{B},\mathbb{Q}}$	$\{g \in G_o : \rho(g)$ leaves invariant $\mathbb{Q}$-span $(\mathcal{B})\}$
H_α	the root vector in $\mathfrak{A}$ determined by a root α in Φ
λ	a highest or lowest weight in Λ(V), where V is a complex $\mathfrak{G}$-module
Λ	the set of abstract weights for $\mathfrak{G} = \{\mu \in \mathfrak{A}^* : \mu(H_\alpha) \in \mathbb{Z}$ for all $\alpha \in \Phi\}$, a vector lattice in $\mathfrak{A}^*$
Λ_r	the $\mathbb{Z}$- span of Φ in $\mathfrak{A}^*$, the root lattice of finite index in Λ
Λ(V)	a finite subset of $\mathfrak{A}^*$, the weights determined by $\mathfrak{A}$ and a complex G (or $\mathfrak{G}$) - module V
μ	an arbitrary weight in Λ(V), V a finite dimensional, complex $\mathfrak{G}$-module.
τ	the unique element of W such that τ^2 = Id, $\tau(\Phi^+) = \Phi^-$ and $\tau(\Phi^-) = \Phi^+$
T_σ	for $\sigma \in$ W, an element of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}} \cap$ GL(V) such that $T_\sigma(V_\mu) = V_{\sigma(\mu)}$ for all $\mu \in \Lambda$(V)
U	a real G_o-module or $\mathfrak{G}_o$ - module
$U^{\mathbb{C}}$	the complexification of U
$\mathfrak{U}(\mathfrak{G})$	the universal enveloping algebra of $\mathfrak{G}$
$\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$	the subring of $\mathfrak{U}(\mathfrak{G})$ generated by 1 and $\{(\xi_\alpha)^n / n! : \alpha \in \Phi$ and $n \in \mathbb{Z}^+\}$
V	a complex G_o - module or $\mathfrak{G}$ - module
$V^{\mathbb{R}}$	the realification of V, V considered as a vector space over $\mathbb{R}$
V_μ	the weight space of V on which A = μ(A) Id for all A in $\mathfrak{A}$
W	the Weyl group, a finite subgroup of GL($\mathfrak{A}$) or GL($\mathfrak{A}^*$)
ξ_α	a vector that spans $\mathfrak{G}_\alpha$ and is an element of a Chevalley basis of $\mathfrak{G}$

Section 2 Classification of invariant $\mathbb{Q}$ - bases for irreducible real $\mathfrak{G}_o$ - modules

We use the notation of sections 1 and 2 of [E]. In this section we consider finite dimensional, irreducible real $\mathfrak{G}_o$-modules U, where $\mathfrak{G}_o$ is a finite dimensional real Lie algebra that is compact and semisimple; that is, the Killing form of $\mathfrak{G}_o$ is negative definite.

Fix a real Chevalley basis $\mathfrak{C}_o$ of $\mathfrak{G}_o$ (cf. section 1.5 of [E]). Let B($\mathbb{Z}$, $\mathfrak{C}_o$) and B($\mathbb{Q}$, $\mathfrak{C}_o$) denote the set of all bases $\mathfrak{B}$ of U such that $\mathfrak{C}_o$ leaves invariant $\mathbb{Z}$ - span ($\mathfrak{B}$) and $\mathbb{Q}$ - span ($\mathfrak{B}$) respectively. In [E] we showed that B($\mathbb{Z}$, $\mathfrak{C}_o$) is nonempty.

Define two bases $\mathfrak{B}_1$ and $\mathfrak{B}_2$ for U to be <u>$\mathbb{Q}$ - equivalent</u> if $\mathbb{Q}$ - span ($\mathfrak{B}_1$) = $\mathbb{Q}$ - span ($\mathfrak{B}_2$). Our first result says that any basis $\mathfrak{B}$' in B($\mathbb{Q}$, $\mathfrak{C}_o$) is $\mathbb{Q}$ - equivalent to a basis in B($\mathbb{Z}$, $\mathfrak{C}_o$).

Theorem A

Let $\mathfrak{G}_o$ be a compact, semisimple Lie algebra, and let U be an irreducible, real $\mathfrak{G}_o$ -module. Let $\mathfrak{B}$' be any $\mathbb{R}$-basis for U such that $\mathfrak{C}_o$ leaves invariant $\mathbb{Q}$-span ($\mathfrak{B}$'). Then there exists an $\mathbb{R}$-basis $\mathfrak{B}$ of U such that

1) $\mathfrak{C}_o$ leaves invariant $\mathbb{Z}$ - span ($\mathfrak{B}$).

2) $\mathbb{Q}$-span ($\mathfrak{B}$) = $\mathbb{Q}$-span ($\mathfrak{B}$').

Proof

We consider separately the two types of real irreducible $\mathfrak{G}_o$-modules described in section 3.1 of [E]. We use the notation of sections 1 and 2 of [E].

Case 1 V= $U^{\mathbb{C}}$ is an irreducible complex $\mathfrak{G} = \mathfrak{G}_o{}^{\mathbb{C}}$-module

1) Let F = $\mathbb{Q}$ + i$\mathbb{Q}$ = {a + ib ∈ $\mathbb{C}$: a ∈ $\mathbb{Q}$ and b ∈ $\mathbb{Q}$}. By hypothesis $\mathfrak{C}_o$ = $\{i H_\beta : \beta \in \Delta ; A_\alpha, B_\alpha : \alpha \in \Phi^+\}$ leaves invariant $\mathbb{Q}$-span ($\mathfrak{B}$'), and hence the Chevalley basis $\mathfrak{C} = \{H_\beta : \beta \in \Delta ; \xi_\alpha : \alpha \in \Phi\}$ for $\mathfrak{G} = \mathfrak{G}_o{}^{\mathbb{C}}$ leaves invariant F-span ($\mathfrak{B}$'). It follows that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves F-span ($\mathfrak{B}$') invariant since $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ is the subring of $\mathfrak{U}(\mathfrak{G}) \subseteq \mathrm{End}(V)$ generated by Id and $\{(\xi_\alpha)^n / n! : \alpha \in \Phi \text{ and } n \in \mathbb{Z}^+\}$.

Let λ be the highest weight in $\Lambda(V)$, and let V_λ denote the corresponding highest weight space. Recall that the projection map $\pi_\lambda: V \to V_\lambda$ lies in $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ ([Hu, p. 156]). Since F is dense in $\mathbb{C}$, V = F-span ($\mathcal{B}$') and $V_\lambda = \pi_\lambda(V)$ we conclude

a) $V_\lambda \cap$ F-span ($\mathcal{B}$') is a dense subset of V_λ.

There exists a unique element τ in the Weyl group W such that τ^2 = Id, $\tau(\Phi^+) = \Phi^-$ and $\tau(\Phi^-) = \Phi^+$ (cf.Proposition 2.3b of [E]). Let T_τ be the transformation in $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}} \cap GL(V)$ constructed in Proposition 2.4a of [E]. Next, we assert

b) There exist nonzero vectors v^+, v^- in $V_\lambda \cap$ F-span ($\mathcal{B}$') such that

$(J \circ T_\tau)(v^+) = v^+$ and $(J \circ T_\tau)(v^-) = -(v^-)$.

If $J : V \to V$ is the conjugation map determined by U, then J is the identity on $\mathbb{Q}$-span ($\mathcal{B}$') and hence J leaves F-span ($\mathcal{B}$') invariant. If τ and T_τ are as above, then T_τ and hence also $J \circ T_\tau$ leave F-span ($\mathcal{B}$') invariant. By Proposition 3.2d of [E] we see that $J \circ T_\tau$ leaves V_λ invariant and $(J \circ T_\tau)^2$ = Id on V_λ. Hence $J \circ T_\tau$ leaves invariant $V'_\lambda = V_\lambda \cap$ F-span ($\mathcal{B}$'), which by a) is a nonzero vector space over F. The conjugate linearity of $J \circ T_\tau$ combined with a) shows that the +1 and –1 eigenspaces of $J \circ T_\tau$ in V'_λ are both nonempty, which proves b).

We now use $\mathcal{B}$' to construct a basis $\mathcal{B}$ in $B(\mathbb{Z}, \mathcal{C}_o)$. Let v be any nonzero vector in $V_\lambda \cap$ F-span ($\mathcal{B}$') that is fixed by $J \circ T_\tau$. Note that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$ is a finitely generated $\mathbb{Z}$- module (cf. [Hu, p.156]), and hence there exists a finite $\mathbb{Z}$-basis $\mathcal{B}^*$ of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$ and a finite $\mathbb{Z}$-basis $\mathcal{B}$ of U_v = $\mathbb{Z}$-span {Re ($\mathcal{B}^*$), Im ($\mathcal{B}^*$)}= $\mathbb{Z}$-span {Re ($\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$) , Im ($\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$)} The proof of the theorem in section 4 of [E] shows that $\mathcal{B}$ is an $\mathbb{R}$-basis of U with $\mathcal{B} \in B(\mathbb{Z}, \mathcal{C}_o)$.

The basis $\mathcal{B}$ satisfies 1) of Theorem A. We prove 2). Let v and $\mathcal{B}$ be as in the previous paragraph. Since $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v) \subseteq$ F-span ($\mathcal{B}$') it follows that Re ($\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$) $\subseteq$ $\mathbb{Q}$-span ($\mathcal{B}$') and Im ($\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$) $\subseteq$ $\mathbb{Q}$-span ($\mathcal{B}$'). Therefore $\mathbb{Q}$-span ($\mathcal{B}$) $\subseteq$ $\mathbb{Q}$-span ($\mathcal{B}$'). Equality follows since both $\mathcal{B}$ and $\mathcal{B}$' have the same cardinality as $\mathbb{R}$-bases of U and are linearly independent over $\mathbb{Q}$. This completes the proof of 2) and of Theorem A in Case 1. $\square$

Case 2 **$U = V^{\mathbb{R}}$, where V is an irreducible complex $\mathfrak{G} = \mathfrak{G}_o{}^{\mathbb{C}}$- module**

We break the proof into a series of smaller steps. As in case 1 we let λ denote the highest weight in $\Lambda(V)$, with corresponding highest weight space V_λ. Let $V = V_o \dotplus \sum_{\mu \in \Lambda(V)} V_\mu$ (direct sum) denote the weight space decomposition determined by the Cartan subalgebra $\mathfrak{A}$ to which the Chevalley basis $\mathcal{C}$ is associated. Let $\{\pi_\mu : V \to V_\mu\}$ denote the corresponding projection maps, which all belong to $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ ([Hu, p.156]).

Lemma A1

1) $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant F-span ($\mathcal{B}'$), and F-span ($\mathcal{B}'$) $\cap V_\lambda \neq \{0\}$.

2) The F-vector space V'_λ = F-span ($\mathcal{B}'$) $\cap V_\lambda$ is 1-dimensional over F.

Proof

The proof of 1) is contained in the first part of the proof of Theorem A in case 1. If ξ and ξ' are any two nonzero elements in F-span ($\mathcal{B}'$) such that $\xi' = c\xi$ for some $c \in \mathbb{C}$, then it is easy to see that $c \in F$. Assertion 2) now follows immediately from 1) and the fact that V_λ is 1-dimensional over $\mathbb{C}$ by the irreducibilty of V. $\square$

For the rest of the proof of the proposition we fix a nonzero element v of F-span ($\mathcal{B}'$) $\cap V_\lambda$, which is possible by Lemma A1. We fix also a $\mathfrak{G}_o$-invariant Hermitian inner product < , > on V such that <v, v> = 1. Let $\mathcal{B}^*$ be a finite $\mathbb{Z}$-basis of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$. We show that $\mathcal{B} = \mathcal{B}^* \cup i\, \mathcal{B}^*$ is an $\mathbb{R}$-basis of U satisfying the two conditions of Theorem A.

The proof of the theorem in section 4 of [E] shows that $\mathcal{B}$ is an $\mathbb{R}$-basis of U with $\mathcal{B} \in B(\mathbb{Z}, \mathcal{C}_o)$; that is, $\mathcal{B}$ satisfies 1) of Theorem A.

Before proving 2) of Theorem A we first reduce to the case that $\mathcal{B} = \mathcal{B}^* \cup$

i $\mathcal{B}^*$, where $\mathcal{B}^*$ is a special $\mathbb{Z}$-basis of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$ that is a union of $\mathbb{C}$-bases $\mathcal{B}_o{}^*$ for V_o and $\mathcal{B}_\mu{}^*$ for V_μ , $\mu \in \Lambda(V)$. Such a basis $\mathcal{B}^*$ exists by 3) of Proposition 2.4c of [E]. If $\mathcal{B}_1{}^*$ is any other $\mathbb{Z}$-basis of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v)$ and $\mathcal{B}_1 = \mathcal{B}_1{}^* \cup i\ \mathcal{B}_1{}^*$, then $\mathbb{Q}$-span $(\mathcal{B}_1) = \mathbb{Q}$-span $(\mathcal{B})$ since $\mathbb{Z}$-span $(\mathcal{B}_1{}^*) = \mathbb{Z}$-span $(\mathcal{B}^*)$. Moreover, $\mathbb{R}$-span $(\mathcal{B}_1) = \mathbb{R}$-span $(\mathcal{B})$ and $|\mathcal{B}_1| = |\mathcal{B}| = \mathbb{Z}$-rank $(\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v))$. Hence $\mathcal{B}_1$ is an $\mathbb{R}$-basis of U, and $\mathbb{Q}$-span $(\mathcal{B}_1) = \mathbb{Q}$-span $(\mathcal{B}') \Leftrightarrow \mathbb{Q}$-span $(\mathcal{B}) = \mathbb{Q}$-span $(\mathcal{B}')$.

To prove 2) we need some further preparation.

Lemma A2

1) If $T \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$, then $T^* \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$, where T^* denotes the metric adjoint of T relative to < , >.

2) Let $\mu \in \Lambda(V)$ be given, and let v_μ be any nonzero element of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v) \cap V_\mu$. Then there exists $T \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ such that $T(v) = v_\mu$ and $T^*(V_\mu) = V_\lambda$.

Proof

1) The ring $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ by definition is generated in End(V) by Id and $\{\tau_{\alpha,n} = \xi_\alpha{}^n / n!$, where $n \in \mathbb{Z}^+$ and $\alpha \in \Phi\}$. By 1) of Proposition 2.5b of [E] we know that $\tau_{\alpha,n}{}^* = \tau_{-\alpha,n}$ for all $n \in \mathbb{Z}^+$ and $\alpha \in \Phi$, which completes the proof.

2) By hypothesis there exists $\varphi \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$, such that $\varphi(v) = v_\mu$. As an element of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$, φ is a finite sum of elements of End(V) of the form $\{(\tau_{\alpha_1, n_1}) \dots (\tau_{\alpha_N, n_N})\}$,where $\alpha_i \in \Phi$ and $n_i \in \mathbb{Z}^+$ for all i}. Divide the summands of φ into two disjoint sets, namely $A_1 = \{ (\tau_{\alpha_1, n_1}) \dots (\tau_{\alpha_N, n_N})\} : (\sum_{i=1}^{N} n_i\alpha_i) + \lambda = \mu\}$ and $A_2 = \{ (\tau_{\alpha_1, n_1}) \dots (\tau_{\alpha_N, n_N}) : (\sum_{i=1}^{N} n_i\alpha_i) + \lambda \neq \mu\}$. Let $T \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ be that element obtained from φ by keeping the terms from A_1 and discarding the terms from A_2. It is well known (cf. [Hu, p.107]) that for any $\alpha \in \Phi$ and $\sigma \in \Lambda(V)$, $\mathfrak{G}_\alpha(V_\sigma) \subseteq V_{\sigma+\alpha}$ if $\sigma + \alpha \in \Lambda(V)$ and $\mathfrak{G}_\alpha(V_\sigma) = \{0\}$ otherwise. By inspection $T(v) = \varphi(v) = v_\mu$, and T^* is a sum of terms of the form $\{ (\tau_{\alpha_1, n_1}) \dots (\tau_{\alpha_N, n_N})\}^* =$

$\{ (\tau_{-\alpha_N}, n_N) \ldots (\tau_{-\alpha_1}, n_1)\}$, where $(\sum_{i=1}^{N} n_i\alpha_i) + \lambda = \mu$. Since $\{ (\tau_{-\alpha_N}, n_N) \ldots (\tau_{-\alpha_1}, n_1)\} (V_\mu) \subseteq V_\lambda$ for each such term it follows that $T^* (V_\mu) \subseteq V_\lambda$. Note that $T^* (V_\mu) \neq \{0\}$ since $< T^*(v_\mu), v > = < v_\mu, T(v) > = < v_\mu, v_\mu > \neq 0$. We conclude that $T^* (V_\mu) = V_\lambda$ since V_λ is 1-dimensional. □

Lemma A3

Let $\mu \in \Lambda(V)$ and consider the basis $\mathcal{B}_\mu{}^* = \{v_1{}^*, \ldots v_m{}^*\}$ for V_μ. Then

1) $<v_i{}^*, v_j{}^* > \in \mathbb{Z}$ for all $1 \leq i, j \leq m$.

2) There exists a basis $\mathcal{B}_\mu{}^{**} = \{v_1{}^{**}, \ldots v_m{}^{**}\}$ for V_μ such that $<v_i{}^{**}, v_j{}^{**}> = 0$ if $i \neq j$ and $\mathbb{Q}$-span $\{v_1{}^{**}, \ldots, v_r{}^{**}\} =$ $\mathbb{Q}$-span $\{v_1{}^*, \ldots, v_r{}^*\}$ for every integer r with $1 \leq r \leq m$.

Proof

1) Since $\mathcal{B}_\mu{}^* \subseteq \mathcal{B}^* \subseteq \mathfrak{U}(\mathfrak{G})_\mathbb{Z}(v)$, Lemma A2 allows us to choose elements $T_i \in \mathfrak{U}(\mathfrak{G})_\mathbb{Z}$, $1 \leq i \leq m$, such that $T_i (v) = v_i{}^*$ and $T_i{}^* (V_\mu) = V_\lambda$ for all i. For $1 \leq i, j \leq m$ we compute $<v_i{}^*, v_j{}^* > = < T_i (v), T_j (v) > = < v, T_i{}^*T_j (v) >$. It suffices to prove that $T_i{}^*T_j (v) = k_{ij} v$ for some integer k_{ij} since $< v, v > = 1$ by the choice of $< , >$.

Note that $T_j (V_\lambda) \subseteq V_\mu$ since V_λ is spanned by v, and hence $T_i{}^*T_j (V_\lambda) \subseteq V_\lambda$. Lemma A2 shows that $T_i{}^*T_j \in \mathfrak{U}(\mathfrak{G})_\mathbb{Z}$ for all i, j, and it follows that $T_i{}^*T_j (v) \in \mathfrak{U}(\mathfrak{G})_\mathbb{Z}(v) \cap V_\lambda = \mathbb{Z}v$ by the lemma in the proof of Proposition 3.2e of [E]. We conclude that $T_i{}^*T_j (v) = k_{ij} v$ for some integer k_{ij}.

2) We proceed by induction on r, using 1). If orthogonal vectors $\{v_1{}^{**}, \ldots, v_r{}^{**}\}$ have been constructed so that $\{\mathbb{Q}$-span $\{v_1{}^{**}, \ldots, v_k{}^{**}\} = \mathbb{Q}$-span $\{v_1{}^*, \ldots, v_k{}^*\}$ for $1 \leq k \leq r$, then define $v_{r+1}{}^{**} = v_{r+1}{}^* - (\sum_{j=1}^{r} \{< v_{r+1}{}^*, v_j{}^{**} > / < v_j{}^{**}, v_j{}^{**} >\} v_j{}^{**}$. □

Lemma A4

$\mathcal{B}' \subseteq$ F-span $(\mathcal{B}^*)$, where $\mathcal{B}'$ is the original $\mathbb{R}$-basis of U such that $\mathfrak{C}_o$ leaves invariant $\mathbb{Q}$-span $(\mathcal{B}')$.

Proof

Let $\xi \in \mathcal{B}'$ and write $\xi = \xi_o + {}^\circ\sum_{\mu\in\Lambda(V)} \xi_\mu$, where $\xi_o \in V_o$ and $\xi_\mu \in V_\mu$ for all $\mu \in \Lambda(V)$. It suffices to prove that $\xi_o \in$ F-span ($\mathcal{B}_o$*) $\subseteq$ F-span ($\mathcal{B}$*) and $\xi_\mu \in$ F-span ($\mathcal{B}_\mu$*) $\subseteq$ F-span ($\mathcal{B}$*) for all $\mu \in \Lambda(V)$. We prove only that $\xi_\mu \in$ F-span ($\mathcal{B}_\mu$*) for all $\mu \in \Lambda(V)$ since the proof for the analogous assertion about ξ_o is similar.

By Lemma A3 there exists a basis $\mathcal{B}_\mu^{**} = \{v_1^{**}, \ldots v_m^{**}\}$ for V_μ such that $<v_i^{**}, v_j^{**}> = 0$ if $i \neq j$ and $\mathbb{Q}$-span ($\mathcal{B}_\mu$*) = $\mathbb{Q}$-span ($\mathcal{B}_\mu$**). Write $\xi_\mu = {}^\infty\sum_{j=1}^{m} c_j v_j^{**}$, where $c_j \in \mathbb{C}$ for all i. It suffices to prove that $c_j \in F$ for all j since F-span ($\mathcal{B}_\mu$*) = F-span ($\mathcal{B}_\mu$**).

Lemma A2 allows us to choose elements $T_i \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$, $1 \leq i \leq m$, such that $T_i(v) = v_i^{**}$ and $T_i^*(V_\mu) = V_\lambda$ for all i. Fix i and define $q_j \in \mathbb{C}$ by $T_i^*(v_j^{**}) = q_j v$ for all j. We compute $q_j = < T_i^*(v_j^{**}), v > = < v_j^{**}, T_i(v) > = < v_j^{**}, v_i^{**} > = 0$ if $i \neq j$. If $i = j$, then $q_i = < v_i^{**}, v_i^{**} > \in \mathbb{Q}$ by Lemma A3. It follows that $T_i^*(\xi_\mu) = (c_i q_i) v$. If $\pi_\mu : V \rightarrow V_\mu$ is the projection, then $\pi_\mu \in \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ (cf. [Hu, p.156]). Hence $\xi_\mu = \pi_\mu(\xi) \in$ F-span ($\mathcal{B}'$) and $T_i^*(\xi_\mu) \in$ F-span ($\mathcal{B}'$) $\cap V_\lambda$ by 1) of Lemma A1 and 1) of Lemma A2. It follows that $(c_i q_i) v = T_i^*(\xi_\mu) = c v$ for some $c \in F$ by 2) of Lemma A1, and we conclude that $c_i \in F$ since $q_i \in \mathbb{Q} \subseteq F$ and $q_i = < v_i^{**}, v_i^{**} > \neq 0$. □

The next result will prove 2) of Theorem A in case 2.

Lemma A5

Let $\mathcal{B} = \mathcal{B}^* \cup i\, \mathcal{B}^*$. Then $\mathbb{Q}$-span ($\mathcal{B}$) = $\mathbb{Q}$-span ($\mathcal{B}'$).

Proof

By the definition of $\mathcal{B}$, F-span ($\mathcal{B}$*) = $\mathbb{Q}$-span ($\mathcal{B}$), and hence $\mathbb{Q}$-span ($\mathcal{B}'$) $\subseteq$ $\mathbb{Q}$-span ($\mathcal{B}$) by Lemma A4. Equality holds since both $\mathcal{B}$ and $\mathcal{B}'$ have the same cardinality as $\mathbb{R}$-bases of U and are linearly independent over $\mathbb{Q}$. □

We now return to the second main result of this section, classifying up to $\mathbb{Q}$-equivalence the elements of B($\mathbb{Q}$, $\mathfrak{C}_o$). We consider only the case that U is irreducible. We begin with separate statements for each of the two cases listed in section 3.1 of [E], and then combine them into a single unified result in Theorem B.

Proposition B1

Let U be an irreducible, real $\mathfrak{G}_o$ - module such that V = $U^{\mathbb{C}}$ is an irreducible $\mathfrak{G}_o{}^{\mathbb{C}}$-module. Let $\mathfrak{C}_o$ be a real Chevalley basis for $\mathfrak{G}_o$. Let $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be bases of U such that $\mathfrak{C}_o$ leaves invariant $\mathbb{Q}$ - span ($\mathfrak{B}_i$) for i = 1, 2. Then $\mathfrak{B}_1$ is $\mathbb{Q}$ - equivalent to t$\mathfrak{B}_2$ for some nonzero real number t.

Proposition B2

Let U be an irreducible, real $\mathfrak{G}_o$ - module such that U = $V^{\mathbb{R}}$, where V is an irreducible, complex $\mathfrak{G}_o{}^{\mathbb{C}}$-module and $V^{\mathbb{R}}$ denotes V considered as a real vector space. Let $\mathfrak{C}_o$ be a real Chevalley basis for $\mathfrak{G}_o$. Let $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be bases of U such that $\mathfrak{C}_o$ leaves invariant $\mathbb{Q}$ - span ($\mathfrak{B}_i$) for i = 1, 2. Then $\mathfrak{B}_1$ is $\mathbb{Q}$ - equivalent to t$\mathfrak{B}_2$ for some nonzero complex number t.

We now combine the two results above into a single statement.

Theorem B

Let U be an irreducible, real $\mathfrak{G}_o$ - module, and let Z($\mathfrak{G}_o$) = {T ∈ GL(U) : T commutes with every element of $\mathfrak{G}_o$}. Let $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be any two elements of B($\mathbb{Q}$, $\mathfrak{C}_o$). Then there exists an element T of Z($\mathfrak{G}_o$) such $\mathfrak{B}_1$ and T($\mathfrak{B}_2$) are $\mathbb{Q}$-equivalent.

Proof of Theorem B

We assume Propositions B1 and B2 for the moment. Under the hypotheses of Proposition B1 we define T = t Id ∈ Z($\mathfrak{G}_o$), where t is the real number that appears in the statement of that result. We may restate Proposition B1 by saying that $\mathfrak{B}_1$ and T($\mathfrak{B}_2$) are $\mathbb{Q}$-equivalent.

Next, let t = a + i b be the complex number that appears in the statement of Proposition B2. Define J_o in $Z(\mathfrak{G}_o)$ to be multiplication by $i = \sqrt{-1}$. If $T = a\,Id + b\,J_o$, then $T \in Z(\mathfrak{G}_o)$, and we may restate Proposition B2 by saying that $\mathcal{B}_1$ and $T(\mathcal{B}_2)$ are $\mathbb{Q}$-equivalent.□

We now prove Propositions B1 and B2.

Proof of Proposition B1

Let λ be the highest weight in Λ(V), and let V_λ denote the corresponding highest weight space. Let τ be the unique element in the Weyl group W such that $\tau^2 = Id$, $\tau(\Phi^+) = \Phi^-$ and $\tau(\Phi^-) = \Phi^+$. Let T_τ be the transformation in $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}} \cap GL(V)$ constructed in Proposition 2.4a of [E]. By Propositions 3.2d and 3.2e of [E], $J \circ T_\tau$ leaves invariant V_λ, and its +1 eigenspace V_λ^+ is a 1-dimensional real subspace of V_λ.

For i = 1, 2, the discussion of case 1 in Theorem A , especially assertion b), says that there exists a nonzero vector v_i in F-span $(\mathcal{B}_i) \cap V_\lambda^+$, a finite $\mathbb{Z}$-basis $\mathcal{B}_i{}^*$ for $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v_i)$ and a finite $\mathbb{Z}$-basis $\mathcal{B}_i{}'$ for $\mathbb{Z}$-span {Re $(\mathcal{B}_i{}^*)$, Im $(\mathcal{B}_i{}^*)$} such that $\mathcal{B}_1{}'$ and $\mathcal{B}_2{}'$ are $\mathbb{R}$-bases for U and $\mathbb{Q}$ - span $(\mathcal{B}_i)$ = $\mathbb{Q}$ - span $(\mathcal{B}_i{}')$ for i = 1, 2. Since V_λ^+ is 1-dimensional over $\mathbb{R}$ there exists a nonzero real number t such that $v_1 = t\, v_2$. It follows routinely that $\mathbb{Q}$ - span $(\mathcal{B}_1)$ = t $\mathbb{Q}$ - span $(\mathcal{B}_2)$ = $\mathbb{Q}$ - span $(t\mathcal{B}_2)$; that is, $\mathcal{B}_1$ is $\mathbb{Q}$ - equivalent to $t\mathcal{B}_2$.□

Proof of Proposition B2

The proof is virtually identical to the proof of Proposition B1. For k = 1, 2, case 2 of Theorem A says that there exists a nonzero vector v_k in F-span $(\mathcal{B}_k) \cap V_\lambda$ and a finite $\mathbb{Z}$-basis $\mathcal{B}_k{}^*$ for $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v_k)$ such that if $\mathcal{B}_1{}' = \mathcal{B}_1{}^* \cup i\, \mathcal{B}_1{}^*$ and $\mathcal{B}_2{}' = \mathcal{B}_2{}^* \cup i\, \mathcal{B}_2{}^*$, then $\mathcal{B}_1{}'$ and $\mathcal{B}_2{}'$ are $\mathbb{R}$-bases for U and $\mathbb{Q}$ - span $(\mathcal{B}_k)$ = $\mathbb{Q}$ - span $(\mathcal{B}_k{}')$ for k = 1,2. The vector space V_λ is 1-dimensional over $\mathbb{C}$ since V is an irreducible, complex$\mathfrak{G}_o{}^{\mathbb{C}}$-module. Hence there exists a nonzero complex number t such that $v_1 = t\, v_2$. As above, it follows routinely that $\mathbb{Q}$ - span $(\mathcal{B}_1)$ = t $\mathbb{Q}$ - span $(\mathcal{B}_2)$ = $\mathbb{Q}$ - span $(t\mathcal{B}_2)$.□

Section 3 Properties of the rational subgroups $G_{o,\mathfrak{B},\mathbb{Q}}$

We adopt the following hypotheses and notation in this section. G_o is a compact, connected semisimple Lie group, and $\mathfrak{G}_o$ is the Lie algebra of G_o. U is a finite dimensional real vector space, and $\rho : G_o \to GL(U)$ is a representation with derived representation $d\rho : \mathfrak{G}_o \to End(U)$. As above, $\mathfrak{C}_o$ is a fixed real Chevalley basis of $\mathfrak{G}_o$, and $B(\mathbb{Q}, \mathfrak{C}_o)$ is the set of bases $\mathfrak{B}$ of U such that $d\rho(\mathfrak{C}_o)$ leaves invariant $\mathbb{Q}$ - span ($\mathfrak{B}$). For $\mathfrak{B} \in B(\mathbb{Q}, \mathfrak{C}_o)$, $G_{o,\mathfrak{B},\mathbb{Q}} = \{g \in G_o : \rho(g)$ leaves invariant $\mathbb{Q}$-span ($\mathfrak{B}$)$\}$. $G_{o,\mathbb{Q}} = \{g \in G_o : Ad(g)$ leaves invariant $\mathbb{Q}$ -span ($\mathfrak{C}_o$)$\}$.

The results of section 2 of [E] will be useful in this section, whose main result is

Theorem C

Let $\rho : G_o \to GL(U)$ be as above, and let $G_o^* = \{g \in G_o : c_{\rho(g)}$ leaves invariant $\mathbb{Q}$-span $\{d\rho(\mathfrak{C}_o)\}\}$, where $c_{\rho(g)}$ denotes conjugation in End(U) by $\rho(g)$. Then

1) The group $G_{o,\mathfrak{B},\mathbb{Q}}$ is independent of the basis $\mathfrak{B}$ in $B(\mathbb{Q}, \mathfrak{C}_o)$.
2) $G_{o,\mathbb{Q}} \subseteq G_o^*$, with equality if ρ has finite kernel.
3) $G_{o,\mathfrak{B},\mathbb{Q}}$ is the kernel of a homomorphism $\varphi : G_o^* \to A$, where A is an abelian group.
4) The group $G_o^* / G_{o,\mathfrak{B},\mathbb{Q}}$ is abelian, and every element of $G_o^* / G_{o,\mathfrak{B},\mathbb{Q}}$ has finite order.

Remarks

1) By 1) of Theorem C the abelian group $G_{o,\mathbb{Q}} / G_{o,\mathfrak{B},\mathbb{Q}}$ is independent of $\mathfrak{B}$ in $B(\mathbb{Q}, \mathfrak{C}_o)$ and hence depends only on the real Chevalley basis $\mathfrak{C}_o$ for $\mathfrak{G}_o$ and the representation $\rho : G_o \to GL(U)$. In fact, the isomorphism type of the group $G_{o,\mathbb{Q}} / G_{o,\mathfrak{B},\mathbb{Q}}$ is unchanged if we replace $\mathfrak{C}_o$ by $Ad(g)\mathfrak{C}_o$ for any $g \in G_o$, which corresponds to replacing the Cartan subalgebra $\mathfrak{A}$ of $\mathfrak{G} = \mathfrak{G}_o^{\mathbb{C}}$ by the Cartan subalgebra $\mathfrak{A}' = Ad(g)(\mathfrak{A})$ of $\mathfrak{G}$.

2) The group $G_o^* / G_{o,\mathcal{B},\mathbb{Q}}$ is sometimes an infinite group as we show in the appendix for certain irreducible real SU(2) modules. Note that in this case ρ always has finite kernel since SU(2) is simple.

Proof of Theorem C

The proof of 1) of Theorem C is rather lengthy, and we sketch a brief outline now. Recall that $F = \mathbb{Q}(i) = \mathbb{Q} + i\,\mathbb{Q}$. If $\mathcal{B}$ is a real basis of U, then $\mathcal{B}$ is also a complex basis of $V = U^{\mathbb{C}}$, and if $B \in B(\mathbb{Q}, \mathcal{C}_o)$, then $B \in B(F, \mathcal{C}) = \{\mathbb{C}$-bases $\mathcal{B}^*$ of V such that $\mathcal{C}$ leaves invariant F-span $(\mathcal{B}^*)\}$. Here $\mathcal{C}$ denotes the Chevalley basis of $\mathfrak{G} = \mathfrak{G}_o^{\mathbb{C}}$ that defines $\mathcal{C}_o$ (cf. section 1.5 of [E]). The key step in the proof is to show that $G_{o,\mathcal{B},\mathbb{Q}} = G_{o,\mathcal{B},F}$, where $G_{o,\mathcal{B},F} = \{g \in G_o : \rho(g)$ leaves invariant F-span $(\mathcal{B})\}$. Note that $Z(\mathfrak{G})$ commutes with $\mathfrak{G}_o$ and hence with G_o, which is generated by exp $(\mathfrak{G}_o)$ Furthermore, for any basis $\mathcal{B}$ in $B(F, \mathcal{C})$ and any elements T of $Z(\mathfrak{G})$ and g of G_o, the matrices of g relative to $\mathcal{B}$ and T $(\mathcal{B})$ are the same. In particular $G_{o,\mathcal{B},F}$ is independent of the basis $\mathcal{B}$ of $B(F, \mathcal{C})$ by Lemma C2 below, and 1) of Theorem C now follows immediately.

To prove 1) we need to work first with isotypic modules.

Let $\mathfrak{G}$ be a finite dimensional complex, semisimple Lie algebra. A complex $\mathfrak{G}$-module V is <u>isotypic</u> if any two irreducible submodules of V are equivalent as $\mathfrak{G}$-modules. If W is any irreducible complex submodule of V, then V is equivalent to the direct sum $W \oplus \ldots \oplus W$ (n times), where n is some positive integer. Moreover, $W \oplus \ldots \oplus W$ (n times) is equivalent to $W \otimes \mathbb{C}^n$, where $\mathfrak{G}$ acts trivially on the $\mathbb{C}^n$ factor by setting $X(v \otimes \xi) = X(v) \otimes \xi$ for all $v \in W$ and all $\xi \in \mathbb{C}^n$. Given a basis $\{\xi_1, \ldots, \xi_n\}$ of $\mathbb{C}^n$ one defines a $\mathfrak{G}$-homomorphism $\varphi : W \oplus \ldots \oplus W$ (n times) $\to W \otimes \mathbb{C}^n$ by $\varphi(v_1, \ldots, v_n) = \sum_{i=1}^{n} v_i \otimes \xi_i$. Given $v \in W$ and $\xi = \sum_{i=1}^{n} c_i\, \xi_i$ it follows that $\varphi(c_1 v, \ldots, c_n v) = v \otimes \xi$, and hence φ is surjective. We conclude that φ is an isomorphism since $W \oplus \ldots \oplus W$ (n times) and $W \otimes \mathbb{C}^n$ have the same dimension. Note that $\varphi^{-1}(W \otimes \xi)$ is an irreducible $\mathfrak{G}$-submodule of V for every $\xi \in \mathbb{C}^n$.

A real $\mathfrak{G}_o$-module U is isotypic if any two irreducible submodules of U are equivalent as $\mathfrak{G}_o$-modules. The discussion above of complex isotypic $\mathfrak{G}$-modules carries over to the real case.

To prove 1) of Theorem C we need some intermediate results. We recall the notation $F = \mathbb{Q}(i) = \mathbb{Q} + i\,\mathbb{Q} = \{a + bi \in \mathbb{C} : a \in \mathbb{Q} \text{ and } b \in \mathbb{Q}\}$.

Lemma C1

Let V be a complex $\mathfrak{G}$-module and write $V = V_1 \oplus \ldots \oplus V_p$, such that each V_i is an isotypic $\mathfrak{G}$-submodule equivalent to $W_i \otimes \mathbb{C}^{n_i}$, where n_i is a positive integer, W_i is an irreducible $\mathfrak{G}$-submodule of V and the submodules W_i, $1 \le i \le p$, are all inequivalent as $\mathfrak{G}$-modules. Fix a Chevalley basis $\mathcal{C}$ for $\mathfrak{G}$, and let $\mathcal{B}^*$ be a basis for V such that $\mathcal{C}$ leaves invariant F-span $(\mathcal{B}^*)$. Then there exists a basis $\mathcal{B}^{**}$ for V with the following properties :

1) $\mathcal{B}^{**}$ is a union of bases $\mathcal{B}_k^{**}$ for V_k for $1 \le k \le p$.

2) $\mathcal{C}$ and $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leave invariant $\mathbb{Z}$-span $(\mathcal{B}_k^{**})$ for $1 \le k \le p$.

3) F-span $(\mathcal{B}^*)$ = F-span $(\mathcal{B}^{**})$. $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant $\mathbb{Z}$-span $(\mathcal{B}^{**})$.

Proof of Lemma C1

Let $V = V_1 \oplus \ldots \oplus V_p$ be the decomposition of V into distinct isotypic components, and write $V_i = W_i \otimes \mathbb{C}^{n_i}$ as above.

If $W_i = (W_i)_o \mathbin{\dot{+}} \sum_{\mu \in \Lambda_i(W_i)} (W_i)_\mu$ (direct sum) is the weight space decomposition for W_i, then since $\mathfrak{G}$ acts trivially on the $\mathbb{C}^{n_i}$ factor of V_i, it is easy to see that $V_i = (W_i)_o \otimes \mathbb{C}^{n_i} \mathbin{\dot{+}} \sum_{\mu \in \Lambda_i(W_i)} \{(W_i)_\mu \otimes \mathbb{C}^{n_i}\}$ (direct sum) is the weight space decomposition for V_i. In particular W_i and V_i have the same weights. Let λ_i be the highest weight for W_i (hence also for V_i), and let W_{λ_i} denote the corresponding 1-

dimensional highest weight space for W_i. If V_{λ_i} is the highest weight space for V_i , then $V_{\lambda_i} = W_{\lambda_i} \otimes \mathbb{C}^{n_i}$ by the discussion above. Note that the highest weights $\{\lambda_i : 1 \le i \le p\}$ are all distinct since the irreducible $\mathfrak{G}$-modules $\{W_i : 1 \le i \le p\}$ are all inequivalent (cf. for example, [Hu, p. 109]). Hence every highest weight space for V is a highest weight space for V_i for some i.

Sublemma 1

1) Let v_i be any nonzero vector in W_{λ_i}. Then $V_{\lambda_i} = \{v_i \otimes \xi : \xi \in \mathbb{C}^{n_i}\}$.

2) Let $\mathcal{B}^*$ be a basis of $V = V_1 \oplus ... \oplus V_p$ such that $\mathfrak{C}$ leaves invariant F-span ($\mathcal{B}^*$). For every integer i with $1 \le i \le p$ there exists a nonzero vector v_i in W_{λ_i} and a dense subset X_i in $\mathbb{C}^{n_i}$ such that $\{v_i \otimes \xi : \xi \in X_i\} =$ F-span $(\mathcal{B}^*) \cap V_{\lambda_i}$.

Proof

1) This follows immediately from the fact that $V_{\lambda_i} = W_{\lambda_i} \otimes \mathbb{C}^{n_i}$ and W_{λ_i} is 1-dimensional.

2) Fix an integer i with $1 \le i \le p$. If π_i is the projection of V onto the highest weight space of V corresponding to λ_i, then π_i is an element of $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ ([Hu. p.156]). By the remark preceding sublemma 1, $\pi_i(V) = V_{\lambda_i} \subseteq V_i$, where V_{λ_i} is the highest weight space of V_i corresponding to λ_i.

Since $\mathfrak{C}$ leaves invariant F-span ($\mathcal{B}^*$) it follows that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant F-span ($\mathcal{B}^*$) (cf. the proof of 1) of Theorem A). We conclude that F-span $(\mathcal{B}^*) \cap V_{\lambda_i}$ is dense in V_{λ_i} since F-span ($\mathcal{B}^*$) is dense in V and F-span $(\mathcal{B}^*) \cap V_{\lambda_i}$ contains the subset π_i (F-span ($\mathcal{B}^*$)), which is dense in $\pi_i(V) = V_{\lambda_i}$. If v_i is any nonzero vector in F-span $(\mathcal{B}^*) \cap V_{\lambda_i}$, then 2) becomes an immediate consequence of 1). □

Sublemma 2

1) For every integer i with $1 \le i \le p$ there exists a nonzero vector v_i in W_{λ_i} and a basis $\{\xi_1, ... , \xi_{n_i}\}$ of $\mathbb{C}^{n_i}$ such that $\{v_i \otimes \xi_j : 1 \le j \le n_i\} \subseteq$ F-span $(\mathcal{B}^*) \cap V_{\lambda_i}$.

2) Let $\mathfrak{B}_i^*$ be a $\mathbb{Z}$-basis for $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ $(v_i) \subseteq W_i$, and let $\mathfrak{B}_i^{**}$ be the union of the sets $\{\mathfrak{B}_i^* \otimes \xi_j : 1 \le j \le n_i\}$. Then for all $1 \le i \le p$, $\mathfrak{B}_i^{**}$ is a basis for V_i such that $\mathfrak{B}_i^{**} \subseteq$ F-span $(\mathfrak{B}^*)$ and $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant $\mathbb{Z}$-span $(\mathfrak{B}_i^{**})$.

Proof

1) This follows immediately from 2) of Sublemma 1.

2) It is known that $\mathfrak{B}_i^*$ is a $\mathbb{C}$-basis of W_i for $1 \le i \le p$ since v_i is a nonzero highest weight vector of W_i. See for example [Hu, p.156]. If $\mathfrak{B}_i^{**}$ is the union of the sets $\{\mathfrak{B}_i^* \otimes \xi_j : 1 \le j \le n_i\}$, then $\mathbb{C}$-span $(\mathfrak{B}_i^{**}) \supseteq W_i \otimes \xi_j$ for $1 \le j \le n_i$ since $\mathfrak{B}_i^* \otimes \xi_j$ is a $\mathbb{C}$-basis for $W_i \otimes \xi_j$. Hence $\mathbb{C}$-span $(\mathfrak{B}_i^{**}) = W_i \otimes \mathbb{C}^{n_i} = V_i$ since $\{\xi_1, \ldots, \xi_{n_i}\}$ is a basis of $\mathbb{C}^{n_i}$. It follows that $\mathfrak{B}_i^{**}$ is a basis of V_i since $|\mathfrak{B}_i^{**}| = n_i\, |\mathfrak{B}_i^*| = \dim V_i$.

Clearly $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant $\mathbb{Z}$-span $(\mathfrak{B}_i^*) = \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ (v_i), and hence for $1 \le j \le n_i$ it follows that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ $((\mathfrak{B}_i^* \otimes \xi_j)) \subseteq$ $\mathbb{Z}$-span $(\mathfrak{B}_i^* \otimes \xi_j) \subseteq \mathbb{Z}$-span $(\mathfrak{B}_i^{**})$. It follows that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ $(\mathfrak{B}_i^{**}) \subseteq \mathbb{Z}$-span $(\mathfrak{B}_i^{**})$, or equivalently that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant $\mathbb{Z}$-span $(\mathfrak{B}_i^{**})$ for all $1 \le i \le p$.

By 1) and the fact that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant F-span $(\mathfrak{B}^*)$ it follows that F-span $(\mathfrak{B}^*)$ contains $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ $(v_i \otimes \xi_j) = \mathbb{Z}$-span $(\mathfrak{B}_i^* \otimes \xi_j)$ for $1 \le i \le p$ and $1 \le j \le n_i$. Hence F-span $(\mathfrak{B}^*) \supseteq \mathfrak{B}_i^{**}$ for $1 \le i \le p$, which completes the proof of 2).□

We now complete the proof of Lemma C1. Let $\mathfrak{B}^{**}$ be the union of the bases $\mathfrak{B}_i^{**}$ for V_i, $1 \le i \le p$. Then $\mathfrak{B}^{**}$ is a basis for V that satisfies 1) of Lemma C1. Assertion 2) of Lemma C1 follows from 2) of Sublemma 2 and the fact that $\mathfrak{C} \subseteq \mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ by the discussion in section 1.6 of [E]. Since $\mathfrak{B}_i^{**} \subseteq$ F-span $(\mathfrak{B}^*)$ for $1 \le i \le p$ by 2) of Sublemma 2 it follows that F-span $(\mathfrak{B}^{**}) \subseteq$ F-span $(\mathfrak{B}^*)$. Equality holds since $\mathfrak{B}^{**}$ and $\mathfrak{B}^*$ have the same cardinality as $\mathbb{C}$-bases of V and both are linearly independent over F. By 2) of Lemma C1, $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ $(\mathfrak{B}_i^{**}) \subseteq \mathbb{Z}$-span $(\mathfrak{B}_i^{**}) \subseteq \mathbb{Z}$-span $(\mathfrak{B}^{**})$ for $1 \le i \le p$. It follows that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant $\mathbb{Z}$-span $(\mathfrak{B}^{**})$, which completes the proof of 3) of Lemma C1.□

If $\mathcal{B}_1^*$ and $\mathcal{B}_2^*$ are two bases of a complex $\mathfrak{G}$-module V, then we say that $\mathcal{B}_1^*$ and $\mathcal{B}_2^*$ are F-equivalent if F-span ($\mathcal{B}_1^*$) = F-span ($\mathcal{B}_2^*$), where F = $\mathbb{Q}(i) = \mathbb{Q} + i\,\mathbb{Q}$. For a Chevalley basis $\mathcal{C}$ of $\mathfrak{G}$ we define B(F, $\mathcal{C}$) to be the set of $\mathbb{C}$-bases $\mathcal{B}^*$ of V such that $\mathcal{C}$ leaves invariant F-span ($\mathcal{B}^*$).

Lemma C2

Let V be an arbitrary complex $\mathfrak{G}$ - module, and let Z($\mathfrak{G}$) = {T ∈ GL(V) : T commutes with every element of $\mathfrak{G}$}. Fix a Chevalley basis $\mathcal{C}$ of $\mathfrak{G}$. Let $\mathcal{B}_1^*$ and $\mathcal{B}_2^*$ be any two elements of B(F, $\mathcal{C}$). Then there exists an element T of Z($\mathfrak{G}$) such that $\mathcal{B}_1^*$ and T($\mathcal{B}_2^*$) are F-equivalent.

Proof

Isotypic case

We first consider the case that $V = W \otimes \mathbb{C}^n$ is an isotypic module, where W is an irreducible $\mathfrak{G}$-module. Let $\mathcal{B}_1^*$ and $\mathcal{B}_2^*$ be any two bases in B(F, $\mathcal{C}$). Let λ be the highest weight for W (and hence also for V), and let W_λ denote the 1-dimensional highest weight space in W. Assertion 1) of Sublemma 2 in Lemma C1 shows

(*) There exist nonzero vectors v_1 and v_2 in W_λ and bases $\{\xi_j^1 : 1 \le j \le n\}$ and $\{\xi_j^2 : 1 \le j \le n\}$ for $\mathbb{C}^n$ such that $\{v_i \otimes \xi_j^i : 1 \le j \le n\} \subseteq$ F-span ($\mathcal{B}_i^*$) for i = 1,2.

Since W_λ is 1-dimensional we may choose a nonzero $\mu \in \mathbb{C}$ such that $\mu v_2 = v_1$. Let $T_\mu : W \to W$ denote multiplication by μ. Define $S \in GL(n,\mathbb{C})$ by requiring $S(\xi_j^2) = \xi_j^1$ for $1 \le j \le n$. If $T = T_\mu \otimes S$, then clearly T ∈ GL(V), and T commutes with $\mathfrak{G}$.

We assert that F-span ($\mathcal{B}_1^*$) = F-span (T($\mathcal{B}_2^*$)), which will complete the proof in the case that V is isotypic. By hypothesis $\mathcal{C}$ leaves invariant F - span ($\mathcal{B}_i^*$) for i = 1,2, and hence $\mathcal{C}$ also leaves invariant F-span (T($\mathcal{B}_2^*$)) = T {F-span ($\mathcal{B}_2^*$)} since T commutes with $\mathfrak{G}$. It follows that $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}$ leaves invariant both F-span ($\mathcal{B}_1^*$) and

F-span (T($\mathcal{B}_2^*$).

By the definition of T both F-span ($\mathcal{B}_1^*$) and F-span (T($\mathcal{B}_2^*$)) contain the set $\overline{\mathcal{B}}_1 = \{v_1 \otimes \xi_j^1 : 1 \le j \le n\}$. Hence by the observation above both F-span ($\mathcal{B}_1^*$) and F - span (T($\mathcal{B}_2^*$)) contain $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(\overline{\mathcal{B}}_1)$, which is the union of the sets $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v_1) \otimes \xi_j^1$ for $1 \le j \le n$. The set $\mathfrak{U}(\mathfrak{G})_{\mathbb{Z}}(v_1)$ contains a $\mathbb{C}$ - basis $\mathcal{B}^*$ for W ([Hu, p.156]). Hence if $\mathcal{B}^{**}$ is the union of the sets $\mathcal{B}^* \otimes \xi_j^1$ for $1 \le j \le n$, then $\mathcal{B}^{**}$ is a $\mathbb{C}$ - basis for V = W $\otimes\ \mathbb{C}^n$, and $\mathcal{B}^{**} \subseteq$ F-span ($\mathcal{B}_1^*$) $\cap$ F-span (T($\mathcal{B}_2^*$)). Since $\mathcal{B}^{**}$, $\mathcal{B}_1^*$ and T($\mathcal{B}_2^*$) are sets with the same cardinality that are linearly independent over F it follows that F-span ($\mathcal{B}_1^*$) = F-span ($\mathcal{B}^{**}$) = F-span (T($\mathcal{B}_2^*$)).

Nonisotypic case

We now consider the case that V is an arbitrary complex $\mathfrak{G}$-module, and we write $V = V_1 \oplus \dots \oplus V_p$, the decomposition of V into distinct maximal isotypic submodules V_i . Let $\mathcal{B}_1^*$ and $\mathcal{B}_2^*$ be any two bases in B(F, $\mathcal{C}$). By Lemma C1 we can find bases $\mathcal{B}_{i,\alpha}^{**}$ for V_α , $1 \le \alpha \le p$, i = 1, 2 such that if $\mathcal{B}_i^{**}$is the union of the bases $\mathcal{B}_{i,\alpha}^{**}$ for $1 \le \alpha \le p$ and i = 1, 2, then

1) $\mathcal{B}_i^{**}$ is a basis for V for i = 1, 2.

2) $\mathcal{C}$ leaves invariant F-span ($\mathcal{B}_{i,\alpha}^{**}$) for $1 \le \alpha \le p$, i = 1, 2.

3) F-span ($\mathcal{B}_i^*$) = F-span ($\mathcal{B}_i^{**}$) for i = 1,2.

By 2) and the isotypic case considered above there exists $T_\alpha \in GL(V_\alpha)$, $1 \le \alpha \le p$, such that T_α commutes with $\mathfrak{G}$ on V_α and F-span ($\mathcal{B}_{1,\alpha}^{**}$) = F-span ($T_\alpha$ ($\mathcal{B}_{2,\alpha}^{**}$)) for $1 \le \alpha \le p$. If $T = T_1 \times \dots \times T_p$, then $T \in GL(V)$ and T commutes with $\mathfrak{G}$ on V. Moreover, F-span ($\mathcal{B}_1^{**}$) = F-span (T ($\mathcal{B}_2^{**}$)) = T (F-span ($\mathcal{B}_2^{**}$)), and Lemma C2 now follows from 3) above.$\square$

We now complete the proof of 1) of Theorem C. We apply the sublemmas above in the case that $V = U^{\mathbb{C}}$ and $\mathfrak{G} = \mathfrak{G}_o^{\mathbb{C}}$. First we observe

(*) Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be bases in $B(\mathbb{Q}, \mathcal{C}_o)$, and let g be any element of G_o. Then g leaves invariant F-span ($\mathcal{B}_1$) $\Leftrightarrow$ g leaves invariant F-span ($\mathcal{B}_2$), regarding $\mathcal{B}_1$ and $\mathcal{B}_2$ as $\mathbb{C}$ - bases of V.

Proof

By the relationship between $\mathcal{C}$ and $\mathcal{C}_o$ described in section 1.5 of [E] it is easy to see that $\mathcal{B}_1$ and $\mathcal{B}_2$ belong to $B(F, \mathcal{C})$ since they belong to $B(\mathbb{Q}, \mathcal{C}_o)$. By Lemma C2 there exists an element T of $Z(\mathfrak{G})$ such that F-span ($\mathcal{B}_1$) = F-span (T ($\mathcal{B}_2$)) = T (F-span ($\mathcal{B}_2$)). The assertion (*) now follows immediately since T commutes with elements of G_o.

Now let $\mathcal{B}_1$ and $\mathcal{B}_2$ be any bases in $B(\mathbb{Q}, \mathcal{C}_o)$, and let g be any element of G_o. For j = 1,2 we note that F - span ($\mathcal{B}_j$) = $\mathbb{Q}$ - span ($\mathcal{B}_j$) + i $\mathbb{Q}$ - span ($\mathcal{B}_j$) and hence $\mathbb{Q}$ - span ($\mathcal{B}_j$) = F - span ($\mathcal{B}_j$) $\cap$ U. It follows that g leaves invariant $\mathbb{Q}$ - span ($\mathcal{B}_j$) $\Leftrightarrow$ g leaves invariant F - span ($\mathcal{B}_j$) since g(U) = U. Hence by (*) $G_{o, \mathcal{B}_1, \mathbb{Q}} = G_{o, \mathcal{B}_2, \mathbb{Q}}$. □

We now prove assertions 2), 3) and 4) of Theorem C. To prove 2) we need a preliminary result.

Lemma C3

Let H be any connected Lie group with Lie algebra $\mathfrak{H}$. Let U be a finite dimensional real vector space, and let $\rho : H \to GL(U)$ be a Lie group homomorphism with derived Lie algebra homomorphism $d\rho : \mathfrak{H} \to End(U)$. Then $d\rho\,(Ad(h)\,Z) = \rho(h) \circ d\rho(Z) \circ \rho(h)^{-1}$ for all $h \in H$ and all $Z \in \mathfrak{H}$.

Proof

For any $t \in \mathbb{R}$ we have $e^{t\, d\rho\, Ad(h)Z} = \rho\,(e^{t\, Ad(h)\, Z}) = \rho\,(h\, e^{t Z} h^{-1}) = \rho(h)\, e^{t\, d\rho(z)}\, \rho(h)^{-1}$. Differentiating at t = 0 proves the lemma. □

We now complete the proof of 2) of Theorem C. Let $g \in G_{o,\mathbb{Q}}$ and $Z \in \mathcal{C}_o$ be given. By hypothesis $Ad(g)Z \in \mathbb{Q}$-span ($\mathcal{C}_o$), and by the lemma above $\rho(g) \circ d\rho(Z) \circ \rho(g)^{-1} = d\rho\,(Ad(g)\,Z) \in \mathbb{Q}$-span ($d\rho\,(\mathcal{C}_o)$). This proves that $G_{o,\mathbb{Q}} \subseteq G_o{}^*$ since $g \in G_{o,\mathbb{Q}}$ and $Z \in \mathcal{C}_o$ were arbitrary.

Now let ρ have finite kernel, which implies that $d\rho : \mathfrak{G}_o \to \mathrm{End}(U)$ is injective and $d\rho^{-1} : d\rho(\mathfrak{G}_o) \to \mathfrak{G}_o$ exists. Given $g \in G_o^*$ and $Z \in \mathcal{C}_o$, we know that $d\rho\,(\mathrm{Ad}(g)\,Z) = \rho(g) \circ d\rho(Z) \circ \rho(g)^{-1} \in \mathbb{Q}$-span $(d\rho\,(\mathcal{C}_o)) = d\rho\,(\mathbb{Q}$-span $(\mathcal{C}_o))$ by the definition of G_o^*. Applying $d\rho^{-1}$ shows that $\mathrm{Ad}(g)\,Z \in \mathbb{Q}$-span $(\mathcal{C}_o)$, which proves that $G_o^* \subseteq G_{o,\mathbb{Q}}$. □

To prove assertions 3) and 4) of Theorem C we consider first the irreducible case and then pass to the reducible case.

The case that U is irreducible

3) We also need a preliminary result here.

Lemma C4

Let X be a finite dimensional real vector space, and let W be a subspace of End(X). Let $\mathcal{L} = \{Z_1, \ldots, Z_n\}$ and $\mathcal{B} = \{u_1, \ldots, u_m\}$ be bases for W and X respectively such that each Z_i has a $\mathbb{Q}$-matrix relative to $\mathcal{B}$. Let $Z \in W$ be an element such that Z has a $\mathbb{Q}$-matrix relative to $\mathcal{B}$. Then $Z \in \mathbb{Q}$-span $(\mathcal{L})$.

Proof Write $Z = \sum_{i=1}^{n} \alpha_i Z_i$, where $\alpha_i \in \mathbb{R}$ for all i. Define a positive definite inner product < , > on W by $\langle Z, Z^* \rangle = \sum_{i,j=1}^{n} Z_{ij} Z_{ij}^*$, where (Z_{ij}) and (Z_{ij}^*) are the matrices of Z and Z* relative to $\mathcal{B}$. By hypothesis $q_{ij} = \langle Z_i, Z_j \rangle \in \mathbb{Q}$ for all i,j and $r_j = \langle Z, Z_j \rangle \in \mathbb{Q}$ for all j. Hence QA = R, where $Q = (q_{ij})$, $A = (\alpha_1, \ldots, \alpha_n)^t$ and $R = (r_1, \ldots, r_n)^t$, and we conclude that $A = Q^{-1}R \in \mathbb{Q}^n$ since Q^{-1} and R have entries in $\mathbb{Q}$. □

For the rest of the proof in the irreducible case we fix a basis $\mathcal{B}$ of the G_o-module U such that $d\rho(\mathcal{C}_o)$ leaves invariant $\mathbb{Q}$-span $(\mathcal{B})$.

Step 1 $G_{o,\mathcal{B},\mathbb{Q}}$ is a subgroup of G_o^*.

Fix an element g of $G_{o,\mathcal{B},\mathbb{Q}}$. We show first that $\mathbb{Q}$-span $(\mathcal{B}) = \mathbb{Q}$-span $(\rho(g)(\mathcal{B}))$, which is equivalent to the statements $\rho(g)\,(\mathcal{B}) \subseteq \mathbb{Q}$-span $(\mathcal{B})$ and $\mathcal{B} \subseteq \mathbb{Q}$-span $(\rho(g)\,(\mathcal{B})$. The first inclusion follows since $g \in G_{o,\mathcal{B},\mathbb{Q}}$. Similarly, $\rho(g^{-1})\,(\mathcal{B}) \subseteq \mathbb{Q}$-span $(\mathcal{B})$, which implies that $\mathcal{B} \subseteq \rho(g)\,\{\mathbb{Q}$-span $(\mathcal{B})\} =$

$\mathbb{Q}$ -span ($\rho(g)$ ($\mathfrak{B}$).

Next, we show that the element $\{\rho(g) \circ d\rho(\mathfrak{C}_o) \circ \rho(g)^{-1}\}$ leaves invariant $\mathbb{Q}$ -span ($\mathfrak{B}$). By the previous paragraph we compute $\{\rho(g) \circ d\rho(\mathfrak{C}_o) \circ \rho(g)^{-1}\}$ ($\mathbb{Q}$ -span ($\mathfrak{B}$)) = $\{\rho(g) \circ d\rho(\mathfrak{C}_o) \circ \rho(g)^{-1}\}$ ($\mathbb{Q}$ -span ($\rho(g)$ ($\mathfrak{B}$)) = $\{\rho(g) \circ d\rho(\mathfrak{C}_o)\}$ ($\mathbb{Q}$ -span ($\mathfrak{B}$)) $\subseteq \rho(g)$ ($\mathbb{Q}$ -span ($\mathfrak{B}$)) $\subseteq \mathbb{Q}$ -span ($\mathfrak{B}$).

We apply Lemma C4 to W = $d\rho$ ($\mathfrak{G}_o$) and X = U. Choose $\{Z_1, \ldots , Z_m\} \subseteq \mathfrak{C}_o$ so that $\{d\rho\ (Z_1), \ldots, d\rho\ (Z_m)\}$ is a basis of $d\rho(\mathfrak{G}_o)$. For any $Z \in \mathfrak{C}_o$ the element $\rho(g) \circ d\rho(Z) \circ \rho(g)^{-1} = d\rho\ (Ad(g)\ Z)$ is an element of $d\rho(\mathfrak{G}_o)$ that has a $\mathbb{Q}$-matrix relative to $\mathfrak{B}$ by the discussion above. Hence $c_{\rho(g)}(d\rho(Z)) = \{\rho(g) \circ d\rho(Z) \circ \rho(g)^{-1}\} \in$ $\mathbb{Q}$-span $\{d\rho\ (Z_1), \ldots, d\rho\ (Z_m)\} \subseteq \mathbb{Q}$-span ($d\rho(\mathfrak{C}_o)$) by Lemma C4. It follows that $c_{\rho(g)}$ leaves invariant $\mathbb{Q}$-span $\{d\rho(\mathfrak{C}_o)$; that is, $g \in G_o^*$, which completes the proof of Step 1.

Next we consider the case that U is an irreducible $\mathfrak{G}_o$-module, and separate the arguments into the two cases 1) and 2) stated in section 3.1 of [E].

Step 2 Let $g \in G_o^*$. Then

1) If U is an irreducible $\mathfrak{G}_o$-module as in Case 1, then for every $g \in G_o^*$ the matrix of g relative to $\mathfrak{B}$ equals t C, where t is a nonzero real number and C is a $\mathbb{Q}$-matrix. Moreover, $t^n \in \mathbb{Q}$, where $n = \dim_{\mathbb{R}} U$.
2) If U is an irreducible $\mathfrak{G}_o$-module as in Case 2, then for every $g \in G_o^*$ the matrix of g relative to $\mathfrak{B}$ equals t C, where t is a nonzero complex number and C is a $\mathbb{Q}$-matrix. Moreover, $t^n \in \mathbb{Q}$, where $n = \dim_{\mathbb{R}} U$.

Proof

We prove 2) only since the proof of 1) is virtually identical, using Proposition B1 instead of Proposition B2. Let $g \in G_o^*$ and $Z \in \mathfrak{C}_o$ be given. Then $g^{-1} \in G_o^*$ and $\rho(g)^{-1} \circ d\rho(Z) \circ \rho(g) \in \mathbb{Q}$-span ($d\rho(\mathfrak{C}_o)$) by the definition of G_o^*. By the choice of $\mathfrak{B}$ we know that $\mathbb{Q}$-span ($d\rho(\mathfrak{C}_o)$) leaves invariant $\mathbb{Q}$-span ($\mathfrak{B}$). It follows that $\{\rho(g)^{-1} \circ d\rho(Z) \circ \rho(g)\}(\mathfrak{B}) \subseteq \mathbb{Q}$-span ($\mathfrak{B}$), which implies that $d\rho(Z)$ ($\rho(g)$ ($\mathfrak{B}$)) $\subseteq$

$\mathbb{Q}$-span ($\rho(g)$ ($\mathcal{B}$)). In particular, $d\rho(\mathcal{C}_o)$ leaves invariant $\mathbb{Q}$-span ($\rho(g)$ ($\mathcal{B}$)) since Z $\in$ $\mathcal{C}_o$ was arbitrary. Hence $\mathbb{Q}$-span ($\rho(g)$ ($\mathcal{B}$)) = $\mathbb{Q}$-span ($t\mathcal{B}$) = t $\mathbb{Q}$-span ($\mathcal{B}$) for some nonzero complex number t by Proposition B2. It follows that the matrix for $\rho(g)$ relative to $\mathcal{B}$ has the form t C, where C is an n x n matrix with entries in $\mathbb{Q}$.

The function $g \to \det \rho(g)$ is a continous homomorphism of G_o into the multiplicative nonzero real numbers $\mathbb{R}^*$. It follows that $\det \rho(g) = 1$ for all $g \in G_o$ since G_o is compact and connected. In particular, $1 = \det \rho(g) = t^n (\det C)$, which implies that $t^n \in \mathbb{Q}$ since $\det C \in \mathbb{Q}$. The proof of 1) and of Step 2 is complete.

Step 3 The group $G_{o,\mathcal{B},\mathbb{Q}}$ is the kernel of a homomorphism $\varphi_{\mathcal{B}} : G_o^* \to A$, where A is an abelian group that equals $\mathbb{C}^* / \mathbb{Q}^*$ in case 2 and $\mathbb{R}^* / \mathbb{Q}^*$ in case 1. Every element in the group $G_o^* / G_{o,\mathcal{B},\mathbb{Q}}$ has finite order that divides $n = \dim_{\mathbb{R}} U$.

Proof

Here $\mathbb{C}^*$,$\mathbb{R}^*$ and $\mathbb{Q}^*$ denote the nonzero elements of $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Q}$ respectively. As in Step 2 we consider case 2) only since the proof in case 1) is almost identical. Given $g \in G_o^*$ we know from Step 2 that the matrix of $\rho(g)$ relative to $\mathcal{B}$ has the form t C, where t is a nonzero complex number and C is an n x n matrix with entries in $\mathbb{Q}$. The complex number t and the matrix C are not unique, but it is easy to see that if t C = t* C*, where t* is another nonzero complex number and C* is another n x n matrix with entries in $\mathbb{Q}$, then $t / t^* \in \mathbb{Q}$. Now define $A = \mathbb{C}^* / \mathbb{Q}^*$, and let $\varphi_{\mathcal{B}} : G_o^* \to A$ be the map given by $\varphi_{\mathcal{B}}(g) = t\, \mathbb{Q}^* \in A$, where $\rho(g)$ has matrix t C relative to $\mathcal{B}$ and C has all entries in $\mathbb{Q}$. It is easy to check that $\varphi_{\mathcal{B}}$ is a well defined homomorphism whose kernel is $G_{o,\mathcal{B},\mathbb{Q}}$. Finally, since $t^n \in \mathbb{Q}$ by Step 2 it follows that $\varphi_{\mathcal{B}}(g)^n = 1$ in for all $g \in G_o^*$, which completes the proof of Step 3.

The proof of Theorem C is now complete in the case that U is irreducible since the proof of 3) is contained in the proof of Step 3) while 4) is an immediate consequence of Step 3.□

The case that U is reducible

Let U be a reducible G_o-module, and and write $U = U_1 \oplus \ldots \oplus U_N$, where each U_i is an irreducible G_o-module. For $1 \le i \le N$ let $\rho_i : G_o \to GL(U_i)$ denote the restriction of $\rho : G_o \to GL(U)$ to U_i, and let $G_{o,i}^* = \{g \in G_o : c_{\rho_i(g)}$ leaves invariant $\mathbb{Q}$-span $(d\rho_i(\mathfrak{C}_o))\}$. From the definition of G_o^* in the statement of Theorem C we obtain

(a) $G_o^* \subseteq \bigcap_{i=1}^{N} G_{o,i}^*$

Next, for $1 \le i \le N$ let $\mathfrak{B}_i$ be a basis of U_i such that $d\rho_i(\mathfrak{C}_o))$ leaves invariant $\mathbb{Q}$-span $(\mathfrak{B}_i)$, and let $\mathfrak{B} = \bigcup_{i=1}^{N} \mathfrak{B}_i$. Then $\mathfrak{B}$ is a basis of U such that $d\rho(\mathfrak{C}_o))$ leaves invariant $\mathbb{Q}$-span $(\mathfrak{B})$. If $G_{o,\mathfrak{B}_i,\mathbb{Q}} = \{g \in G_o : \rho_i(g)$ leaves invariant $\mathbb{Q}$-span $(\mathfrak{B}_i)\}$, then

(b) $G_{o,\mathfrak{B},\mathbb{Q}} = \bigcap_{i=1}^{N} G_{o,\mathfrak{B}_i,\mathbb{Q}}$

Note that $G_{o,\mathfrak{B},\mathbb{Q}}$ is independent of the basis $\mathfrak{B}$ in $B(\mathbb{Q},\mathfrak{C}_o)$ by 1) of Theorem C.

For $1 \le i \le N$, by the irreducible case just completed, there exists an abelian group A_i and a homomorphism $\varphi_i : G_{o,i}^* \to A_i$ such that $G_{o,\mathfrak{B}_i,\mathbb{Q}} = \mathrm{Ker}\,(\varphi_i)$. If $A = A_1 \times \ldots \times A_N$ and $\varphi = \varphi_1 \times \ldots \times \varphi_N$, then $\varphi : G_o^* \to A$ is a homomorphism by (a), and $\mathrm{Ker}\,(\varphi) = G_{o,\mathfrak{B},\mathbb{Q}}$ by (b). This proves 3) of Theorem C in the reducible case.

To prove 4) of Theorem C in the reducible case observe that $G_o^* / G_{o,\mathfrak{B},\mathbb{Q}}$ is isomorphic to $\varphi(G_o^*) = \varphi_1(G_{o,1}^*) \times \ldots \times \varphi_N(G_{o,N}^*) \subseteq A_1 \times \ldots \times A_N = A$. By (3) in the irreducible case every element of $\varphi_i(G_{o,i}^*)$ has finite order for $1 \le i \le N$, and hence every element of $\varphi(G_o^*)$ has finite order. The proof of 4) and hence of Theorem C is complete.□

Appendix SU(2) Examples

In this appendix we illustrate the results in the text for the irreducible, real representations of SU(2), which can be described completely and rather simply. Before beginning this description we obtain a result that will be immediately useful for the SU(2) representations and useful in general for real irreducible representations of type 1 in the terminology of Proposition 3.1a of [E].

Proposition A1

Let G_o be a compact, connected, semisimple Lie group with Lie algebra $\mathfrak{G}_o$. Let U be a finite dimensional real G_o-module, and let $V = U^{\mathbb{C}}$, a complex $\mathfrak{G}$-module ,where $\mathfrak{G} = \mathfrak{G}_o{}^{\mathbb{C}}$. Suppose that U and V admit respectively an $\mathbb{R}$-basis $\mathcal{B}$ and a $\mathbb{C}$-basis $\mathcal{B}^*$ with the following properties :

1) J leaves invariant $\mathbb{Q}$-span ($\mathcal{B}^*$), where $J : V \to V$ is the conjugation map determined by U.
2) $\mathbb{Q}$-span ($\mathcal{B}$) = $\mathbb{Q}$-span (Re ($\mathcal{B}^*$), Im ($\mathcal{B}^*$))

Then given $T \in$ End (U), T leaves invariant $\mathbb{Q}$-span ($\mathcal{B}$) $\Leftrightarrow$ T leaves invariant F-span ($\mathcal{B}^*$), where $F = \mathbb{Q}(i) = \mathbb{Q} + i\,\mathbb{Q}$.

Remark We have not assumed that either U or V is irreducible.

Before proving this result we derive two corollaries that allow us to use more familiar data and methods from the setting of complex semisimple Lie algebras.

Corollary 1

Let U, V, $\mathcal{B}$ and $\mathcal{B}^*$ be as above. Let $\mathcal{C} = \{H_\beta : \beta \in \Delta\ ; \xi_\alpha : \alpha \in \Phi\}$ be a Chevalley basis for $\mathfrak{G}$ such that $\mathfrak{G}_o = \mathbb{R}$-span ($\mathcal{C}_o$), where $\mathcal{C}_o = \{i\,H_\beta : \beta \in \Delta\ ; A_\alpha, B_\alpha : \alpha \in \Phi^+\}$ is the corresponding real Chevalley basis. Then $\mathcal{C}_o$ leaves invariant $\mathbb{Q}$-span ($\mathcal{B}$) $\Leftrightarrow$ $\mathcal{C}$ leaves invariant F-span ($\mathcal{B}^*$).

Corollary 2

Let $\mathcal{C} = \{H_\beta : \beta \in \Delta\ ; \xi_\alpha : \alpha \in \Phi\}$ be a Chevalley basis for $\mathfrak{G}$ such that $\mathfrak{G}_o = \mathbb{R}$-span ($\mathcal{C}_o$), where $\mathcal{C}_o = \{i\,H_\beta : \beta \in \Delta\ ; A_\alpha, B_\alpha : \alpha \in \Phi^+\}$ is the corresponding real Chevalley basis. Let G_o be any compact, connected semisimple Lie group with Lie algebra

$\mathfrak{G}_o$. If $g \in G_o$ is arbitrary, then Ad(g) leaves invariant $\mathbb{Q}$-span ($\mathfrak{C}_o$) $\Leftrightarrow$ Ad(g) leaves invariant F-span ($\mathfrak{C}$).

Proof of corollary 1

Observe that $A_\alpha = \xi_\alpha - \xi_{-\alpha}$ and $B_\alpha = i\,\xi_\alpha + i\,\xi_{-\alpha}$ for all $\alpha \in \Phi^+$, which imply that $\xi_\alpha = (1/2)\,(A_\alpha - i\,B_\alpha)$ and $\xi_{-\alpha} = -\,(1/2)\,(A_\alpha + i\,B_\alpha)$. Hence $\mathfrak{C}_o$ leaves invariant F-span ($\mathfrak{B}^*$) $\Leftrightarrow$ $\mathfrak{C}$ leaves invariant F-span ($\mathfrak{B}^*$). The assertion is now an immediate consequence of the proposition above.$\square$

Proof of corollary 2

We apply the proposition above to the adjoint representation Ad : $G_o \to GL(\mathfrak{G}_o)$ and the bases $\mathfrak{B} = \mathfrak{C}_o$ for $U = \mathfrak{G}_o$ and $\mathfrak{B}^* = \mathfrak{C}$ for $V = \mathfrak{G}_o{}^{\mathbb{C}}$. It is easy to verify from the relations between $\mathfrak{C}_o$ and $\mathfrak{C}$ as stated in the proof of corollary 1 that the bases $\mathfrak{C}_o$ and $\mathfrak{C}$ satisfy the conditions 1) and 2) of the proposition above.

To prove Proposition A1 we need a preliminary result.

Lemma

1) If $\xi \in$ F-span ($\mathfrak{B}^*$), then Re (ξ) $\in$ F-span ($\mathfrak{B}^*$) and Im (ξ) $\in$ F-span ($\mathfrak{B}^*$).

2) Re {F-span ($\mathfrak{B}^*$)} = Im {F-span ($\mathfrak{B}^*$)} = $\mathbb{Q}$-span ($\mathfrak{B}$).

3) F-span ($\mathfrak{B}^*$) = $\mathbb{Q}$-span ($\mathfrak{B}$) + i $\mathbb{Q}$-span ($\mathfrak{B}$).

Proof of the lemma

1) It suffices to show that the conjugation operator J leaves F-span ($\mathfrak{B}^*$) invariant since Re (ξ) = (1/2) (ξ+J(ξ)) and Im (ξ) = (1/ 2i) (ξ–J(ξ)). If $\mathfrak{B}^* = \{v_1, \ldots, v_n\}$ and $\xi \in$ F-span ($\mathfrak{B}^*$), then $\xi = \sum_{j=1}^{n}{}^{\circ} (\alpha_j + i\,\beta_j)\, v_j$, where $\alpha_j, \beta_j \in \mathbb{Q}$ for all j. Hence $J(\xi) = \sum_{j=1}^{n}{}^{\circ} (\alpha_j - i\,\beta_j)\, J(v_j) \in$ F-span ($\mathfrak{B}^*$) since J leaves invariant $\mathbb{Q}$-span ($\mathfrak{B}^*$) by hypothesis.$\square$

2) If $\xi \in$ F-span ($\mathfrak{B}^*$), then $i\,\xi \in$ F-span ($\mathfrak{B}^*$). Since Re (ξ) = Im ($i\,\xi$) and Im (ξ) = Re ($-\,i\,\xi$) it follows that Re {F-span ($\mathfrak{B}^*$} = Im {F-span ($\mathfrak{B}^*$}.

Let $\mathfrak{B}^* = \{v_1, \ldots, v_n\}$ and let $\xi \in$ F-span ($\mathfrak{B}^*$) be given. If we write ξ =

$\sum_{j=1}^{n} (\alpha_j + i\,\beta_j)\, v_j$, where $\alpha_j, \beta_j \in \mathbb{Q}$ for all j, then by breaking each v_j into real and imaginary parts we obtain

$\xi = \sum_{j=1}^{n} (\alpha_j \operatorname{Re}(v_j) - \beta_j \operatorname{Im}(v_j)) + i\,\{\sum_{j=1}^{n} (\alpha_j \operatorname{Im}(v_j) + \beta_j \operatorname{Re}(v_j))\}$. By hypothesis $\mathbb{Q}$-span $(\mathcal{B})$ = $\mathbb{Q}$-span (Re $(\mathcal{B}^*)$, Im $(\mathcal{B}^*)$) , and it follows that Re {F-span $(\mathcal{B}^*)$} = Im {F-span $(\mathcal{B}^*)$} $\subseteq$ $\mathbb{Q}$-span $(\mathcal{B})$. To show the reverse inclusion it suffices to show that $\mathcal{B} \subseteq$ Re {F-span $(\mathcal{B}^*)$} = Im {F-span $(\mathcal{B}^*)$. If $u \in \mathcal{B} \subseteq$ $\mathbb{Q}$-span (Re $(\mathcal{B}^*)$, Im $(\mathcal{B}^*)$), then we may write $u = u_1 + u_2$, where $u_1 \in$ $\mathbb{Q}$-span (Re $(\mathcal{B}^*)$) and $u_2 \in$ $\mathbb{Q}$-span (Im $(\mathcal{B}^*)$). Note that $\mathbb{Q}$-span (Re $(\mathcal{B}^*)$ = Re ($\mathbb{Q}$-span $(\mathcal{B}^*)$) $\subseteq$ Re {F-span $(\mathcal{B}^*)$}, and hence $u_1 \in$ Re {F-span $(\mathcal{B}^*)$}. Similarly $u_2 \in$ Im {F-span $(\mathcal{B}^*)$} = Re {F-span $(\mathcal{B}^*)$}, and we conclude that $u = u_1 + u_2 \in$ Im {F-span $(\mathcal{B}^*)$} = Re {F-span $(\mathcal{B}^*)$} for all $u \in \mathcal{B}$. □

3) If $\xi \in$ F-span $(\mathcal{B}^*)$, then Re (ξ) and Im (ξ) lie in $\mathbb{Q}$-span $(\mathcal{B})$ by 2), and hence F-span $(\mathcal{B}^*)$ $\subseteq$ $\mathbb{Q}$-span $(\mathcal{B})$ + i $\mathbb{Q}$-span $(\mathcal{B})$. To show the reverse inclusion it suffices to show that $\mathbb{Q}$-span $(\mathcal{B})$ $\subseteq$ F-span $(\mathcal{B}^*)$, but this is an immediate consequence of 1) and 2). □

Proof of Proposition A1

Let T be an element of End(U) that leaves invariant $\mathbb{Q}$-span $(\mathcal{B})$, and let $\xi \in$ F-span $(\mathcal{B}^*)$ be given. Then Re (ξ) and Im (ξ) belong to $\mathbb{Q}$-span $(\mathcal{B})$ by 2) of the lemma above, and it follows that T (ξ) = T (Re (ξ)) + i T (Im (ξ)) $\in$ $\mathbb{Q}$-span $(\mathcal{B})$ + i $\mathbb{Q}$-span $(\mathcal{B})$ = F-span $(\mathcal{B}^*)$ by 3) of the lemma. Conversely, let T be an element of End(U) that leaves invariant F-span $(\mathcal{B}^*)$, and let $x \in$ $\mathbb{Q}$-span $(\mathcal{B})$ be given. By 2) of the lemma x = Re (ξ) for some $\xi \in$ F-span $(\mathcal{B}^*)$, and hence T (x) = T (Re (ξ)) = Re (T (ξ)) $\in$ Re {F-span $(\mathcal{B}^*)$} = $\mathbb{Q}$-span $(\mathcal{B})$. □

Irreducible complex SU(2) representations

We describe first the irreducible, complex representations of SU(2) = $\{g \in GL(2, \mathbb{C}) : gg^* = Id, \det g = 1\}$, where g^* denotes the conjugate transpose of g. Hence SU(2) = $\left\{ \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} : \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1 \right\}$. SU(2) is also isomorphic to the group of unit quaternions acting on $\mathbb{H}$ by left translations, and hence SU(2) is diffeomorphic to S^3.

For each integer $n \geq 1$ let V_n denote the set of complex, homogeneous polynomials of degree n in the two complex variables z_1 and z_2. The complex dimension of V_n is n+1, and a natural basis for V_n is given by the set $\mathcal{B}^* = \{P_o, P_1, \ldots, P_n\}$, where $P_k(z_1, z_2) = z_1^k z_2^{n-k}$ for $0 \leq k \leq n$. GL(2, $\mathbb{C}$) acts on V_n by $(gP)(z_1, z_2) = P((z_1, z_2)g) = P(az_1 + cz_2, bz_1 + dz_2)$ for $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{C})$ and $P \in V_n$. The subgroup SU(2) acts irreducibly on V_n for each n, and each complex, irreducible representation of SU(2) is equivalent to V_n for some n. The representation of SU(2) on V_n is faithful for every positive integer n. See [B.- tD, pp. 84-86] for details.

Let $g_o = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \in GL(2,\mathbb{C})$. For each irreducible SU(2) module V_n let $c : V_n \to V_n$ be the unique conjugate linear map that fixes each P_k, $0 \leq k \leq n$. For each n we define the map $J = g_o \circ c : V_n \to V_n$, which can also be described by $(J\,P)(z_1, z_2) = \sum_{j=0}^{n} \overline{c_j}\, P_j\,(i z_2, -i z_1)$, where $P = \sum_{j=0}^{n} c_j P_j$.

The transformation J has the following properties :

1) J is conjugate linear

2) $J \circ g = g \circ J$ for all $g \in SU(2)$.

3) $J P_k = i^n (-1)^{n-k} P_{n-k}$ for all $0 \leq k \leq n$.

4) $J^2 = Id$ if n is even

5) $J^2 = -Id$ if n is odd.

Properties 1, 3), 4) and 5) follow routinely from the definition of J although 1) is also useful for the proofs of 4) and 5).

We prove 2). Let $g = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$ be an arbitrary element of SU(2). It suffices to show that $(J \circ g)(P_k) = (g \circ J)(P_k)$ for $0 \le k \le n$ since both $g \circ J$ and $J \circ g$ are conjugate linear maps of V_n. Note that $g_o \bar{g} = g g_o$ for all $g \in$ SU(2), where $\bar{g} = \begin{bmatrix} \bar{\alpha} & \bar{\beta} \\ -\beta & \alpha \end{bmatrix}$. For $0 \le k \le n$ it is easy to show that $gP_k = \sum_{j=o}^{n} Q_{kj}(g)\, P_j$, where each Q_{kj} is a polynomial with integer coefficients in the coordinate functions $\{z_{ij} : 1 \le i,j \le 2\}$ of $M(2,\mathbb{C})$. It follows immediately that $c(gP_k) = \bar{g}P_k$. Hence $(J \circ g)(P_k) = (g_o\bar{g})(P_k) = gg_o(P_k) = (g \circ J)(P_k)$.□

If n is even, then V_n is called of real type while if n is odd then V_n is called of quaternionic type because of the properties 1), 2) 4) and 5) above. See [B- tD, pp.93-100] for further details.

Irreducible real SU(2) representations

We now explain how each complex irreducible SU(2) - module V_n gives rise to a real irreducible SU(2)-module U_n. Every irreducible SU(2) module is equivalent to one of the modules U_n, $n \ge 1$, and the construction will show that each of the representations of SU(2) on U_n is faithful.

If $n = 2m+1$ is odd, then $J^2 = -\,\mathrm{Id}$ and V_n is of quaternionic type. It follows that $U_n = V_n^{\mathbb{R}}$ is irreducible as a real SU(2)-module by (ix) of Proposition 6.6 in [B- tD, p.99]. Hence U_n is of type 2 in the notation of Proposition 3.1a of [E]. In this case $\dim_{\mathbb{R}} U_n = 2 \dim_{\mathbb{C}} V_n = 4m+4 = 2n+2$. An $\mathbb{R}$-basis for U_n is given by $\mathcal{B} = \mathcal{B}^* \cup i\, \mathcal{B}^*$, where $\mathcal{B}^* = \{P_o, P_1, \dots, P_n\}$ as above, which implies that $\mathbb{Q}$-span $(\mathcal{B})$ = F-span $(\mathcal{B}^*)$. In particular we obtain cheaply the analogue of Proposition A1 in this case : if T is an element of End(U_n), then T leaves invariant $\mathbb{Q}$-span ($\mathcal{B}$) $\Leftrightarrow$ T leaves invariant F-span ($\mathcal{B}$*).

If n = 2m is even, then J^2 = Id and $V_n^{\mathbb{R}}$ is not irreducible as a real SU(2) module ; SU(2) commutes with J and hence SU(2) leaves invariant the real +1 and −1 eigenspaces of J. In this case we define U_n to be the +1 eigenspace of J in V. Note that i U_n is the −1 eigenspace of J in V since J is conjugate linear, and it follows that $V_n = U_n \oplus i\, U_n = U_n^{\mathbb{C}}$. The space U_n is irreducible as a real SU(2)-module, for if U_n were a direct sum of proper real SU(2)-submodules A_n and B_n , then V_n would be a direct sum of the proper complex SU(2)-submodules $A_n^{\mathbb{C}}$ and $B_n^{\mathbb{C}}$, contradicting the fact that V_n is irreducible. In this case $\dim_{\mathbb{R}} U_n = \dim_{\mathbb{C}} V_n = n+1$.

By Proposition 3.1a of [E] and the discussion above it follows that we have found all of the irreducible real representations of SU(2) in the sequence $\{U_n, n \geq 1\}$.

Natural bases for the irreducible real SU(2)-modules

We construct bases $\mathcal{B}_n$ for the irreducible SU(2) modules U_n, n ≥1 such that $\mathbb{Q}$-span ($\mathcal{B}_n$) is left invariant by the natural real Chevalley basis $\mathcal{C}_o$ for *su*(2), where $\mathcal{C}_o$ = $\{Z_1, Z_2, Z_3\}$ with $Z_1 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $Z_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $Z_3 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

Case 1 n is odd $\Rightarrow \dim_{\mathbb{R}} U_n = 2n+2$.

If $\mathcal{B}_n^* = \{P_o, P_1, \ldots, P_n\}$, then let $\mathcal{B}_n = \{u_o, u_1, \ldots, u_{2n+1}\}$, where $u_{2k} = P_k$ and $u_{2k+1} = i\, P_k$ for $0 \leq k \leq n$. In particular, $\mathcal{B}_n = \mathcal{B}_n^* + i\, \mathcal{B}_n^*$ and $\mathbb{Q}$-span ($\mathcal{B}_n$) = F-span ($\mathcal{B}_n$*).

Case 2 n = 2m is even $\Rightarrow \dim_{\mathbb{R}} U_n = n+1$.

If P is any element of V_n in the case n = 2m, then P+J (P) = (Id + J)(P) is an element of U_n, the +1 eigenspace of J. To obtain an $\mathbb{R}$-basis $\mathcal{B}_n$ of U_n from the $\mathbb{C}$-basis

$\mathcal{B}_n^* = \{P_o, P_1, \ldots, P_n\}$ of V_n we consider separately the cases a) $m = 2p \Rightarrow n = 4p$ and b) $m = 2p+1 \Rightarrow n = 4p+2$.

a) Since $n = 4p$ we observe that $i^n = 1$ and hence $J(P_k) = (-1)^{n-k} P_{n-k}$ for $0 \le k \le n$ by 3) above. In particular we obtain

(i) J leaves invariant $\mathbb{Z}$-span ($\mathcal{B}_n^*$).

The basis $\mathcal{B}_n^*$ is also an illustration of Proposition 3.2e of [E].

Next, we define

$u_{2k} = (Id+J)(P_k) = P_k + (-1)^{n-k} P_{n-k}$ for $0 \le k \le m-1 = (n/2)-1$.

$u_{2k+1} = (Id+J)(i P_k) = i \{P_k + (-1)^{n-k+1} P_{n-k}\}$ for $0 \le k \le m-1 = (n/2)-1$.

$u_n = P_m = P_{n/2}$

If $\mathcal{B}_n = \{u_r : 0 \le r \le n\}$, then $\mathcal{B}_n$ is an $\mathbb{R}$-basis of U_n ; $|\mathcal{B}_n| = \dim_{\mathbb{R}} U_n = n+1$ and the elements of $\mathcal{B}_n$ are linearly independent over $\mathbb{R}$ since $\mathcal{B}_n^* = \{P_o, P_1, \ldots, P_n\}$ is a $\mathbb{C}$-basis of V_n. From the definitions of the elements $\{u_r : 0 \le r \le n\}$ we obtain immediately

$u_{2k} + i\, u_{2k+1} = (-1)^{n-k}\, 2 P_{n-k}$ for $0 \le k \le m-1$

$u_{2k} - i\, u_{2k+1} = 2 P_k$ for $0 \le k \le m-1$

$u_n = P_m = P_{n/2}$

From these relations we see immediately that $\{Re(\mathcal{B}_n^*), Im(\mathcal{B}_n^*)\} \subseteq \mathbb{Q}$-span ($\mathcal{B}_n$) and $\mathcal{B}_n \subseteq \mathbb{Q}$-span $\{Re(\mathcal{B}_n^*), Im(\mathcal{B}_n^*)\}$. This proves

(ii) $\mathbb{Q}$-span ($\mathcal{B}_n$) = $\mathbb{Q}$-span $\{Re(\mathcal{B}_n^*), Im(\mathcal{B}_n^*)\}$

Hence by (i) and (ii) the bases $\mathcal{B}_n$ for U_n and $\mathcal{B}_n^*$ for V_n satisfy the hypotheses of Proposition A1 above.

b) Since $n = 2m$ and $m = 2p+1$ it follows that $i^n = -1$ and hence $J(P_k) = (-1)^{n-k+1} P_{n-k}$ for $0 \le k \le n$ by 3) above. In particular we obtain

(i) J leaves invariant $\mathbb{Z}$-span ($\mathcal{B}_n^*$).

Next we define

$u_{2k} = (Id+J)\,(P_k) = P_k + (-1)^{n-k+1} P_{n-k}$ for $0 \le k \le m-1 = (n/2)-1$.

$u_{2k+1} = (Id+J)\,(i\,P_k) = i\,\{P_k + (-1)^{n-k} P_{n-k}\}$ for $0 \le k \le m-1 = (n/2)-1$.

$u_n = P_m = P_{n/2}$

As above in case a), the set $\mathcal{B}_n = \{u_r : 0 \le r \le n\}$ is an $\mathbb{R}$-basis of U_n, and from the definitions we obtain

$u_{2k} + i\,u_{2k+1} = (-1)^{n-k+1}\, 2\, P_{n-k}$ for $0 \le k \le m-1$

$u_{2k} - i\,u_{2k+1} = 2\, P_k$ for $0 \le k \le m-1$

$u_n = P_m = P_{n/2}$

The argument from case a) also shows here that

(ii) $\mathbb{Q}$-span $(\mathcal{B}_n) = \mathbb{Q}$-span $\{\mathrm{Re}\,(\mathcal{B}_n{}^*),\ \mathrm{Im}\,(\mathcal{B}_n{}^*)\}$

Hence by (i) and (ii) the bases $\mathcal{B}_n$ for U_n and $\mathcal{B}_n{}^*$ for V_n satisfy the hypotheses of Proposition A1 above.

The natural real Chevalley basis $\mathfrak{C}_o$ for $\mathfrak{G}_o = \mathfrak{su}\,(2)$

We fix a particular real Chevalley basis $\mathcal{C}_o = \{Z_1, Z_2, Z_3\}$ for $\mathfrak{G}_o = su\,(2)$,where $Z_1 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $Z_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $Z_3 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$. If $\mathcal{C} = \{\xi_1, \xi_2, \xi_3\}$, where $\xi_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $\xi_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\xi_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, then $\mathcal{C}$ is a Chevalley basis for $\mathfrak{G}_o{}^{\mathbb{C}} = s\ell(2, \mathbb{C})$ and induces $\mathcal{C}_o$ in the standard way described in section 1.5 of [E] since $Z_1 = i\,\xi_1$, $Z_2 = \xi_2 - \xi_3$ and $Z_3 = i\,\xi_2 + i\,\xi_3$.

To calculate the groups $G_{o,\mathcal{B},\mathbb{Q}}$, where $G_{o,\mathcal{B},\mathbb{Q}} = \{g \in G_o : \rho(g)$ leaves invariant $\mathbb{Q}$-span $(\mathcal{B})\}$, we will apply 1) of Theorem C. In order to apply this result to the bases $\mathcal{B} = \mathcal{B}_n$ for U_n we need the next result.

Lemma

The real Chevalley basis $\mathcal{C}_o$ leaves invariant $\mathbb{Q}$-span $(\mathcal{B}_n)$ for every integer $n \ge 1$.

Proof

By Corollary 1 of Proposition A1, $\mathfrak{C}_o$ leaves invariant $\mathbb{Q}$-span ($\mathfrak{B}_n$) $\Leftrightarrow$ $\mathfrak{C}$ = $\{\xi_1, \xi_2, \xi_3\}$ leaves invariant F-span ($\mathfrak{B}_n{}^*$). For Z $\in$ $su(2)$ we may calculate the action of Z on V_n by calculating the action of $e^{tZ} \subseteq SU(2)$ on V_n as defined above and then differentiating at t = 0. We obtain

$$Z_1(P_k) = (2k-n)\, i\, P_k \qquad 0 \le k \le n$$

$$Z_2(P_k) = -\,k\, P_{k-1} + (n-k)\, P_{k+1} \qquad 0 \le k \le n$$

$$Z_3(P_k) = k\, i\, P_{k-1} + (n-k)\, i\, P_{k+1} \qquad 0 \le k \le n$$

Since $\xi_1 = -\,i\, Z_1$, $\xi_2 = (1/2)\,(Z_2 - i\, Z_3)$ and $\xi_3 = -\,(1/2)\,(Z_2 + i\, Z_3)$ we obtain

$$\xi_1(P_k) = (2k-n)\, P_k \qquad 0 \le k \le n$$

$$\xi_2(P_k) = (n-k)\, P_{k+1} \qquad 0 \le k \le n$$

$$\xi_3(P_k) = k\, P_{k-1} \qquad 0 \le k \le n$$

The proof of the lemma is complete. □

$G_{o,\mathfrak{B},\mathbb{Q}}$ and $G_{o,\mathbb{Q}}$ for the real irreducible SU(2) representations

We fix the real Chevalley basis $\mathfrak{C}_o$ and the corresponding notation defined above for the rest of the discussion in this appendix. We are now ready to describe the groups $G_{o,\mathfrak{B},\mathbb{Q}}$ and $G_{o,\mathbb{Q}}$ for the real irreducible representations of G_o = SU(2). We recall the notation F = $\mathbb{Q}(i) = \{a + i\, b : a \in \mathbb{Q}$ and $b \in \mathbb{Q}\}$.

Proposition A2

For G_o = SU(2) define $G_{o,\mathbb{Q}} = \{g \in G_o :$ Ad(g) leaves invariant $\mathbb{Q}$-span -$\mathfrak{C}_o\}$. Then $G_{o,\mathbb{Q}} = \{g \in SU(2)$: there exists $\lambda \neq 0$ in $\mathbb{C}$ such that $\lambda^2 \in F$ and $\lambda g \in GL(2,F)\}$.

Remark : The adjoint representation Ad : $G_o \to GL(\mathfrak{G}_o)$ is irreducible since any subspace of $\mathfrak{G}_o$ invariant under Ad(G_o) would be an ideal of $\mathfrak{G}_o$, and $\mathfrak{G}_o = su(2)$ is a simple 3-dimensional real Lie algebra. From the discussion and terminology above, in which all real and complex representations of SU(2) were described, it follows from dimension considerations that the adjoint representation must be U_2.

Proposition A3

For G = SU(2) let $\{U_n : 1 \le n < \infty\}$ be the real irreducible representations of G up to equivalence, as defined above, where dim U_n = n+1 if n is even and dim U_n = 2n+2 if n is odd. Let $\mathcal{B}$ be a basis for U_n such that $\mathcal{C}_o = \{Z_1, Z_2, Z_3\}$ leaves invariant $\mathbb{Q}$-span ($\mathcal{B}$). Let $G_{o,\mathcal{B},\mathbb{Q}} = \{g \in SU(2) : g$ leaves invariant $\mathbb{Q}$-span $(\mathcal{B})\}$. Then

1) If n is odd, then $G_{o,\mathcal{B},\mathbb{Q}} = SU(2) \cap GL(2,F)$, where $F = \mathbb{Q}(i)$.

2) If n is even, then $G_{o,\mathcal{B},\mathbb{Q}} = G_{o,\mathbb{Q}}$.

As a consequence of the previous two results we will obtain the following

Corollary

If G = SU(2), then for U_n and $\mathcal{B}$ as above we have

1) If n is even, then $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}} = \{1\}$

2) If n is odd, then $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}}$ is isomorphic to A / F*, where F* denotes the multiplicative group of nonzero elements of F and $A = \{\lambda \in \mathbb{C} : \lambda^2 \in F^*$ and $|\lambda^2| \in \mathbb{Q}\}$. In particular, $G_{o,\mathbb{Q}} / G_{o,\mathcal{B},\mathbb{Q}}$ is an infinite abelian group in which each nonidentity element has order two.

Proof of the Corollary

Assertion 1) is an immediate consequence of Propositions A2 and A3. To prove 2) we need some preliminary results.

Lemma 1

1) If $\lambda = a + i\,b$ is an arbitrary nonzero element of $\mathbb{C}$, then $\lambda \in A \Leftrightarrow a^2, b^2$ and ab are elements of $\mathbb{Q}$.

2) Let λ be a nonzero element of $\mathbb{C}$ such that $\lambda^2 \in F^*$ and $\lambda g \in GL(2,F)$ for some $g \in SU(2)$. Then $\lambda \in A$.

Lemma 2

Let q be any positive rational number. Then there exist rational numbers r_1, r_2, r_3 and r_4 such that $q = \sum_{i=1}^{4} r_i^2$.

The proof of Lemma 1 follows routinely from the definitions. We prove Lemma 2, as pointed out to us by Marc Burger. Write q = a / b, where a and b are positive integers. By a theorem of Lagrange (cf. [HW, p.302]) we may choose positive integers $\{x_i, y_i : 1 \leq i \leq 4\}$ such that $a = \sum_{i=1}^{4} x_i^2$ and $b = \sum_{i=1}^{4} y_i^2$. Then $q = (\sum_{i=1}^{4} x_i^2) (\sum_{i=1}^{4} (y_i / b)^2)$. Define rational quaternions $p_1 = x_1 + i\, x_2 + j\, x_3 + k\, x_4$ and $p_2 = (y_1 / b) + i\, (y_2 / b) + j\, (y_3 / b) + k\, (y_4 / b)$. Then $p_1\, p_2 = r = r_1 + i\, r_2 + j\, r_3 + k\, r_4$ is also a rational quaternion. If $N(a) = \sum_{i=1}^{4} x_i^2$ for an arbitrary quaternion $a = a_1 + i\, a_2 + j\, a_3 + k\, a_4$, then since N is a group homomorphism of $\mathbb{H}^*$ into $\mathbb{R}^*$ we obtain $q = N(p_1)\, N(p_2) = N(p_1\, p_2) = \sum_{i=1}^{4} r_i^2$, as desired.$\square$

We now complete the proof of assertion 2) of the corollary. Define a function $T : G_{o,\mathbb{Q}} / G_{o,\mathfrak{B},\mathbb{Q}} \rightarrow A / F^*$ by $T(g\, G_{o,\mathfrak{B},\mathbb{Q}}) = \lambda F^*$, where λ is any nonzero element of $\mathbb{C}$ such that $\lambda^2 \in F^*$ and $\lambda g \in GL(2,F)$. The complex number λ is not well defined for a given element g of $G_{o,\mathbb{Q}}$, but if λ_1 and λ_2 are any two complex numbers such that $\lambda_i^2 \in F^*$ and $\lambda_i g \in GL(2,F)$ for i = 1,2, then $\lambda_2 = \lambda_1 f$ for some element f of F^*. It follows easily from Lemma 1 that T is a well defined injective homomorphism.

To see that T is surjective we apply Lemma 2. Let $\lambda \in A$ be given. By the definition of A and Lemma 2 we can find rational numbers r_1, r_2, r_3 and r_4 such that $\sum_{i=1}^{4} r_i^2 = |\lambda^2| \in \mathbb{Q}$. Define $\alpha^* = r_1 + i\, r_2$, $\beta^* = r_3 + i\, r_4$, $\alpha = \alpha^* / \lambda$ and $\beta = \beta^* / \lambda$. If $g = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}$, then it is routine to show that $\lambda g \in GL(2,F)$, and $g \in SU(2)$ since det (g) = $\alpha^2| + |\beta^2| = 1$. Hence $T(g\, G_{o,\mathfrak{B},\mathbb{Q}}) = \lambda F^*$, which completes the proof that T is surjective.$\square$

Proof of Proposition A2

By Corollary 2 to Proposition A1 we know that $G_{o,\mathbb{Q}} = \{g \in G_o : Ad(g)$ leaves invariant F-span $-\mathcal{C}\}$, where $\mathcal{C} = \{\xi_1, \xi_2, \xi_3\}$ is the Chevalley basis for $\mathfrak{G}_o^{\mathbb{C}} = \mathfrak{sl}(2,\mathbb{C})$ described. The action of Ad(g) on $\mathcal{C}$ is just conjugation by g since SU(2) is a subgroup of GL(2,$\mathbb{C}$). Hence $g \in G = SU(2)$ lies in $G_{o,\mathbb{Q}} \Leftrightarrow$

(*) $g\,\xi_i\,g^{-1} \in$ F-span $\{\xi_1, \xi_2, \xi_3\}$ for i = 1, 2, 3.

If $g \in SU(2)$, then $g = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$ some $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Requiring that the coefficients of $g\,\xi_i\,g^{-1}$ lie in F for i = 1, 2, 3 is a set of 12 conditions, which are easily seen to be equivalent to the following conditions on α and β :

(**) 1) $|\alpha|^2 - |\beta|^2 \in F$

2) $\alpha^2 \in F$ and $\beta^2 \in F$.

3) $\alpha\beta \in F$ and $\alpha\bar{\beta} \in F$.

It is easy to verify that (**) is equivalent to

(***) 1) $\alpha^2 \in F$ and $\beta^2 \in F$.

2) If $\alpha \neq 0$, then there exist numbers λ_1, λ_2 in F such that $\bar{\alpha} = \lambda_1\alpha$ and $\beta = \lambda_2\alpha$.

3) If $\beta \neq 0$, then there exist numbers μ_1, μ_2 in F such that $\bar{\beta} = \mu_1\beta$ and $\alpha = \mu_2\beta$.

Finally, it is routine to show that (***) is equivalent to the condition that there exist a nonzero number $\lambda \in \mathbb{C}$ such that $\lambda^2 \in F$ and $\lambda g \in GL(2,F)$. This completes the proof of Proposition A2.□

Proof of Proposition A3

As above we let V_n denote the (n+1)-dimensional complex vector space consisting of all homogeneous polynomials of degree n in the two complex variables z_1, z_2. Recall also the natural basis $\mathcal{B}_n^* = \{P_o, P_1, \ldots, P_n\}$, where $P_k(z_1, z_2) = z_1^k z_2^{n-k}$ for $0 \leq k \leq n$.

When computing $G_{o,\mathcal{B},\mathbb{Q}}$ = {g ∈ SU(2) : g leaves invariant $\mathbb{Q}$-span ($\mathcal{B}$)} for the irreducible real SU(2) module U_n it suffices by 1) of Theorem C to consider any basis $\mathcal{B}$ of U_n such that $\mathcal{C}_o$ leaves invariant $\mathbb{Q}$-span ($\mathcal{B}$). In the discussion above we constructed a natural basis $\mathcal{B}_n$ = {u_1, u_2, ...} of U_n satisfying this property. Moreover, the bases $\mathcal{B}_n$ for U_n and $\mathcal{B}_n$* for V_n satisfy the two hypotheses in the statement of Proposition A1. Hence for G = SU(2) acting on U_n Proposition A1 says that $G_{o,\mathcal{B},\mathbb{Q}}$ = {g ∈ SU(2) : g leaves invariant $\mathbb{Q}$-span ($\mathcal{B}_n$)} = {g ∈ SU(2) : g leaves invariant F-span ($\mathcal{B}_n$*)}

Lemma

Let $g = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$, where α, β ∈ $\mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$, be an arbitrary element of SU(2). Then $g(P_k)$ ∈ F-span {P_o, P_1, ... , P_n} for 0 ≤ k ≤ n ⇔

a) There exists a nonzero number λ ∈ $\mathbb{C}$ such that λ^2 ∈ F and λg ∈ GL(2,F).

b) α^n and β^n are elements of F.

Remark

This lemma is strikingly similar to Proposition A2. Before proving it we use it to complete the proof of Proposition A3.

Proof of Proposition A3

1) We suppose first that n is odd. Since λα is a matrix entry of λg, whose matrix entries all lie in F, it follows that $\alpha^2 = (\lambda\alpha)^2 / \lambda^2$ is an element of F by a) of the lemma. Since n = 2k+1 is odd and α^n ∈ F by b) it follows that $\alpha = \alpha^n / \alpha^{2k}$ lies in F. Similarly, β ∈ F and we conclude that $G_{o,\mathcal{B},\mathbb{Q}}$ ⊆ SU(2) ∩ GL(2,F). The reverse inclusion is obvious.

2) Next suppose that n = 2k is even. The argument in 1) shows that α^2 and β^2 are elements of F, and it follows $\alpha^n = (\alpha^2)^k$ and $\beta^n = (\beta^2)^k$ are elements of F. Hence a) ⇒ b) in the lemma if n is even, and we conclude from the lemma and Proposition A2 that

$G_{o,\mathcal{B},\mathbb{Q}} = G_{o,\mathbb{Q}}$. □

Proof of the lemma

We compute $(gP_k)(z_1, z_2) = (\alpha z_1 - \overline{\beta} z_2)^k (\beta z_1 + \overline{\alpha} z_2)^{n-k}$. In particular $(gP_n)(z_1, z_2) = (\alpha z_1 - \overline{\beta} z_2)^n = \sum_{k=o}^{n} \{(-1)^{n-k} \binom{n}{k} \alpha^k \overline{\beta}^{n-k} P_k\}$ and $(gP_0)(z_1, z_2) = (\beta z_1 + \overline{\alpha} z_2)^n = \sum_{k=o}^{n} \{\binom{n}{k} \beta^k \overline{\alpha}^{n-k} P_k\}$.

Suppose first that $g(P_k) \in$ F-span $\{P_o, P_1, \ldots, P_n\}$ for $0 \le k \le n$. In particular $g(P_n) \in$ F-span $\{P_o, P_1, \ldots, P_n\}$ and we obtain

(1) $\alpha^k \overline{\beta}^{n-k} \in F$ for $0 \le k \le n$.

For $k = n$ and $k = n-1$ this implies that $\alpha^n \in F$ and $\alpha^{n-1} \overline{\beta} \in F$. We obtain

(2) $\alpha^n \in F$ and $\overline{\beta} = \lambda_1 \alpha$ for some $\lambda_1 \in F$ if $\alpha \ne 0$.

Similarly, since $g(P_0) \in$ F-span $\{P_o, P_1, \ldots, P_n\}$ we obtain

(3) $\beta^k \overline{\alpha}^{n-k} \in F$ for $0 \le k \le n$.

(4) $\beta^n \in F$ and $\overline{\alpha} = \lambda_2 \beta$ for some $\lambda_2 \in F$ if $\beta \ne 0$.

We consider first the case that $\alpha \ne 0$. From (2) it follows that $\beta = \overline{\lambda_1}\, \overline{\alpha}$ and after plugging this into the formula for $(gP_k)(z_1, z_2)$ we obtain $(gP_k)(z_1, z_2) = \alpha^k \overline{\alpha}^{n-k} \{(z_1 - \lambda_1 z_2)^k (\overline{\lambda_1} z_1 + z_2)^{n-k}\} = \alpha^k \overline{\alpha}^{n-k} P_k^*$, where P_k^* is an element of F-span $\{P_o, P_1, \ldots, P_n\}$. Since $gP_k \in$ F-span $\{P_o, P_1, \ldots, P_n\}$ we conclude that $\alpha^k \overline{\alpha}^{n-k} \in F$ for all $0 \le k \le n$. For $k = n-1$ we see that $\alpha^{n-1}\overline{\alpha} \in F$, and by combining this with (2) we obtain

(5) $\overline{\alpha} = \lambda_3 \alpha$ for some $\lambda_3 \in F$ if $\alpha \ne 0$.

If $\beta \ne 0$, then a similar argument using (4) shows

(6) $\overline{\beta} = \lambda_4 \beta$ for some $\lambda_4 \in F$ if $\beta \ne 0$.

The assertions (2) and (5) show that if $\alpha \ne 0$, then $g = \alpha g'$, where $g' \in GL(2,F)$. Hence $1 = \det(g) = \alpha^2 \det(g')$, and we conclude that $\alpha^2 = 1 / \det(g') \in F$ if $\alpha \ne 0$. Hence if $\lambda = (1/\alpha)$, then $\lambda g \in GL(2,F)$ and $\lambda^2 \in F$. A similar argument using (4) and (6) shows that if $\beta \ne 0$ and $\lambda = (1/\beta)$, then $\lambda g \in GL(2,F)$ and $\lambda^2 \in F$. Since either α or β is nonzero the conditions a) and b) of the lemma now follow from 2) and 4) above.

Conversely suppose that conditions a) and b) of the lemma hold for an element g of SU(2). Let λ be a nonzero complex number such that $\lambda^2 \in$ F and $\lambda g \in$ GL(2,F). Note that $\lambda\alpha$ and $\lambda\beta$ are elements of F since $\lambda g = g'$ has all matrix entries in F. Hence $\lambda^n \in$ F by hypothesis b) since $\lambda^n = (\lambda\alpha)^n / \alpha^n$ if $\alpha \neq 0$ while $\lambda^n = (\lambda\beta)^n / \beta^n$ if $\beta \neq 0$. It is evident that $(g'P_k) \in$ F-span $\{P_o, P_1, \ldots, P_n\}$ for $0 \leq k \leq n$ since the matrix entries of g' lie in F , and we conclude that $(gP_k) = (1 / \lambda^n)(g'P_k) \in$ F-span $\{P_o, P_1, \ldots, P_n\}$ for $0 \leq k \leq n$. The proof of the lemma is complete, and Proposition A3 now follows as indicated above.□

References

[B-tD] T. Br cker and T. tom Dieck, Representations of Compact Lie Groups, Graduate Texts in Mathematics, Number 98, Springer, Heidelberg, 1985.

[E] P. Eberlein, " Rational approximation in compact Lie groups and their Lie algebras " , preprint 1999

[Hu] J. Humphreys, Introduction to Lie Algebras and Representation Theory, Graduate Texts in Mathematics, Number 9, Springer, Heidelberg, 1972.

[HW] G.H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, Oxford, Fifth Edition, 1979.