ANÉIS DE REPRESENTAÇÃO DE ALGUNS GRUPOS CLÁSSICOS

Nelio Baldin

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciências da Computação da Universidade Estadual de Campinas como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Antonio Conde

CAMPINAS
1975

Meus Agradecimentos

ao

Prof. Dr. ANTONIO CONDE

SUMÁRIO

O objetivo deste trabalho é apresentar, de um modo acessível, o cálculo dos anéis de representação para alguns grupos clássicos, a saber, o toro Tn, o unitário U(n), o grupo das rotações SO(n) e Spin(n).

No capítulo I introduzimos as noções de anel de representação RG e de caráter, demonstrando que dois G-módulos são isomorfos se e somente se possuem o mesmo caráter, para qualquer grupo topológico compacto G. Utilizamos a noção de integral de Haar, afim de se obter o Lema de ortogonalidade de Schur.

No capítulo II definimos os grupos Tn, U(n), SO(n) e Spin(n) e calculamos os respectivos anéis de representação.

Para isto, encontramos um toro maximal T e o respectivo grupo de Weyl para cada um dos grupos acima, uma vez que o anel de representação é subanel do anel de todos os elementos de RT invariantes pela ação do grupo de Weyl.

Demos especial ênfase ao grupo Spin(n), em vista de suas inúmeras aplicações. Sua definição e principais propriedades foram obtidas utilizando-se da álgebra de Clifford A_n, segundo o trabalho de Brauer e Weyl [2], e apresentamos a prova de que Spin(n) é grupo de revestimento para SO(n), de acordo com Chevalley [4] . O anel de representação RSpin(n) é calculado a partir do fato de que todo Spin(n)-módulo se decompõe como soma direta de um SO(n)-módulo e de um módulo a esquerda sobre a álgebra de Clifford.

ANÉIS DE REPRESENTAÇÃO DE ALGUNS GRUPOS CLÁSSICOS

- ÍNDICE -

Capítulo I

Noções Básicas sobre Anel de Representação

O objetivo deste capítulo é conceituar anel de representação e fornecer os requisitos necessários afim de calculá-lo para alguns grupos clássicos.

1. Representação de um grupo topológico G

1.1 Definição:

Um grupo topológico é uma terna $(G, \tau, *)$, onde G é um conjunto munido de uma topologia τ e $*$ é uma aplicação de GxG em G que define em G uma estrutura de grupo de tal forma que as aplicações

$$\begin{array}{ccc} G \times G \longrightarrow G & \text{e} & G \longrightarrow G \\ (x,y) \longmapsto x_* y & & x \longmapsto x^{-1} \end{array}$$

são contínuas.

Quando não houver perigo de confusão, nos referiremos ao grupo topológico $(G, \tau, *)$ como G simplesmente.

Dizemos que o grupo topológico $(G, \tau, *)$ é Hausdorff, compacto, conexo, etc., se o espaço topológico (G, τ) o for.

Dois grupos topológicos G e G' são isomorfos se existir um homeomorfismo de G sobre G' que é também isomorfismo de grupos.

Sejam G um grupo topológico compacto e M um espaço vetorial de dimensão finita sobre o corpo C dos complexos.

1.2 Definição:

Dizemos que G atua como grupo de automorfismo de M se exis -

tir uma aplicação contínua

$$. : G \times M \longrightarrow M$$
$$(g,m) \longmapsto g.m$$

com as seguintes propriedades:

para quaisquer g, g_1, g_2 em G, t_1, t_2 em C e m, m_1, m_2 em M, temos :

i) $g.(t_1m_1 + t_2m_2) = t_1g.m_1 + t_2g.m_2$,

ii) $(g_1 * g_2).m = g_1.(g_2.m)$ e

iii) $1.m = m$,

onde 1 é o elemento unidade do grupo $(G, *)$.

Uma tal aplicação contínua é denominada <u>atuação</u> de G como grupo de automorfismo de M.

Esta terminologia é justificada notando-se que uma atuação origina um homomorfismo ψ entre o grupo G e o grupo de todos os automorfismos de M, associando a cada $g \in G$ o automorfismo

$$\psi_g : M \longrightarrow M$$
$$m \longmapsto g.m \quad .$$

Salvo menção em contrário, consideraremos sempre G como grupo topológico compacto.

1.3 Definição:

Um G-módulo (sobre C) é um espaço vetorial M de dimensão finita sobre C junto com uma atuação de G como grupo de automorfismos de M. Um G-módulo é também denominado uma representação de G.

Quando não houver perigo de confusão, nos referiremos a M como G-módulo sem especificar a atuação.

1.4 Definição:

Dois G-módulos M e M' são ditos isomorfos se existir um isomorfismo de espaços vetoriais h de M sobre M' compatível com a atuação de G, ou seja, para quaisquer $g \in G$ e $m \in M$, devemos ter

$$h(g.m) = g.h(m) \quad .$$

Aqui estamos representando com a mesma notação as atuações de G em M e em M'.

Se M for isomorfo a M', escrevemos $M \cong M'$.

1.5 Definição:

Um subespaço vetorial M' de um G-módulo M é um G-submódulo de M se for um G-módulo com a atuação restrição da de M. Em outras palavras, se g.m pertencer a M', para todos $g \in G$ e $m \in M'$.

Notemos que todas as definições acima podem ser reescritas considerando-se o corpo R dos reais ao invés de C.

2. <u>Exemplos de G-módulos</u>

2.1 Consideremos o espaço vetorial C dos complexos sobre C com a atuação

$$G \times C \dashrightarrow C$$
$$(g,z) \mapsto z \quad .$$

Este G-módulo é denominado trivial. Quando nos referirmos a C como G-módulo sem especificar a atuação, estaremos subentendendo esta atuação.

2.2 O conjunto S^1 dos complexos de módulo 1 é um grupo compacto com a topologia usual induzida de C e com a multiplicação complexa .

O espaço vetorial R^2 sobre R torna-se um S^1-módulo real com a atuação

$$S^1 \times R^2 \dashrightarrow R^2$$

$$(e^{i\theta}, (x,y)) \mapsto (x\cos\theta - y\,\mathrm{sen}\theta,\ y\cos\theta + x\,\mathrm{sen}\theta)\ .$$

Geometricamente S^1 atua como o grupo das rotações em R^2 .

2.3 O G-módulo $\mathrm{Hom}_C(M,M')$

Sejam M e M' G-módulos sobre C e $\mathrm{Hom}_C(M,M')$ o espaço vetorial sobre C dos homomorfismos de espaços vetoriais de M em M' (ou seja, das aplicações lineares de M em M').

Tornamos $\mathrm{Hom}_C(M,M')$ um G-módulo complexo definindo a atuação

$$G \times \mathrm{Hom}_C(M,M') \dashrightarrow \mathrm{Hom}_C(M,M')$$

$$(g, h) \mapsto g_*h$$

onde g_*h é a aplicação linear de M em M' dada por

$$g_*h(m) = g.h(g^{-1}.m)\ ,\quad \forall\, m \in M\ .$$

Seja agora $\mathrm{Hom}_{CG}(M,M')$ o subespaço vetorial de todas as aplicações lineares h de M em M' tais que

$$h(g.m) = g.h(m)\ ,\quad \forall\, g \in G \ \text{ e } \ \forall\, m \in M.$$

Então $\mathrm{Hom}_{CG}(M,M')$ é precisamente o submódulo de $\mathrm{Hom}_C(M,M')$ das aplicações lineares invariantes pela atuação de G, ou seja, de todos os elementos h em $\mathrm{Hom}_C(M,M')$ tais que

$$g_*h = h\ ,\quad \forall\, g \in G.$$

O G-módulo M^* igual a $\mathrm{Hom}_C(M,C)$ é denominado G-módulo dual de M.

com a topologia usual induzida de C e com a multiplicação complexa .

O espaço vetorial R^2 sobre R torna-se um S^1-módulo real com a atuação

$$S^1 \times R^2 \dashrightarrow R^2$$
$$(e^{i\theta}, (x,y)) \mapsto (x\cos\theta - y\operatorname{sen}\theta,\ y\cos\theta + x\operatorname{sen}\theta) .$$

Geometricamente S^1 atua como o grupo das rotações em R^2 .

2.3 O G-módulo $Hom_C(M,M')$

Sejam M e M' G-módulos sobre C e $Hom_C(M,M')$ o espaço vetorial sobre C dos homomorfismos de espaços vetoriais de M em M' (ou seja, das aplicações lineares de M em M').

Tornamos $Hom_C(M,M')$ um G-módulo complexo definindo a atuação

$$G \times Hom_C(M,M') \dashrightarrow Hom_C(M,M')$$
$$(g, h) \mapsto g_* h$$

onde $g_* h$ é a aplicação linear de M em M' dada por

$$g_* h(m) = g.h(g^{-1}.m) \ , \ \forall\, m \in M .$$

Seja agora $Hom_{CG}(M,M')$ o subespaço vetorial de todas as aplicações lineares h de M em M' tais que

$$h(g.m) = g.h(m) \ , \ \forall\, g \in G \ \text{ e } \ \forall\, m \in M.$$

Então $Hom_{CG}(M,M')$ é precisamente o submódulo de $Hom_C(M,M')$ das aplicações lineares invariantes pela atuação de G, ou seja, de todos os elementos h em $Hom_C(M,M')$ tais que

$$g_* h = h \ , \ \forall\, g \in G.$$

O G-módulo M^* igual a $Hom_C(M,C)$ é denominado G-módulo dual de M.

$$= g.(\Sigma\, \alpha_{ij}\, h_i(g^{-1}.v)w_j) = g.(\phi(\Sigma\, \alpha_{ij}\, h_i \otimes w_j)(g^{-1}.v)) =$$
$$= g_*\phi(\Sigma\, \alpha_{ij}\, h_i \otimes w_j)(v) \quad , \quad \forall\, v \in M,$$

mostrando assim que ϕ é isomorfismo de G-módulos.

2.6 O G-módulo produto exterior

Seja M um G-módulo sobre C ou R e seja $T(M) = \sum_{k\geq 0} T_k(M)$ a álgebra tensorial de M, onde $T_0(M) = C$ ou R e $T_{k+1}(M) = T_k(M) \otimes M$, para $k \geq 0$.

Definimos a álgebra exterior de M como a álgebra graduada quociente

$$\Lambda(M) = T(M)/D(M^2),$$

onde $D(M^2)$ é o ideal de $T(M)$ gerado por todos os elementos do tipo $m \otimes m$, com m em M. A operação binária multiplicação de dois elementos $a,b \in \Lambda(M)$ é representada por $(a,b) \longmapsto a \wedge b$, e denominada produto exterior.

Temos $\Lambda^0(M) = C$ ou R, $\Lambda^1(M) = M$ e $\Lambda^k(M)$ é o espaço vetorial sobre C ou R gerado pelos produtos $m_1 \wedge \ldots \wedge m_k$ de k elementos de M. Se $\{m_1, \ldots, m_p\}$ for base para M, é fácil ver que $\{m_{i_1} \wedge \ldots \wedge m_{i_k} : 1 \leq i_1 < \ldots < i_k \leq p\}$ é base para $\Lambda^k M$.

Estudemos um pouco os espaços vetoriais reais $\Lambda^k R^n$.

Como $\Lambda^n R^n$ é gerado apenas pelo elemento $e_1 \wedge \ldots \wedge e_n$, $\Lambda^n R^n$ é isomorfo como espaço vetorial a R, através do isomorfismo canônico $\mathrm{Det}: \Lambda^n R^n \longrightarrow R$ que associa a $e_1 \wedge \ldots \wedge e_n$ a unidade $1 \in R$. Aqui $\{e_1, \ldots, e_n\}$ é a base canônica do R^n, que é ortonormal em relação ao produto interno usual. Procuremos definir em $\Lambda^k R^n$ um produto interno de forma que a base $\{e_{i_1}\wedge\ldots\wedge e_{i_k} : 1 \leq i_1 < \ldots < i_k \leq n\}$ seja ortonormal.

Consideremos para isto a matriz $k\times k$ $B = (B_{rs})$, onde $B_{rs} = \langle e_{i_r}, e_{j_s}\rangle$, $1 \leq r,s \leq k$.

Vemos que $\det B = 1$ se $e_{i_1}\wedge\ldots\wedge e_{i_k} = e_{j_1}\wedge\ldots\wedge e_{j_k}$ e $\det B = 0$ em caso contrário.

Então o produto interno desejado pode ser definido por

$$\langle x_1\wedge\ldots\wedge x_k, y_1\wedge\ldots\wedge y_k\rangle = \det(\langle x_i, y_j\rangle)_{i,j=1,\ldots,k}.$$

Notemos que, se A for uma matriz $k\times k$ ortogonal, temos

$$\langle Ax_1\wedge\ldots\wedge Ax_k, Ay_1\wedge\ldots\wedge Ay_k\rangle = \det(\langle Ax_i, Ay_j\rangle) =$$
$$= \det(\langle x_i, y_j\rangle) = \langle x_1\wedge\ldots\wedge x_k, y_1\wedge\ldots\wedge y_k\rangle \quad ,$$

o que mostra que, num certo sentido, este produto é invariante pela ação de matrizes ortogonais.

Mais detalhes sobre produto exterior podem ser encontrados em [8].

Podemos tornar o espaço vetorial $\Lambda^k(M)$ um G-módulo simplesmente definindo a atuação de G como grupo de automorfismos sobre $\Lambda^k(M)$ por

$$g.m_1\wedge\ldots\wedge m_k = g.m_1\wedge\ldots\wedge g.m_k \quad .$$

Os exemplos 2.3, 2.4, 2.5 e 2.6 permitem construir G-módulos .

Vamos agora relacionar G-módulos entre si.

2.7 Lema:

Seja M um G-módulo e suponhamos que M se decomponha como soma direta de G-módulos unidimensionais.

$$M = M_1 \oplus \ldots \oplus M_m \quad .$$

Então o G-módulo $\Lambda^k(M)$ é isomorfo ao G-módulo $\bigoplus M_{i_1}\otimes\ldots\otimes M_{i_k}$, soma direta sobre todas as k-uplas $(i_1, \ldots, i_k)$ com $1 \leq i_1 < \ldots < i_k \leq m$ dos G-módulos unidimensionais $M_{i_1} \otimes \ldots \otimes M_{i_k}$.

Prova:

O isomorfismo $\psi: \oplus M_{i_1} \otimes \ldots \otimes M_{i_k} \longrightarrow \Lambda^k(M)$ que a cada elemento $m_{i_1} \otimes \ldots \otimes m_{i_k}$ associa o elemento $m_{i_1} \wedge \ldots \wedge m_{i_k}$ de $\Lambda^k(M)$ preserva a atuação de G.

3. Anel de Representação

3.1 Integração

Como sempre, G é um grupo topológico compacto.

Seja $\mathcal{C}(G)$ o espaço vetorial sobre R das funções contínuas definidas em G com valores reais.

Denominamos <u>integral</u> em G a uma aplicação linear

$$\int: \mathcal{C}(G) \longrightarrow R$$

que a cada $f \in \mathcal{C}(G)$ associa um número real $\int f$ satisfazendo as seguintes propriedades:

i) $\int e = 1$, onde $e: G \longrightarrow R$ é dada por $e(g) = 1$, $\forall g \in G$;

ii) se $p_x: G \longrightarrow G$ e $q_x: G \longrightarrow G$ são definidas por $p_x(g) = gx$ e $q_x(g) = xg$, $\forall g \in G$, onde $x \in G$ é fixo, temos

$$\int f \circ p_x = \int f = \int f \circ q_x, \quad \forall f \in \mathcal{C}(G);$$

iii) se $f \geq 0$, $f \in \mathcal{C}(G)$, então $\int f \geq 0$ e, além disso, se f for não identicamente nula, então $\int f >$ ·

A propriedade (ii) significa que é invariante por translações a direita e a esquerda.

Pode-se construir integrais em qualquer grupo compacto, mas isto foge a nossos propósitos. Vide [10].

Se considerarmos funções contínuas f de G em C, definimos integral $\int f$ por $\int f = \int re\, f + i \int im\, f$.

Generalizando, se f for aplicação contínua de G com valores num espaço vetorial complexo (ou real) M de dimensão finita, podemos escrever

$$f(g) = f_1(g)\, e_1 + \ldots + f_m(g)\, e_m\,, \quad \forall\, g \in G,$$

onde $\{e_1, \ldots, e_m\}$ é uma base para M e as funções f_i, definidas em G com valores em C (ou R), são as funções coordenadas de f.

Definimos então integral de f por

$$\int f = (\int f_1)\, e_1 + \ldots + (\int f_m)\, e_m\ .$$

Exemplo:

Seja S^1 o grupo multiplicativo compacto dos complexos de módulo 1. Seja $r: R \dashrightarrow S^1$ dada por $r(t) = e^{2\pi i t}$, para $t \in R$, a aplicação de revestimento.

Definimos integral de uma função contínua $f: S^1 \dashrightarrow R$ por

$\int f = \int_0^1 f \circ r(t)\, dt$, onde a integral a direita é a usual em R.

3.2 Definição:

Um G-módulo M é irredutível se não possue G-submódulos distintos de $\{0\}$ e M.

3.3 Lema:

Todo G-módulo M possue um produto interno hermitiano K invariante pela atuação de G.

Prova:

Seja H um produto interno hermitiano qualquer de M. A aplicação

$$h_{m,m'}: G \dashrightarrow C$$
$$g \mapsto H(g.m,g.m')$$

é contínua para cada par m e m' em M.

Então podemos definir $K: M \times M \dashrightarrow C$ por $K(m,m') = \int h_{m,m'}$.

Utilizando-se as propriedades da integral e de H, vemos que K é produto interno hermitiano.

Mostremos que é invariante pela atuação de G.

Se $g' \in G$, temos

$$K(g'.m,g'.m') = \int h_{m,m'} \circ p_{g'} = \int h_{m,m'} = K(m,m') \quad ,$$

onde $p_{g'}$ é a translação a direita por g', obtendo-se assim o resultado desejado.

Chegamos agora a um dos resultados principais.

3.4 Teorema:

Todo G-módulo M (de dimensão finita) se decompõe como soma direta de G-submódulos irredutíveis.

Prova:

Por indução sobre a dimensão de M.

Se a dimensão de M for zero ou um, o resultado é imediato.

Suponhamos que, para qualquer natural $n > 0$, o teorema seja verdadeiro para todo natural $m < n$.

Vamos demonstrá-lo para dimensão n.

Seja M um G-módulo de dimensão n. Se M for irredutível , não há nada a demonstrar.

Podemos então supor que existe um G-submódulo S de M distinto de {0} e M.

Pelo lema 3.3, podemos dotar M de um produto interno hermitiano K invariante pela atuação de G.

Seja $T = \{v \in M;\ K(v,w) = 0,\ \forall\, w \in S\}$ o subespaço vetorial de M complementar ortogonal de S. Então T é G-submódulo de M pois para todos $g \in G$ e $v \in T$, temos $g.v \in T$, uma vez que

$$K(g.v,w) = K(g^{-1}.g.v, g^{-1}.w) = K(v, g^{-1}.w) = 0, \quad \forall\, w \in S.$$

Então M é soma direta dos G-submódulos S e T :

$$M = S \oplus T .$$

Como S e T possuem dimensões menores que n, a hipótese de indução permite decompô-los em soma direta de G-submódulos irredutíveis e portanto a afirmação do teorema é válida para M de dimensão n.

Isto completa a indução.

3.5 Contra-exemplo

O resultado de 3.4 não é válido se G não for compacto.

Consideremos R^2 como espaço vetorial real e seja V o subespaço dos vetores do tipo $(x,0) \in R^2$. Seja G o grupo de todas as matrizes reais do tipo $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, com $ac \neq 0$.

Com a atuação que a cada par

$$\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix},\ (x,y) \right) \in G \times R^2$$

associa o elemento $(ax + by, cy) \in R^2$, consideramos R^2 como G-módulo .

Então V é G-submódulo de R^2 unidimensional e nenhum outro subespaço unidimensional de R^2 é invariante sob G.

De fato, suponhamos que exista um subespaço W gerado por um elemento $(a,b) \in R^2$, não nulo, invariante sob a atuação de G.

Ora, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ pertence a G, e portanto o elemento $(a,-b)$ deve pertencer a W, o que é absurdo.

Logo R^2 é um G-módulo que não se decompõe como soma direta de G-submódulos irredutíveis.

3.6 Proposição:

Seja $\{M_i\}_{i \in I}$ uma coleção de G-módulos irredutíveis, não isomorfos entre si. Seja kM a soma direta de k cópias de M.

Se $\bigoplus_{i \in I} m_i M_i \cong \bigoplus_{i \in I} n_i M_i$, então $m_i = n_i$, para todo $i \in I$, onde $\bigoplus_{i \in I}$ indica a soma direta de todos os elementos indexados por I.

Prova:

Seja $\mathrm{Hom}_{CG}(M,M')$ o G-módulo das aplicações lineares de M em M' invariantes sob a atuação de G, como em 2.3.

Então $\mathrm{Hom}_{CG}(M_j, \bigoplus_{i \in I} m_i M_i) \cong \mathrm{Hom}_{CG}(M_j, \bigoplus_{i \in I} n_i M_i)$, para qualquer $j \in I$. Decorre que

$$\bigoplus_{i \in I} m_i \mathrm{Hom}_{CG}(M_j, M_i) \cong \bigoplus_{i \in I} n_i \mathrm{Hom}_{CG}(M_j, M_i) \quad .$$

Ora, se $i \neq j$, os G-módulos irredutíveis M_i e M_j não são isomorfos e temos $\mathrm{Hom}_{CG}(M_j, M_i) = 0$.

De fato, se $h: M_j \dashrightarrow M_i$ é uma aplicação linear tal que

$h(g.m) = g.h(m)$, para todos m em M_j e g em G, seu núcleo $\ker h$ e sua imagem $h(M_j)$ são G-submódulos, e portanto $\ker h$ é igual a $\{0\}$ ou M_j. Como M_i não é isomorfo a M_j, concluimos que $\ker h$ é igual a M_j, donde $h = 0$.

Logo para cada $j \in I$,

$$n_j \mathrm{Hom}_{CG}(M_j, M_j) \cong \bigoplus_{i \in I} n_i \mathrm{Hom}_{CG}(M_j, M_i) \cong \bigoplus_{i \in I} m_i \mathrm{Hom}_{CG}(M_j, M_i) \cong$$
$$\cong m_j \mathrm{Hom}_{CG}(M_j, M_j) \quad ,$$

donde $n_j = m_j$.

Uma consequência imediata é :

3.7 Corolário:

A decomposição de um G-módulo M em G-submódulos irredutíveis é única a menos da ordem e de isomorfismos.

Seja M um G-módulo, de dimensão n, com a atuação de G dada pelos automorfismos

$$\begin{aligned} \psi_g : M &\longrightarrow M \quad , \quad \forall\, g \in G. \\ m &\longmapsto g.m \end{aligned}$$

Seja $\{m_1, \ldots, m_n\}$ uma base para M. Então a aplicação linear $f: C^n \longrightarrow M$ que a cada elemento e_i da base canônica de C^n associa o elemento m_i de M é isomorfismo de espaços vetoriais.

Façamos G atuar sobre C^n através de $\phi_g : C^n \longrightarrow C^n$ dada por $\phi_g(z_1, \ldots, z_n) = g.(z_1, \ldots, z_n) = f^{-1} \circ \psi_g \circ f(z_1, \ldots, z_n)$, para todos $(z_1, \ldots, z_n) \in C^n$ e $g \in G$.

Como $f(g.(z_1, \ldots, z_n)) = f(f^{-1} \circ \psi_g \circ f(z_1, \ldots, z_n)) =$

$$= \psi_g \circ f(z_1, \ldots, z_n) = g.f(z_1, \ldots, z_n) \quad ,$$

concluímos que C^n com esta atuação é isomorfo como G-módulo a M.

Então a classe de isomorfismo $[M]$ de M, ou seja, a classe de todos os G-módulos isomorfos a M, tem como representante o G-módulo C^n acima descrito.

Como a coleção de todos os G-módulos C^n é um conjunto (é subconjunto de $\{C^n\} \times \mathcal{P}(G \times C^n \times C^n)$), podemos dizer que a coleção S de todas as classes de isomorfismo de G-módulos é um conjunto, por ser união de conjuntos.

As operações

$$[M] + [N] = [M \oplus N]$$
$$\text{e} \qquad [M] \cdot [N] = [M \otimes N] \quad ,$$

para todos $[M]$, $[N] \varepsilon$ S, dão a S uma estrutura de semi-anel comutativo com unidade $[C]$, onde C é o G-módulo trivial.

Queremos tornar S um anel. Para isto, procederemos como segue. Consideremos S x S com a seguinte relação de equivalência:

$$([M],[N]) \sim ([M'],[N']) \text{ see existe } [D] \varepsilon S \text{ tal que}$$
$$[M]+[N']+[D] = [M']+[N]+[D] \quad .$$

Denotemos $<[M],[N]>$ a classe de equivalência de $([M],[N])$ pertencente ao conjunto quociente $RG = S \times S / \sim$.

As operações

$$<[M],[N]> + <[M'],[N']> = <[M] + [M'],[N] + [N']>$$
$$\text{e} \qquad <[M],[N]> \cdot <[M'],[N']> = <[M].[M'] + [N].[N'],[N].[M'] + [M].[N']>$$

tornam RG um anel comutativo com unidade $<[C],[0]>$, onde o oposto de $<[M],[N]>$ é $<[N],[M]>$ e o elemento nulo é $0 = <[0],[0]>$.

Como a aplicação

$$i: S \dashrightarrow RG$$
$$[M] \dashrightarrow <[M],[0]>$$

é monomorfismo de semi-anéis com unidade, podemos considerar S como sub-semi-anel de RG, identificando-o com sua imagem por i. Vemos que os elementos de RG se escrevem então como subtração de elementos de S:

$$<[M],[N]> = [M] - [N] \quad .$$

3.8 Definição:

O anel RG é denominado anel de representação do grupo topológico compacto G.

Como todo G-módulo M é soma direta de G-submódulos irredutíveis, o anel RG é gerado pelo conjunto das classes de isomorfismo de G-módulos irredutíveis.

Seja $h: G' \dashrightarrow G$ um homomorfismo entre os grupos topológicos compactos G' e G, ou seja, h é contínua e preserva a estrutura de grupo.

Para cada G-módulo M definamos o G'-módulo M' da seguinte maneira:

M' é o espaço vetorial M com G' atuando pela regra

$g'_* m = h(g').m \ , \quad \forall\, g' \in G' \ \text{ e } \ \forall\, m \in M.$

Isto permite definir um homomorfismo de anéis $Rh: RG \dashrightarrow RG'$ associando a cada $[M]-[N]$ em RG o elemento $[M']-[N']$ em RG'.

Se G'' for outro grupo compacto e $h_1: G'' \dashrightarrow G'$ for homomorfismo de grupos topológicos, então temos $R(h \circ h_1) = Rh_1 \circ Rh$.

É claro que se $h: G \dashrightarrow G$ for a aplicação identidade, Rh será a aplicação identidade em RG.

3.9 Lema:

Se $h: G \dashrightarrow G$ for automorfismo interno de G, então $Rh:RG \dashrightarrow RG$ é a aplicação identidade.

Prova:

Como h é automorfismo interno, existe $\lambda \in G$ tal que $h(g) = \lambda g\lambda^{-1}$, para todo $g \in G$.

Se M for G-módulo, $Rh([M])$ é a classe de isomorfismo de G-módulos que admite como representante o G-módulo M' constituído do espaço vetorial M com a atuação

$$g_* m = (\lambda g\lambda^{-1}).m, \quad \forall\, g \in G, \forall\, m \in M.$$

Basta mostrar que M' é isomorfo a M.

Seja $f: M' \dashrightarrow M$ dada por $f(m) = \lambda^{-1}.m$, para todo $m \in M$. Então f é automorfismo do espaço vetorial M e para quaisquer $g \in G$ e $m \in M$, temos

$$f(g_* m) = f((\lambda g\lambda^{-1}).m) = \lambda^{-1}((\lambda g\lambda^{-1}).m) = (\lambda^{-1}\lambda g\lambda^{-1}).m =$$
$$= (g\lambda^{-1}).m = g.(\lambda^{-1}.m) = g.f(m) ,$$

e portanto f é isomorfismo de G-módulos.

Vamos agora estudar a importante noção de caráter de um G-módulo M.

Poderemos então mostrar que o grupo abeliano RG é gerado livremente pelas classes de G-módulos irredutíveis e determinar se dois G-módulos são isomorfos.

Sabemos que, em qualquer G-módulo M, as aplicações

$$\psi_g : M \longrightarrow M$$
$$m \longmapsto g.m$$

são automorfismos de M e denotaremos por $tr\psi_g$ o traço de ψ_g, ou seja, a soma dos elementos diagonais da matriz representante de ψ_g em relação a uma base de M.

É fácil mostrar que o traço de um operador independe da escolha da base.

3.10 Definição:

O caráter de M é a aplicação contínua $\chi_M : G \longrightarrow C$ que a cada $g \in G$ associa o número complexo $tr\psi_g$.

A continuidade de χ_M decorre da continuidade da atuação.

Para $g, g' \in G$, temos:

$$\chi_M(g'gg'^{-1}) = tr\psi_{g'gg'^{-1}} = tr(\psi_{g'} \circ \psi_g \circ \psi_{g'}^{-1}) = tr\psi_g \quad ,$$

já que matrizes semelhantes apresentam o mesmo traço.

Mostramos então a identidade

$$\chi_M(g'gg'^{-1}) = \chi_M(g) \quad , \quad \forall\, g, g' \in G.$$

É fácil mostrar as igualdades:

$$\chi_{M \oplus N} = \chi_M + \chi_N \quad ,$$
$$\chi_{M \otimes N} = \chi_M \cdot \chi_N \quad .$$

3.11 Lema:

Sejam M um G-módulo e $\psi : G \longrightarrow Hom_C(M,M)$ a aplicação contínua que a cada $g \in G$ associa o automorfismo

$$\psi_g : M \longrightarrow M$$
$$m \longmapsto g.m \quad .$$

Então a aplicação $I = \int\psi \in Hom_C(M,M)$ é uma projeção, isto é, $I \circ I = I$, e a imagem $I(M)$ é o subespaço M_G de todos os elementos de M invariantes pela atuação de G.

Prova:

Para qualquer $m \in M$, consideremos a aplicação linear

$$\begin{aligned} \theta_m: Hom_C(M,M) &\dashrightarrow M \\ h &\mapsto h(m) \quad . \end{aligned}$$

Então $I(m) = \theta_m(I) = \theta_m(\int\psi) = \int\theta_m \circ \psi$, pois θ_m é linear. Logo $I(M) \subset M_G$ pois se $g' \in G$, temos

$$g'.I(m) = g'.\int\theta_m \circ \psi = \int g'.(\theta_m \circ \psi) \quad \text{(pois } g' \text{ atua linearmente)},$$

e como

$$g'.(\theta_m \circ \psi)(g) = g'.(g.m) = (g'g).m \ ,$$

concluímos que

$$g'.I(m) = I(m) \ ,$$

desde que a integral é invariante por translações.

A restrição $I|M_G$ de I a M_G é a identidade em M_G pois se $m \in M_G$, temos

$$I(m) = \int\theta_m \circ \psi = \int m = m \ ,$$

desde que

$$\theta_m \circ \psi(g) = \theta_m(\psi_g) = g.m = m \quad .$$

Concluímos que $I(M) = M_G$ e $I \circ I = I$, como queríamos.

Este lema mantém a validade se substituirmos C por R.

3.12 Proposição:

Seja M um G-módulo. Então

$$\int \chi_M = \dim M_G \quad ,$$

onde M_G é o subespaço dos elementos de M invariantes pela atuação de G.

Prova:

A função traço tr é linear e portanto

$$\int \chi_M = \int tr\ \psi = tr \int \psi = tr\ I \ .$$

Pelo lema 3.11, I é projeção e $I(M) = M_G$. Temos então

$$M = M_G \oplus \ker I$$

e podemos encontrar uma base $\{m_1, \ldots, m_r, m_{r+1}, \ldots, m_n\}$ para M de tal forma que os primeiros r elementos formem uma base para M_G e os demais uma para $\ker I$.

Então a matriz de I em relação a esta base é diagonal com os r primeiros elementos iguais a 1 e os demais nulos.

Logo $\int \chi_M = tr\ I = \dim M_G$, como queríamos.

3.13. Teorema:

Se M e M' são G-módulos isomorfos, então $\chi_M = \chi_{M'}$.

Prova:

Sejam $\psi: G \dashrightarrow Hom_C(M,M)$ e $\theta: G \dashrightarrow Hom_C(M',M')$ as atuações de G como grupo de automorfismos de M e M', respectivamente.

Seja $f: M \dashrightarrow M'$ um isomorfismo de G-módulos. Então

$$f^{-1} \circ \theta_g \circ f = \psi_g \quad ,$$

donde concluimos que

$$\chi_M(g) = tr\ \psi_g = tr(f^{-1} \circ \theta_g \circ f) = tr\ \theta_g = \chi_{M'}(g) \quad ,$$

para qualquer $g \in G$, uma vez que matrizes semelhantes possuem o mesmo traço. Logo $\chi_M = \chi_{M'}$, como queríamos.

Este teorema mostra que a cada classe de isomorfismo de G-módulos corresponde um caráter bem definido.

3.14 Lema da Ortogonalidade de Schur :

Se M e M' são G-módulos irredutíveis sobre C, então $\int \chi_M \overline{\chi_{M'}}$ é igual a 1 se M e M' são isomorfos e a 0 caso contrário.

Prova:

Mostremos inicialmente que $\overline{\chi_{M'}}$ é igual a $\chi_{M'^*}$. Para isto definamos um novo espaço vetorial $\overline{M'}$, a partir de M', mantendo a estrutura aditiva mas tomando para produto por escalar o conjugado do anterior, isto é, definimos um novo produto por escalar:

$$C \times M' \dashrightarrow M'$$
$$(z,m) \longmapsto \overline{z}\, m \ .$$

Então podemos considerar $\overline{M'}$ como G-módulo com a mesma atuação que M'. Segue-se que $\chi_{\overline{M'}} = \overline{\chi}_{M'}$.

Seja K um produto interno hermitiano em M' invariante pela atuação de G.

A aplicação $\alpha\colon \overline{M'} \dashrightarrow M'^*$ que a cada $v \in \overline{M'}$ associa a aplicação

$$\alpha_v\colon M' \dashrightarrow C$$
$$w \longmapsto K(w,v)$$

é isomorfismo de G-módulos. Mostremos apenas que preserva a atuação:

$$\alpha(g.v)(w) = K(w,g.v) = K(g.g^{-1}.w,g.v) = K(g^{-1}.w,v) = \alpha_v(g^{-1}.w)$$
$$= g.\alpha(v)(w) \quad ,$$

como queríamos.

Pelo teorema 3.13, temos $\chi_{\overline{M'}} = \chi_{M'^*}$, donde $\overline{\chi}_{M'} = \chi_{M'^*}$.

Logo

$$\int \chi_M \overline{\chi}_{M'} = \int \chi_M \chi_{M'^*} = \int \chi_{M'^* \otimes M} = \int \chi_{\mathrm{Hom}_C(M',M)} = \dim \mathrm{Hom}_{CG}(M',M),$$

pelas observações em 2.5 e 3.12.

Resta mostrar que $\dim \mathrm{Hom}_{CG}(M',M)$ é zero se M' não é isomorfo a M e 1 em caso contrário.

A primeira asserção já foi demonstrada na proposição 3.6 .

Mostremos a segunda.

Consideremos M isomorfo a M'. Então $\mathrm{Hom}_{CG}(M',M)$ é isomorfo a $\mathrm{Hom}_{CG}(M,M)$.

Seja $h \in \mathrm{Hom}_{CG}(M,M)$ arbitrário. Como M é espaço vetorial complexo, existe $\lambda \in C$ tal que $\ker(h-\lambda I)$, o submódulo dos auto-vetores de h, é não nulo, onde I é o operador identidade de M.

Como M é irredutível, temos $\ker(h-\lambda I) = M$, donde $h = \lambda I$.

Logo $\dim \mathrm{Hom}_{CG}(M,M) = 1$, terminando a demonstração.

3.15 Corolário:

O conjunto das classes de isomorfismo dos G-módulos irredutíveis gera livremente o grupo abeliano RG.

Prova:

Por 3.8, o conjunto de todas as classes de isomorfismo de G-módulos irredutíveis gera o grupo abeliano RG.

Se a combinação linear $\Sigma a_i [M_i]$ de classes de isomorfismo de G-módulos irredutíveis não isomorfos, com coeficientes inteiros, for nula, temos

$$\Sigma a_i \chi_{M_i} = 0 \quad ,$$

donde $\quad a_j = \int a_j \chi_{M_j} \overline{\chi}_{M_j} = \int \Sigma a_i \chi_{M_i} \overline{\chi}_{M_j} = \int (\Sigma a_i \chi_{M_i}) \overline{\chi}_{M_j} = 0 \ , \quad \forall j \ .$

Isto mostra o corolário.

Um raciocínio semelhante ao da prova de 3.15 mostra que o número de vezes que cada classe de isomorfismo de G-módulo comparece na decomposição de um G-módulo M só depende dos caracteres da classe e de M.

Vamos agora demonstrar a recíproca de 3.13.

3.16 Teorema:

Se dois G-módulos M e M' possuem o mesmo caráter então são isomorfos.

Temos portanto um método para determinar isomorfismos entre G módulos.

Prova:

Suponhamos $\chi_M = \chi_{M'}$. O número de vezes que cada classe de isomorfismo $[M_i]$ de G- módulos irredutíveis aparece na decomposição de M só depende de χ_M e de χ_{M_i} e portanto é o mesmo que na decomposição de M'.

Logo M e M' possuem a mesma decomposição em G-módulos irredutíveis (a menos de isomorfismos e da ordem), sendo portanto isomorfos.

Vamos agora enunciar um dos resultados mais úteis para o cálculo de anéis de representação.

3.17 Teorema:

Seja $h: G' \longrightarrow G$ um homomorfismo de grupos tal que cada clas se de conjugação em G intersecciona a imagem $h(G')$. Então $Rh: RG \dashrightarrow RG'$ tem núcleo nulo, e podemos considerar RG como subanel de RG'.

Prova:

Consideremos dois G-módulos M_1 e M_2. Se os G'-módulos correspondentes através de Rh M_1' e M_2' forem isomorfos, vamos provar que M_1 e M_2 também o são.

Lembremos que, para $i = 1, 2$, M_i' é o espaço vetorial M_i com a atuação de G' dada por

$$g' {}_* m = h(g').m \ , \quad \forall\, g' \in G' \ \text{ e } \ \forall\, m \in M_i \ ,$$

onde a atuação a direita é a de M_i.

Então os caracteres de M_1' e M_2' são $\chi_{M_1} \circ h$ e $\chi_{M_2} \circ h$, respectivamente.

Se $M_1' \cong M_2'$, temos $\chi_{M_1} \circ h = \chi_{M_2} \circ h$, donde χ_{M_1} e χ_{M_2} coincidem na imagem $h(G') \subset G$.

Como cada classe de conjugação em G intersecciona $h(G')$ e a função caráter de qualquer G-módulo é constante em cada classe de conjugação em G, concluimos que $\chi_{M_1} = \chi_{M_2}$ e portanto $M_1 \cong M_2$.

Mostremos agora que Rh tem núcleo zero.

Se $Rh([M_1] - [M_2]) = 0$, temos $[M_1'] - [M_2'] = 0$, donde $M_1' \cong M_2'$.

O argumento acima mostra que $M_1 \cong M_2$, e portanto $\ker Rh = \{0\}$, completando a prova.

Capítulo II

Cálculo do anel de representação RG para alguns grupos clássicos

O objetivo deste capítulo é encontrar os anéis de representação de alguns grupos de Lie familiares, dando especial ênfase ao grupo Spin.

1. O grupo toro Tn

Consideremos o grupo abeliano aditivo das n-uplas reais R^n e o subgrupo $2\pi Z^n$ de R^n constituido por aquelas cujas coordenadas são múltiplos inteiros de 2π.

1.1 Definição:

O toro n-dimensional Tn é o grupo abeliano quociente de R^n por $2\pi Z^n$:

$$Tn = R^n/2\pi Z^n \quad .$$

Cada elemento de Tn é uma classe de equivalência $[(\theta_1,\ldots,\theta_n)]$ de todas as n-uplas reais $(\phi_1,\ldots,\phi_n)$ com $\phi_i = \theta_i + 2k_i\pi$, com k_i inteiro, para $i = 1,\ldots,n$.

A topologia quociente, coinduzida pela projeção canônica

$$p: \quad R^n \longrightarrow Tn$$
$$(x_1,\ldots,x_n) \longmapsto [(x_1,\ldots,x_n)]$$

torna Tn um grupo topológico.

Como $[0,2\pi]^n = [0,2\pi]\times \ldots \times[0,2\pi]$, o produto cartesiano de n-cópias do intervalo fechado $[0,2\pi]$, é compacto em R^n, e Tn é a imagem de $[0,2\pi]^n$ pela função contínua p, concluimos que Tn é compacto.

Um dos Tn-módulos mais importantes é o espaço vetorial complexo unidimensional C com a atuação de Tn dada pela regra

$$[(\theta_1,\ldots,\theta_n)].m = e^{ik_1\theta_1+\ldots+ik_n\theta_n}\, m\,,$$

para quaisquer $[(\theta_1,\ldots,\theta_n)] \in Tn$ e $m \in C$, onde $k_1,\ldots,k_n$ são inteiros fixos.

Denotaremos por $C(k_1,\ldots,k_n)$ este Tn-módulo. Certamente é irredutível por ser unidimensional.

Vamos mostrar que estes são essencialmente os únicos Tn-módulos irredutíveis.

Seja S^1 o grupo topológico abeliano multiplicativo dos complexos de módulo 1, com a topologia induzida de C.

1.2. Lema:

Todo homomorfismo contínuo $\alpha: Tn \dashrightarrow S^1$ se escreve como

$$\alpha([(\theta_1,\ldots,\theta_n)]) = e^{ik_1\theta_1+\ldots+ik_n\theta_n}\,,$$

para certos inteiros $k_1,\ldots,k_n$.

Prova:

Iniciamos com $n = 1$.

Seja $\alpha: T_1 \dashrightarrow S^1$ um homomorfismo contínuo não trivial (caso contrário é evidente). Seja $p: R \dashrightarrow T_1$ a projeção canônica. Para qualquer inteiro k, $2k\pi$ pertence ao núcleo do homomorfismo de grupos $\alpha \circ p$.

Seja x_0 o menor real positivo pertencente a $\ker(\alpha\circ p)$.

Se tal número não existir, qualquer vizinhança aberta de zero em R contém um elemento não nulo de $\ker(\alpha\circ p)$. Seja $x \in R$ arbitrário. Para qualquer inteiro positivo n, existe y_n não nulo em $(-1/n, 1/n)$ pertencente ao núcleo de $\alpha\circ p$ tal que $z_n = my_n \in (x-1/n, x+1/n)$, para algum inteiro m. Como a sequência (z_n) converge para x e está contida no núcleo de $\alpha\circ p$, concluimos que $\alpha\circ p(x) = 1$, e portanto $\alpha\circ p$ é trivial, uma contradição.

Temos então $\alpha\circ p(x_0) = e^{i2\pi}$. Como $\alpha\circ p(1/2\ x_0)$ é raiz quadrada de 1, temos $\alpha\circ p(1/2\ x_0) = -1 = e^{i2\pi/2}$.

Devido a definição de x_0 , $\alpha\circ p$ restrito a $[0,x_0)$ é injetor. Como α é contínuo, acontece apenas uma das duas afirmações:

(1) $\forall t_1, t_2$, $0\leq t_1<t_2<x_0$, temos $\mathrm{Arg}\ \alpha\circ p(t_1) < \mathrm{Arg}\ \alpha\circ p(t_2)$

ou (2) $\forall t_1, t_2$, $0\leq t_1<t_2<x_0$, temos $\mathrm{Arg}\ \alpha\circ p(t_1) > \mathrm{Arg}\ \alpha\circ p(t_2)$,

onde $\mathrm{Arg}\ z$ representa o argumento principal do complexo z .

Suponhamos que aconteça (1).

Utilizando indução sobre n, podemos mostrar que

$$\alpha\circ p(1/2^n\ x_0) = e^{i2\pi\ 1/2^n} \quad ,$$

para qualquer n natural.

Logo $\alpha\circ p(m/2^n\ x_0) = e^{i2\pi m/2^n}$, para qualquer inteiro m.

Os números da forma $m/2^n$, com m e n inteiros, são densos em R e, por continuidade, concluimos que

$$\alpha\circ p(x\ x_0) = e^{i2\pi x}, \text{ para todo } x \in R.$$

Então $\alpha\circ p(x) = \alpha\circ p(x/x_0\ \ x_0) = e^{i2\pi/x_0\ x}$, para todo x real. Em particular $\alpha\circ p(2\pi) = e^{i2\pi\ /x_0\ 2\pi} = 1$, donde $k = 2\pi/x_0$ é inteiro. Portanto $\alpha([x]) = e^{ikx}$, para todo $[x] \in T_1$.

Se acontecer (2), por raciocínio similar, obtemos

$$\alpha\circ p(x\ x_0) = e^{-i2\pi x} ,$$

donde $k = -2\pi/x_0$ é inteiro.

No caso de α ser homomorfismo contínuo de Tn em S^1, definamos o homomorfismo contínuo $j_i: T_1 \dashrightarrow Tn$ por $j_i([t])=[(0,\ldots,0,t,0,\ldots,0)]$ onde o t aparece na i-ésima posição, para cada $i = 1,\ldots,n$.

Então $\alpha([(t_1,\ldots,t_n)]) = \alpha\circ j_1([t_1])\,.\;\ldots\;.\,\alpha\circ j_n([t_n]) = e^{ik_1t_1}\,.\;\ldots\;.\,e^{ik_nt_n}$, para $k_1,\ldots,k_n$ inteiros, pelo resultado acima.

Isto demonstra o lema.

1.3 Proposição:

Cada Tn-módulo irredutível é isomorfo a um único $C(k_1,\ldots,k_n)$. O produto $C(k_1,\ldots,k_n) \otimes C(f_1,\ldots,f_n)$ é isomorfo a $C(k_1+f_1,\ldots,k_n+f_n)$.

Prova:

Seja M um Tn-módulo irredutível sobre C.

Para cada $g\varepsilon Tn$, seja ψ_g o operador linear sobre M que associa a cada $m\,\varepsilon M$ o elemento $g.m\,\varepsilon M$.

Como C é algebricamente fechado, existe $\alpha_g\,\varepsilon C$, autovalor de ψ_g, tal que o subespaço vetorial $V = \ker(\psi_g-\alpha_g I)$ dos autovetores de ψ_g é não nulo.

Para qualquer $g'\,\varepsilon\,Tn$ e qualquer $m\,\varepsilon\,V$, temos

$$\psi_g(g'.m) = g.(g'.m) = (g.g').m = g'.(g.m) = $$
$$= g'.(\alpha_g m) = \alpha_g(g'.m)\ ,$$

pois Tn é abeliano, mostrando que V é submódulo de M.

Como M é irredutível, M é igual a V e ψ_g é igual a $\alpha_g I$, onde I é o operador identidade de M.

Se g_1 e g_2 forem elementos de Tn, vemos que $\psi_{g_1g_2} = \alpha_{g_1g_2}I$.

Seja K um produto interno hermitiano em M invariante pela atuação de Tn.

Para qualquer $m \in M$ não nulo, temos

$$K(m,m) = K(g.m,g.m) = K(\alpha_g m,\alpha_g m) = |\alpha_g|^2 K(m,m) \quad ,$$

donde $|\alpha_g| = 1$, para qualquer $g \in Tn$.

Então podemos definir o homomorfismo de grupos $\alpha: Tn \dashrightarrow S^1$ que a cada $g \in Tn$ associa o número complexo $\alpha_g \in S^1$. Como a atuação de Tn sobre M é contínua, também α o é.

Pelo lema 1.2, existem inteiros $k_1, \ldots, k_n$ tais que

$$\alpha([(\theta_1,\ldots,\theta_n)]) = e^{ik_1\theta_1+\ldots+ik_n\theta_n} \quad ,$$

para qualquer $[(\theta_1,\ldots,\theta_n)] \in Tn$.

Então temos

$$[(\theta_1,\ldots,\theta_n)].m = e^{ik_1\theta_1+\ldots+ik_n\theta_n}\, m, \quad \forall\, m \in M.$$

Mostremos que M é unidimensional.

Seja $m \in M$ um elemento não nulo. O subespaço vetorial gerado por m é um Tn-submódulo de M pois

$$g.(zm) = \alpha_g zm, \quad \forall\, g \in Tn \ \text{ e } \ \forall\, z \in C.$$

Como M é irredutível, temos M igual ao subespaço gerado por m, e portanto é unidimensional.

É imediato então que M é isomorfo como Tn-módulo a um único $C(k_1,\ldots,k_n)$. Isto pode ser visto calculando-se os caracteres.

A segunda parte da proposição é evidente, lembrando que a atuação de um grupo G sobre o produto tensorial é dada pela relação

$$g.(m \otimes m') = g.m \otimes g.m' \ .$$

Isto completa a prova da proposição.

Observação:

Na verdade, qualquer G-módulo irredutível, onde G é um grupo topológico abeliano compacto, é unidimensional. A prova é análoga.

Os geradores livres de RTn são portanto as classes $[C(k_1,\ldots,k_n)]$, representadas por $\alpha_1^{k_1}\ldots\alpha_n^{k_n}$.

Como $(\alpha_1^{k_1}\ldots\alpha_n^{k_n}).(\alpha_1^{f_1}\ldots\alpha_n^{f_n}) = [C(k_1,\ldots,k_n)].[C(f_1,\ldots,f_n)]$
$= [C(k_1+f_1,\ldots,k_n+f_n)] = \alpha_1^{k_1+f_1}.\ \ldots\ .\alpha_n^{k_n+f_n}$,
vemos que esta notação é compatível com o produto de RTn.

Provamos então o seguinte teorema.

1.4 Teorema:

O anel de representação RTn é o anel $Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_n,\alpha_n^{-1}]$, de todos os polinômios nas indeterminadas $\alpha_1,\ldots,\alpha_n$ e suas inversas, com α_i correspondendo a classe $[C(0,\ldots,0,1,0,\ldots,0)]$, onde o 1 aparece na i-ésima posição.

1.5 Definição:

Denominaremos toro, de uma maneira geral, a qualquer grupo topológico isomorfo a um toro n-dimensional Tn.

Vamos agora iniciar o estudo dos grupos O(n), SO(n) e Spin(n).

Estamos interessados em encontrar subgrupos toros T destes grupos com a propriedade de que a união das classes de conjugação de T seja o grupo todo.

Seja T um subgrupo toro de um grupo G compacto tal que

$$G = \bigcup_{g\,\varepsilon\, G} gTg^{-1} .$$

Nestas condições, T é denominado toro maximal de G.

Como T é conexo, concluimos que G também o é, por ser união de conjuntos conexos que possuem ponto comum. Logo não é verdade que qualquer grupo G contenha um subgrupo T como acima.

Observação:

Pode-se provar (vide [7]) que um toro maximal T de G é na verdade um elemento maximal no conjunto ordenado por inclusão de todos os subgrupos toro de G e que se $s \in G$ comutar com todos os elementos de T então $s \in T$.

Denotemos por N_T o normalizador de T em G, ou seja, N_T é o subgrupo de todos os elementos $g \in G$ tais que $gTg^{-1} = T$.

1.6 Definição:

O grupo de Weyl W de G em relação a T é o grupo quociente N_T/T.

Fixando g pertencente a N_T, a aplicação que a cada $t \in T$ associa o conjugado gtg^{-1} é um automorfismo de T que é restrição a T de um automorfismo interno de G.

Pela observação acima, este automorfismo de T é a identidade se e somente se g pertencer a T.

Associando a cada elemento de W, com representante $g \in N_T$, o automorfismo de T conjugação por g, definido acima, podemos dizer que W atua por conjugação sobre T.

A inclusão i de T em G é um homomorfismo de grupos e pelo teorema 3.17 do capítulo I o homomorfismo Ri de RG em RT é monomorfismo e podemos considerar RG como subanel de RT.

O grupo de Weyl W também atua sobre RT, associando a cada g em N_T a aplicação de RT em RT correspondente através da operação R ao automorfismo de T conjugação por g.

O subanel RT_W dos elementos de RT invariantes pela atuação de W contém RG, uma vez que, pelo lema 3.9 do capítulo I, todo automorfismo interno de G induz a identidade em RG. Para calcularmos RG, é conveniente calcularmos primeiramente RT_W, já que RG é subanel de RT_W.

2. O grupo unitário $U(n)$

2.1 Definição:

O grupo unitário $U(n)$ consiste de todas as matrizes $n \times n$ complexas inversíveis A com $A^{-1} = \bar{A}^t$, com a operação de multiplicação usual, onde $\bar{A}^t$ representa a conjugada transposta de A.

Qualquer matriz de $U(n)$ é denominada matriz unitária.

Como o espaço vetorial das matrizes $n \times n$ complexas é isomorfo a C^{n^2}, vamos identificá-los, e tornamos $U(n)$ um grupo topológico com a topologia induzida de C^{n^2}. É fácil ver que $U(n)$ é compacto lembrando que, como

$$||A|| = \left(\sum_{i,j=1}^{n} |a_{ij}|^2\right)^{1/2} = \sqrt{n}\ , \quad \forall\, A = (a_{ij}) \in U(n)\ ,$$

$U(n)$ é limitado, e que $U(n)$ é fechado por ser imagem inversa da identidade $I \in C^{n^2}$ pela aplicação contínua que a cada $A \in C^{n^2}$ associa a matriz $A\bar{A}^t \in C^{n^2}$.

O grupo $U(n)$ atua de maneira natural sobre o espaço vetorial complexo C^n através da multiplicação

$$A.(z_1,\ldots,z_n) = \left(\sum_{k=1}^{n} a_{1k}z_k,\ldots,\sum_{k=1}^{n} a_{nk}z_k\right) \quad ,$$

onde $A = (a_{ij}) \in U(n)$ e $(z_1,\dots,z_n) \in C^n$.

Denotemos simplesmente por C^n este $U(n)$-módulo e por λ_1 a classe $[C^n]$ de $RU(n)$.

O elemento $[\Lambda^k C^n] \in RU(n)$ correspondente ao k-ésimo produto exterior será denotado por λ_k.

Observemos que $\Lambda^n C^n$ é unidimensional com $U(n)$ atuando por

$$A.(z_1 \wedge \dots \wedge z_n) = \det A \; z_1 \wedge \dots \wedge z_n \quad ,$$

para quaisquer $A \in U(n)$ e $(z_1,\dots,z_n) \in C^n$.

De fato, se $\{e_1,\dots,e_n\}$ é a base canônica de C^n, então $\{e_1 \wedge \dots \wedge e_n\}$ é base de $\Lambda^n C^n$ e, para qualquer matriz unitária $A = (a_{ij})$, temos

$$A.(e_1 \wedge \dots \wedge e_n) = A.e_1 \wedge \dots \wedge A.e_n =$$

$$= (\sum_{j=1}^{n} a_{j1} e_j) \wedge \dots \wedge (\sum_{j=1}^{n} a_{jn} e_j) = (\sum_{\sigma \in Sn} (\operatorname{sgn} \sigma) a_{\sigma(1)1} \cdot \dots \cdot a_{\sigma(n)n}) e_1 \wedge$$

$$\wedge \dots \wedge e_n = \det A \; e_1 \wedge \dots \wedge e_n \; ,$$

onde Sn é o n-ésimo grupo simétrico e $\operatorname{sgn} \sigma$ vale +1 se σ for par e -1 caso contrário.

As matrizes unitárias diagonais formam um subgrupo T de $U(n)$ que é claramente isomorfo ao toro n-dimensional Tn, uma vez que cada matriz $A \in T$ se escreve como

$$A = \operatorname{Diag}(e^{i\theta_1},\dots,e^{i\theta_n}) = \begin{bmatrix} e^{i\theta_1} & 0 & \dots & 0 \\ 0 & e^{i\theta_2} & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & e^{i\theta_n} \end{bmatrix}$$

com $\theta_1,\dots,\theta_n$ reais, e podemos associar-lhe o elemento $[(\theta_1,\dots,\theta_n)]$ de Tn.

É fato bem conhecido da álgebra linear que cada matriz unitária é unitariamente equivalente a uma matriz diagonal, ou seja, para cada A em $U(n)$, existe B em $U(n)$ tal que BAB^{-1} pertence a T. Concluímos que $U(n) = \bigcup_{A \in U(n)} ATA^{-1}$ e que T é toro maximal de $U(n)$.

Determinemos o grupo de Weyl W de $U(n)$ em relação a T.

Se $A \in N_T$, temos $ATA^{-1} = T$ ou $A^{-1}TA = T$. Seja $B = \text{Diag}(a_1, \ldots, a_n)$, onde os complexos de módulo 1 $a_1, \ldots, a_n$ são dois a dois distintos.

A relação $A^{-1}BA \in T$ implica que, para qualquer j,

$$A^{-1}BA\, e_j = b_j e_j \quad ,$$

para algum b_j complexo de módulo 1. Portanto $B(Ae_j) = b_j Ae_j$, donde Ae_j é autovetor de B. Concluímos que Ae_j é múltiplo não nulo de algum e_k.

Então podemos associar a cada matriz $A \in N_T$ uma permutação $\sigma_A \in Sn$ dada por $\sigma_A(j) = k$, para $j = 1, \ldots, n$. É claro que $A \in T$ se e somente se σ_A é igual a identidade.

Podemos então considerar o homomorfismo de grupos h de W em Sn que a cada classe de equivalência com representante $A \in N_T$ associa a permutação σ_A.

A verificação de que h está bem definida e é um homomorfismo de grupos é trivial. Na realidade, h é um isomorfismo.

A injetividade decorre de que, se σ_A é a identidade, temos $Ae_j = c_j e_j$, e portanto A é diagonal, pertencendo a T.

Para vermos que é sobrejetora, consideremos o elemento $A_{ij} \in U(n)$ caracterizado por :

$A_{ij}\, e_i = e_j$, $A_{ij}\, e_j = e_i$ e $A_{ij}\, e_k = e_k$, para qualquer k distinto de i e de j.

Então A_{ij} pertence a N_T e $\sigma_{A_{ij}}$ é o 2-ciclo $(i\ j)$. Como os 2-ciclos geram Sn, temos $Sn = h(W)$.

Isto mostra que o grupo de Weyl é isomorfo ao grupo Sn das permutações de $\{1,\ldots,n\}$.

Vamos estudar um pouco a atuação de W sobre o anel

$$RT = Z[\alpha_1,\alpha_1^{-1}, \ldots,\alpha_n,\alpha_n^{-1}] \, .$$

Se $A \in N_T$, denotemos por $[A]$ o elemento correspondente em W.

Como α_j é a classe $[C(0,\ldots,0,\underset{(j)}{1},0,\ldots,0)]$ de todos os T-módulos isomorfos ao espaço vetorial C com a atuação

$$\mathrm{Diag}(e^{i\theta_1},\ldots,e^{i\theta_n}).z = e^{i\theta_j}\, z \quad ,$$

$[A].\alpha_j$ é a classe de todos os T-módulos que são isomorfos a C com a atuação

$$\mathrm{Diag}(e^{i\theta_1},\ldots,e^{i\theta_n})_* z = (A\mathrm{Diag}(e^{i\theta_1},\ldots,e^{i\theta_n})A^{-1}).z \, .$$

Calculemos $X = A\ \mathrm{Diag}(e^{i\theta_1},\ldots,e^{i\theta_n})\ A^{-1}$.

Sabemos que, para cada $j = 1,\ldots,n$, $A\, e_j = a_j\, e_{\sigma_A(j)}$, com a_j pertencente a C. Logo a k-ésima coluna da matriz $Y = A\mathrm{Diag}(e^{i\theta_1}, \ldots,e^{i\theta_n})$ será formada pelas coordenadas do vetor

$$A\ (e^{i\theta_k}\, e_k) = e^{i\theta_k}\, a_k\, e_{\sigma_A(k)} \quad .$$

Então Y^t terá a k-ésima linha formada pelas coordenadas do vetor $e^{i\theta_k} a_k e_{\sigma_A(k)}$ e portanto terá sua k-ésima coluna formada pelas coordenadas do vetor $e^{i\theta_{\sigma_A^{-1}(k)}} a_{\sigma_A^{-1}(k)}\, e_{\sigma_A^{-1}(k)}$.

Portanto $\overline{X}^t$ será a matriz $\overline{A}^{-1\,t}\ \overline{Y}^{\,t} = A\ \overline{Y}^t$ cujas k-ésima colu na $\bar{e}$ constituida pelas coordenadas do vetor

$$A\,(e^{-i\theta_{\sigma_A^{-1}(k)}}\,\bar{a}_{\sigma_A^{-1}(k)}\,e_{\sigma_A^{-1}(k)}\,) = e^{-i\theta_{\sigma_A^{-1}(k)}}\bar{a}_{\sigma_A^{-1}(k)}a_{\sigma_A^{-1}(k)}e_k\,,$$

e, como A leva base ortonormal em base ortonormal, temos $|a_j| = 1$.

Mostramos assim que $\bar{X}^t = \mathrm{Diag}(e^{-i\theta_{\sigma_A^{-1}(1)}},\dots,e^{-i\theta_{\sigma_A^{-1}(n)}})$, ou seja,

$$X = \mathrm{Diag}(e^{i\theta_{\sigma_A^{-1}(1)}},\dots,e^{i\theta_{\sigma_A^{-1}(n)}})\quad .$$

Então $[A]\cdot\alpha_j$ é o espaço vetorial C com a atuação

$$\mathrm{Diag}(e^{i\theta_1},\dots,e^{i\theta_n})_* z = e^{i\theta_{\sigma_A^{-1}(j)}} z$$

e portanto $[A]\cdot\alpha_j = \alpha_{\sigma_A^{-1}(j)}$.

A atuação de W sobre RT consiste então em permutar os elementos α_i .

Logo o anel RT_W dos polinômios de RT invariantes pela atuação de W consiste exatamente nos polinômios simétricos em relação a α_1, $\dots, \alpha_n$.

2.2 Teorema:

O anel de representação $RU(n)$ é o anel $Z[\lambda_1,\dots,\lambda_n,\lambda_n^{-1}]$ de todos os polinômios com coeficientes inteiros em $\lambda_1,\lambda_2,\dots,\lambda_n$ e λ_n^{-1}, onde não existem relações polinomiais entre $\lambda_1,\dots,\lambda_n$.

Notemos que uma base aditiva para $RU(n)$ é constituida pelos monômios $\lambda_1^{i_1}\lambda_2^{i_2}\dots\lambda_n^{i_n}$, onde os inteiros $i_1,\dots,i_{n-1}$ são todos não negativos, enquanto i_n pode assumir valores negativos.

Prova:

Temos $RU(n) \subset RT_W \subset RT = Z[\alpha_1,\alpha_1^{-1},\dots,\alpha_n,\alpha_n^{-1}]$.

Considerando C^n como T-módulo, vemos que é soma direta de n T-módulos unidimensionais com classes de isomorfismo $\alpha_1,\dots,\alpha_n$.

Pelo lema 2.7 do capítulo I, temos

$$\lambda_0 = 1, \quad \lambda_1 = \alpha_1+\ldots+\alpha_n, \quad \ldots, \quad \lambda_n=\alpha_1\ldots\alpha_n \quad .$$

Podemos então considerá-los como funções simétricas elementares em $\alpha_1,\ldots,\alpha_n$.

Sabemos que λ_n é a classe dos $U(n)$-módulos unidimensionais isomorfos a C com a atuação

$$A.z = \det A \; z \quad , \quad \forall\, A \in U(n), \; \forall\, z \in C.$$

Denotando por λ_n^{-1} a classe dos $U(n)$-módulos unidimensionais isomorfos a C com a atuação

$$A.z = (\det A)^{-1} z \; , \quad \forall\, A \in U(n), \; \forall\, z \in C,$$

temos $\lambda_n\lambda_n^{-1} = 1$ e $\lambda_n^{-1} = \alpha_1^{-1}\ldots\alpha_n^{-1}$.

Vamos agora utilizar algumas propriedades de funções simétricas que se encontram demonstradas, por exemplo, em [11] .

Não existem relações polinomiais entre $\lambda_1,\ldots,\lambda_n$.

Já concluimos que $Z[\lambda_1,\ldots,\lambda_n,\lambda_n^{-1}]$ RT_W. Vamos mostrar que são realmente iguais.

Seja $f \in RT$ um polinômio em $\alpha_1,\alpha_1^{-1},\ldots,\alpha_n,\alpha_n^{-1}$ com coeficientes inteiros invariantes por permutações de $\alpha_1,\ldots,\alpha_n$, ou seja, pertencente a RT_W. Então, para algum inteiro K, temos $\lambda_n^K f = g$, onde g é um polinômio em $\alpha_1,\ldots,\alpha_n$, com coeficientes inteiros, invariante por permutações de $\alpha_1,\ldots,\alpha_n$.

Como todo polinômio simétrico se escreve como polinômio nas funções simétricas elementares, concluimos que g é polinômio com coeficientes inteiros em $\lambda_1,\ldots,\lambda_n$. Logo, como $f = \lambda_n^{-K}g$, f pertence a

$Z[\lambda_1,\ldots,\lambda_n,\lambda_n^{-1}]$. Isto mostra que

$$RU(n) = RT_W = Z[\lambda_1,\ldots,\lambda_n,\lambda_n^{-1}] ,$$

como queríamos.

3. O grupo de rotações $SO(n)$

3.1 Definição:

O grupo de rotações $SO(n)$ consiste de todas as matrizes A reais $n \times n$ com determinante $+1$ tais que $A^{-1} = A^t$, com a multiplicação usual. É fácil verificar que $SO(n)$ é um grupo topológico compacto com a topologia induzida do R^{n^2}.

Este grupo atua de maneira natural sobre o espaço vetorial real R^n pela multiplicação matricial

$$A.x = \left(\sum_{i=1}^{n} a_{1i}x_i,\ldots,\sum_{i=1}^{n} a_{ni}x_i\right) ,$$

para todos $A = (a_{ij}) \in SO(n)$ e $x = (x_1,\ldots,x_n) \in R^n$.

Então R^n torna-se um $SO(n)$-módulo real e podemos considerar o $SO(n)$-módulo k-ésimo produto exterior $\Lambda^k R^n$.

Sejam $\{ e_1,\ldots,e_n \}$ a base canônica do R^n e $\{e_{i_1}\wedge\ldots\wedge e_{i_k} : 1 \leq i_1<\ldots<i_k \leq n \}$ a base canônica de $\Lambda^k R^n$.

Os $SO(n)$-módulos reais $\Lambda^k R^n$ e $\Lambda^{n-k} R^n$ são isomorfos. Construamos o isomorfismo.

Para cada $e_{i_1}\wedge\ldots\wedge e_{i_k}$ da base de $\Lambda^k R^n$, com k distinto de 0 e de n, seja $e_{j_1}\wedge\ldots\wedge e_{j_{n-k}}$ o elemento da base de $\Lambda^k R^n$ tal que

$$e_{i_1}\wedge\ldots\wedge e_{i_k}\wedge\ldots\wedge e_{j_{n-k}} = \operatorname{sgn}\sigma\, e_1\wedge\ldots\wedge e_k\wedge e_{k+1}\wedge\ldots\wedge e_n ,$$

onde σ é a permutação

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & k & k+1 & \ldots & n \\ i & i_2 & \ldots & i_k & j_1 & \ldots & j_{n-k} \end{pmatrix}$$

Seja então f_k a transformação linear de $\Lambda^k R^n$ sobre $\Lambda^{n-k} R^n$ que a cada $e_{i_1} \wedge \ldots \wedge e_{i_k}$ da base canônica de $\Lambda^k R^n$ associa o elemento $\operatorname{sgn} \sigma \; e_{j_1} \wedge \ldots \wedge e_{j_{n-k}}$ de $\Lambda^{n-k} R^n$.

Então $e_{i_1} \wedge \ldots \wedge e_{i_k} \wedge f_k(e_{i_1} \wedge \ldots \wedge e_{i_k}) = e_1 \wedge \ldots \wedge e_n$. É claro que f_k é isomorfismo de espaços vetoriais pois leva base em base, e vamos mostrar que f_k preserva a atuação de $SO(n)$.

Se $w \in \Lambda^k R^n$ e $\mu \in \Lambda^{n-k} R^n$, temos

$$A.(w \wedge \mu) = A.w \wedge A.\mu = \det A \; w \wedge \mu = w \wedge \mu \quad .$$

É útil mostrar que $f_k(w)$ possui a seguinte propriedade: para qualquer $\mu \in \Lambda^{n-k} R^n$, temos $\langle f_k(w), \mu \rangle = \operatorname{Det}(w \wedge \mu)$, onde Det é o isomorfismo canônico entre $\Lambda^n R^n$ e R.

Basta demonstrá-la para $w = e_{i_1} \wedge \ldots \wedge e_{i_k}$ e $\mu = e_{r_1} \wedge \ldots \wedge e_{r_{n-k}}$.

Temos $f_k(e_{i_1} \wedge \ldots \wedge e_{i_k}) = \operatorname{sgn} \sigma \; e_{j_1} \wedge \ldots \wedge e_{j_{n-k}}$ e

$$\langle f_k(w), \mu \rangle = \operatorname{sgn} \sigma \; \det(\langle e_{j_s}, e_{r_t} \rangle) \; .$$

Se $\{e_{i_1}, \ldots, e_{i_k}\}$ e $\{e_{r_1}, \ldots, e_{r_{n-k}}\}$ tiverem algum elemento comum, digamos e_{r_1}, então certamente e_{r_1} não pertence a $\{e_{j_1}, \ldots, e_{j_{n-k}}\}$ e a matriz $(\langle e_{j_s}, e_{r_t} \rangle)$ terá a primeira coluna nula, donde

$$\langle f_k(e_{i_1} \wedge \ldots \wedge e_{i_k}), e_{r_1} \wedge \ldots \wedge e_{r_{n-k}} \rangle = 0 \quad .$$

Por outro lado, $e_{i_1} \wedge \ldots \wedge e_{i_k} \wedge e_{r_1} \wedge \ldots \wedge e_{r_{n-k}} = 0$, donde $\langle f_k(w), \mu \rangle = \operatorname{Det}(w \wedge \mu)$.

Se $\{e_{i_1}, \ldots, e_{i_k}\}$ e $\{e_{r_1}, \ldots, e_{r_{n-k}}\}$ não possuirem elemento comum, então existe uma permutação de $n-k$ elementos ρ tal que

$$e_{j_1} \wedge \ldots \wedge e_{j_{n-k}} = \operatorname{sgn} \rho \; e_{r_1} \wedge \ldots \wedge e_{r_{n-k}} \quad ,$$

e

$$\langle f_k(e_{i_1} \wedge \ldots \wedge e_{i_k}), e_{r_1} \wedge \ldots \wedge e_{r_{n-k}} \rangle =$$

$$= \text{sgn}\,\sigma\ \text{sgn}\,\rho <e_{r_1}\wedge\ldots\wedge e_{r_{n-k}}, e_{r_1}\wedge\ldots\wedge e_{r_{n-k}}> = \text{sgn}\sigma\ \text{sgn}\rho\ .$$

Por outro lado,

$$\text{Det}(e_{i_1}\wedge\ldots\wedge e_{i_k}\wedge e_{r_1}\wedge\ldots\wedge e_{r_{n-k}}) = \text{sgn}\,\rho\ \text{Det}(e_{i_1}\wedge\ldots\wedge e_{i_k}\wedge e_{j_1}\wedge\ldots\wedge$$
$$\wedge\, e_{j_{n-k}}) = \text{sgn}\,\rho\ \text{sgn}\,\sigma\ ,$$

mostrando a igualdade desejada.

Vamos demonstrar que f_k comuta com a atuação de $SO(n)$.

Se $A \in SO(n)$, temos , para qualquer $\mu \in \Lambda^{n-k}R^n$,

$<A.f_k(w),\mu> = <A.f_k(w),AA^t.\mu> = <f_k(w),A^t.\mu>$ (pois A é ortogonal)

$= \text{Det}(w\wedge A^t.\mu) = \text{Det}(A.w\wedge AA^t.\mu) = \text{Det}(A.w\wedge\mu) = <f_k(A.w),\mu>$.

Logo

$<A.f_k(w),\mu> - <f_k(A.w),\mu> = <A.f_k(w)-f_k(A.w),\mu> = 0.$

Em particular, para $\mu = A.f_k(w)-f_k(A.w)$, temos

$<A.f_k(w)-f_k(A.w),A.f_k(w)-f_k(A.w)> = 0,$

donde .. $A.f_k(w) = f_k(A.w)$, como queríamos.

Isto mostra que f_k é isomorfismo de $SO(n)$-módulos.

Para $k = n$, definimos $f_n: \Lambda^nR^n \dashrightarrow R$ como a aplicação linear que a $e_1\wedge\ldots\wedge e_n \in \Lambda^nR^n$ associa o elemento $1 \in R$. Então f_n é isomorfismo de espaços vetoriais e para cada $A \in SO(n)$, temos

$$f_n(A.e_1\wedge\ldots\wedge e_n) = f_n(\det A\ e_1\wedge\ldots\wedge e_n) = \det A\ f_n(e_1\wedge\ldots\wedge e_n) =$$
$$= 1.1 = 1 = A.1 = A.f_n(e_1\wedge\ldots\wedge e_n)\ ,$$

o que mostra que f_n é isomorfismo de $SO(n)$-módulos (aqui R é considerado um $SO(n)$-módulo real com a atuação trivial) .

Como para qualquer elemento $e_{i_1}\wedge\ldots\wedge e_{i_k}$ da base canônica de Λ^kR^n temos $e_{i_1}\wedge\ldots\wedge e_{i_k}\wedge f_k(e_{i_1}\wedge\ldots\wedge e_{i_k}) = e_1\wedge\ldots\wedge e_n$, segue-se que

$$f_{n-k}\circ f_k(e_{i_1}\wedge \ldots \wedge e_{i_k}) = (-1)^{k(n-k)} e_{i_1}\wedge \ldots \wedge e_{i_k} .$$

No caso de n ser par, ou seja, $n = 2k$, para algum k, f_k é um automorfismo de $\Lambda^k R^n$. Se k, por sua vez, também for par, temos $f_k \circ f_k$ igual a identidade, donde os autovalores de f_k serão ± 1 .

Logo $\Lambda^k R^{2k}$ se decomporá como soma direta de dois subespaços de autovetores associados a $+1$ e a -1, respectivamente. Como f_k preserva a atuação de $SO(n)$, é claro que estes subespaços são na verdade submódulos.

Se k for ímpar, os autovalores de f_k serão $\pm i$ e portanto não existe uma tal decomposição.

Consideremos então o $SO(n)$-módulo complexificado $\Lambda^k R^{2k} \otimes C$.

Este módulo é construido como segue.

Pensemos no espaço vetorial real C como um $SO(n)$-módulo real com a atuação trivial

$$A.z = z \ , \quad \forall\, z \in C, \ \forall\, A \in SO(n) \quad .$$

Então podemos formar o $SO(n)$-módulo real produto tensorial $\Lambda^k R^{2k} \otimes C$. Podemos considerar o conjunto $\Lambda^k R^{2k} \otimes C$ como $SO(n)$-módulo complexo conservando a adição e a atuação anteriores e definindo o produto por escalar através de

$$C \times \Lambda^k R^{2k} \otimes C \longrightarrow \Lambda^k R^{2k} \otimes C$$
$$(z_1, \phi \otimes z_2) \quad \longmapsto \phi \otimes z_1 z_2 \qquad .$$

É trivial verificar que este produto por escalar, quando restrito ao caso real, coincide com o anterior.

Se $f: \Lambda^k R^{2k} \longrightarrow \Lambda^k R^{2k}$ for uma transformação linear de espaços vetoriais reais, podemos "extendê-la" a uma transformação linear complexa $\tilde{f}: \Lambda^k R^{2k} \otimes C \longrightarrow \Lambda^k R^{2k} \otimes C$ definida por $\tilde{f}(\phi \otimes z) = f(\phi) \otimes z$, para quais -

quer $\phi \in \Lambda^k R^{2k}$ e $z \in C$.

É interessante notar que, se $\{\phi_1,\ldots,\phi_m\}$ for base para $\Lambda^k R^{2k}$, então $\{\phi_1 \otimes 1,\ldots,\phi_m \otimes 1\}$ é base para o complexificado $\Lambda^k R^{2k} \otimes C$, de modo que a matriz real representando f em relação a base considerada acima coincide com a matriz complexa representante de $\tilde{f}$ em relação a base acima de $\Lambda^k R^{2k} \otimes C$.

Identificamos então f com $\tilde{f}$.

Em tudo o que segue, $\Lambda^k R^n \otimes C$ representa o $SO(n)$-módulo complexificado.

Agora, se $n = 2k$ com k ímpar, os autovalores de f_k são i e $\Lambda^k R^{2k} \otimes C$ se decompõe como soma direta de dois submódulos de autovetores associados a $+i$ e a $-i$, respectivamente.

Notemos também que, para quaisquer n e k, $\Lambda^k R^n \otimes C$ é isomorfo, como $SO(n)$-módulo, a $\Lambda^k C^n$. Para ver isto, basta considerar o isomorfismo de $\Lambda^k R^n \otimes C$ sobre $\Lambda^k C^n$ que a cada $e_{i_1} \wedge \ldots \wedge e_{i_k} \otimes 1 \in \Lambda^k R^n \otimes C$ associa $e_{i_1} \wedge \ldots \wedge e_{i_k} \in \Lambda^k C^n$.

Seja λ_k o elemento do anel de representação de $SO(n)$ cujo representante é o $SO(n)$-módulo $\Lambda^k R^n \otimes C \cong \Lambda^k C^n$. Vimos que $\lambda_k = \lambda_{n-k}$ e que, se $n = 2r$, $\Lambda^r R^n \otimes C$ se decompõe como soma direta de dois $SO(n)$-submódulos complexos formados respectivamente por todos os autovetores associados a $+1$ ou $+i$ e a -1 ou $-i$, conforme r seja par ou ímpar.

Denotemos estes submódulos por V e W, respectivamente. Logo λ_r é igual a soma

$$\lambda_r = [V] + [W] \quad .$$

3.2 Teorema:

Se $n = 2r+1$, o anel de representação $RSO(n)$ é o anel de polinômios $Z[\lambda_1,\ldots,\lambda_r]$. Se $n = 2r$, o anel $RSO(n)$ é gerado, como anel de polinômios, pelos elementos $\lambda_1,\ldots,\lambda_{r-1},\lambda_r^+,\lambda_r^-$, que não são algebricamente independentes. Satisfazem a relação

$$(\lambda_r^+ + \lambda_{r-2} + \lambda_{r-4} + \ldots)(\lambda_r^- + \lambda_{r-2} + \lambda_{r-4} + \ldots) =$$
$$= (\lambda_{r-1} + \lambda_{r-3} + \ldots)^2 ,$$

onde cada soma termina em $\lambda_4 + \lambda_2 + 1$ ou $\lambda_3 + \lambda_1$ e λ_r^+ e λ_r^- são notações convenientes de $[V]$ e $[W]$.

Prova:

Inicialmente consideremos o caso $n = 2r+1$.

Seja $A(\theta)$ a matriz 2×2 dada por

$$A(\theta) = \begin{bmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{bmatrix}, \ \theta \in R .$$

A matriz $A(\theta)$ representa uma rotação de ângulo θ em R^2.

Seja T o subgrupo de $SO(n)$ de todas as matrizes da forma $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$, ou seja, das matrizes $n \times n$ formadas por r blocos $A(\theta_i)$ dispostos ao longo da diagonal principal, cujo último elemento é 1 e os demais elementos da matriz são nulos.

A topologia induzida de $SO(n)$ torna T um grupo topológico isomorfo ao r-ésimo toro Tr. Um isomorfismo é dado pela aplicação de T sobre Tr que a cada $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$ associa $[(\theta_1,\ldots,\theta_r)]$.

Vamos mostrar que T é um toro maximal em $SO(n)$.

3.3 Lema:

Cada elemento de $SO(2r+1)$ é conjugado em $SO(2r+1)$ a algum elemento do toro T.

Por ora, suporemos este fato como verdadeiro.

Então $RSO(2r+1)$ pode ser considerado como subanel de $RT = Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}]$, onde α_j é a classe de isomorfismo do T-módulo C com a atuação $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1).z = e^{i\theta_j}z$, para todos $z \in C$ e $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1) \in T$.

O grupo de Weyl $W = N_T/T$ de $SO(2r+1)$ em relação a T consiste de todas as permutações dos índices de $\theta_1,\ldots,\theta_r$ compostas com as substituições $(\theta_1,\ldots,\theta_r) \dashrightarrow (\pm\theta_1,\ldots,\pm\theta_r)$, tendo portanto $2^r\, r!$ elementos.

Realmente, o automorfismo de T que a cada $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$ associa $\mathrm{Diag}(A(-\theta_1),A(\theta_2),\ldots,A(\theta_r),1)$ pode ser obtido por conjugação pela matriz $B = \mathrm{Diag}(-1,1,\ldots,1,-1)$ pertencente a $N_T \subset SO(2r+1)$.

Por outro lado, também os automorfismos de T que efetuam permutações nos índices de $\theta_1,\ldots,\theta_r$ são obtidos por conjugação através de elementos de N_T. Isto pode ser visto notando que a matriz

$$D = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

pertence a $SO(4)$ e

$$D\,\mathrm{Diag}(A(\theta_1),A(\theta_2))\,D^{-1} = \mathrm{Diag}(A(\theta_2),A(\theta_1)) \quad .$$

Então todas as permutações que trocam dois elementos consecutivos são obtidas por conjugação por matrizes do tipo $\mathrm{Diag}(1,\ldots,1,D,1,\ldots,1)$

pertencentes a N_T.

Por exemplo, o automorfismo de T que a cada matriz $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$ associa $\mathrm{Diag}(A(\theta_1),A(\theta_3),A(\theta_2),A(\theta_4),\ldots,A(\theta_r),1)$ é obtido por conjugação através da matriz $(2r+1)\times(2r+1)$

$$\mathrm{Diag}(1,1,D,1,\ldots,1) .$$

Então todos os automorfismos de T correspondentes as transposições $(i\ i+1)$, com $1\leq i\leq r-1$, são obtidos por conjugações por elementos de N_T e como estas transposições geram o grupo simétrico Sr, W contém todas as permutações de índices de $\theta_1, \ldots,\theta_r$, todas as substituições de θ_i por $\pm\theta_i$ e todas as composições feitas a partir destes elementos.

Mostremos agora que W contém apenas estes elementos.

Seja $U = \mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$, onde os θ_i são números reais distintos e não nulos.

Um cálculo simples mostra que seus autovalores são 1, $e^{\pm i\theta_1},\ldots, e^{\pm i\theta_r}$ com respectivos autovetores e_{2r+1}, $e_1 \pm ie_2,\ldots, e_{2r-1} \pm ie_{2r}$.

Se $B \in N_T$, temos $BUB^{-1} \in T$, e aplicando BUB^{-1} a qualquer autovetor acima, digamos, a $e_{2j-1} + ie_{2j}$, obtemos

$$BUB^{-1}(e_{2j-1} + ie_{2j}) = b_j(e_{2j-1} + ie_{2j}) ,$$

com b_j complexo de módulo 1. Logo $B^{-1}(e_{2j-1} + ie_{2j})$ é autovetor de U e portanto

$$B^{-1}(e_{2j-1} + ie_{2j}) = a_j(e_{2k-1} \pm ie_{2k}) , \quad \text{com } a_j \in C.$$

Da mesma forma,

$$B^{-1} e_{2r+1} = a\, e_{2r+1} , \text{ com } a \in C.$$

Concluimos então que

$$B(e_{2k-1} + ie_{2k}) = c_k(e_{2j-1} \pm ie_{2j}),$$

com c_k complexo de módulo 1 e $j = \sigma(k)$, para $k = 1,\dots,r$, onde $\sigma \in Sr$.

Fazendo $c_k = \cos\phi_k + i\,\text{sen}\,\phi_k$, a comparação das partes real e imaginária da igualdade acima fornece

$$B\,e_{2k-1} = \cos\phi_k\,e_{2j-1} \mp \text{sen}\,\phi_k\,e_{2j} \qquad \text{e}$$

$$B\,e_{2k} = \text{sen}\,\phi_k\,e_{2j-1} \pm \cos\phi_k\,e_{2j} .$$

Também $B\,e_{2r+1} = c\,e_{2r+1}$, com $c \in C$ de módulo 1.

Logo a ação de B sobre os pares de eixos e_{2k-1} e e_{2k} é dada por

$$(1) \qquad \begin{aligned} B\,e_{2k-1} &= \cos\phi_k\,e_{2j-1} - \text{sen}\,\phi_k\,e_{2j} \\ B\,e_{2k} &= \text{sen}\,\phi_k\,e_{2j-1} + \cos\phi_k\,e_{2j} \end{aligned} ,$$

e então B realiza essencialmente uma rotação seguida por uma permutação de eixos, ou

$$(2) \qquad \begin{aligned} B\,e_{2k-1} &= \cos\phi_k\,e_{2j-1} + \text{sen}\,\phi_k\,e_{2j} \\ B\,e_{2k} &= \text{sen}\,\phi_k\,e_{2j-1} - \cos\phi_k\,e_{2j} \end{aligned} ,$$

e então B realiza uma rotação seguida por uma permutação de eixos e de uma reflexão do eixo e_{2j}.

Definamos então as matrizes reais $2r+1 \times 2r+1$ auxiliares R_f, P e R por :

$$R_f\,e_{2k-1} = e_{2k-1}\,,\ R_f\,e_{2k} = \begin{cases} -e_{2k}\,, & \text{caso } B \text{ atue como em } (2) \\ e_{2k}\,, & \text{caso } B \text{ atue como em } (1) \end{cases} ,$$

$$P\ e_{2k-1} = e_{2j-1}\,,\ P\ e_{2k} = e_{2j} ,$$

para $k = 1,\dots, r$, e

$$R_f\,e_{2r+1} = e_{2r+1}\,,\ P\ e_{2r+1} = c\,e_{2r+1} ,$$

e finalmente

$$R = \text{Diag}(A(\phi_1),\dots,A(\phi_r),1) .$$

Então $B = R_f PR$, donde para qualquer matriz $D = \mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$ pertencente a T, temos

$$BDB^{-1} = R_f PRDR^{-1}P^{-1}R_f^{-1} = R_f PDP^{-1}R_f^{-1} ,$$

uma vez que R pertence a T.

Um simples cálculo mostra que $PD = X$, onde

$$X_{2j-1\ 2k-1} = \cos\theta_k ,\ X_{2j-1\ 2k} = \mathrm{sen}\,\theta_k ,$$

$$X_{2j\ 2k-1} = -\mathrm{sen}\,\theta_k ,\ X_{2j\ 2k} = \cos\theta_k .$$

Logo $(XP^{-1})^t = PX^t = \mathrm{Diag}(A(-\theta_{\sigma_1^{-1}}),\ldots,A(-\theta_{\sigma_r^{-1}}),1)$ donde $PDP^{-1} = \mathrm{Diag}(A(\theta_{\sigma_1^{-1}}),\ldots,A(\theta_{\sigma_r^{-1}}),1)$.

Como $R_f DR_f^{-1} = \mathrm{Diag}(A(\pm\theta_{\sigma_1^{-1}}),\ldots,A(\pm\theta_{\sigma_r^{-1}}),1)$, concluimos que qualquer automorfismo de T obtido por conjugação através de um elemento de N_T é composição de permutações dos índices de $\theta_1,\ldots,\theta_r$ com substituições de θ_i por $\pm\theta_i$.

O anel RT_W de todos os elementos de RT que são invariantes pela atuação de W é então constituido pelos polinômios em $\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}$ que são invariantes por permutações de $\alpha_1,\ldots,\alpha_r$ e por substituições de α_j por α_j^{-1}.

Temos $RSO(2r+1) \subset RT_W$. Vamos calcular RT_W.

Primeiramente consideremos um elemento $\phi \in RT$ invariante pela troca de α_1 por α_1^{-1}. Então ϕ pode ser escrito como polinômio em $\alpha_1+\alpha_1^{-1}$, $\alpha_2, \alpha_2^{-1},\ldots,\alpha_r,\alpha_r^{-1}$.

De fato, podemos escrever

$$\phi = \Sigma\, \alpha_1^j\, f_j(\alpha_2,\alpha_2^{-1},\ldots,\alpha_r,\alpha_r^{-1}) ,$$

onde f_j é polinômio em $\alpha_2,\alpha_2^{-1},\ldots,\alpha_r,\alpha_r^{-1}$ e a somatória é efetuada sobre todos os j inteiros.

Como ϕ é invariante pela troca de α_1 por α_1^{-1}, temos $f_j = f_{-j}$ e $\phi = \sum_{j>0} (\alpha_1^j + \alpha_1^{-j}) f_j(\alpha_2, \alpha_2^{-1}, \ldots, \alpha_r, \alpha_r^{-1}) + f_0(\alpha_2, \alpha_2^{-1}, \ldots, \alpha_r, \alpha_r^{-1})$.

Sejam $h_1 = \alpha_1 + \alpha_1^{-1}$ e $h_2 = \alpha_1^2 + \alpha_1^{-2} = (\alpha_1 + \alpha_1^{-1})^2 - 2$.

Se $h_n = \alpha_1^n + \alpha_1^{-n}$, $n \geq 3$, podemos demonstrar, por indução, que $h_n = (\alpha_1 + \alpha_1^{-1}) h_{n-1} - h_{n-2}$.

Isto implica que ϕ pode ser escrito como polinômio em $\alpha_1 + \alpha_1^{-1}$, $\alpha_2, \alpha_2^{-1}, \ldots, \alpha_r, \alpha_r^{-1}$.

Agora suponhamos que $\phi \in RT$ seja invariante sob todas as trocas de α_i por α_i^{-1}, $i = 1, \ldots, r$.

Um argumento indutivo mostra que ϕ pode ser escrito como polinômio em $\alpha_1 + \alpha_1^{-1}, \ldots, \alpha_r + \alpha_r^{-1}$, ou seja, $\phi \in Z[\alpha_1 + \alpha_1^{-1}, \ldots, \alpha_r + \alpha_r^{-1}]$.

Se ϕ for ainda invariante sob permutações dos índices de $\alpha_1, \ldots, \alpha_r$, então, do mesmo modo que para $U(n)$, ϕ pode ser expresso como polinômio em $\tau_1, \ldots, \tau_r$, onde τ_k é a k-ésima função simétrica elementar de $\alpha_1 + \alpha_1^{-1}, \ldots, \alpha_r + \alpha_r^{-1}$, ou seja,

$$\tau_k = \sum_{1 \leq i_1 < \cdots < i_k \leq r} (\alpha_{i_1} + \alpha_{i_1}^{-1}) \ldots (\alpha_{i_k} + \alpha_{i_k}^{-1}) .$$

Como claramente $\tau_k \in RT_W$, concluimos que

$$RT_W = Z[\tau_1, \ldots, \tau_k] .$$

Vamos agora expressar os elementos $\lambda_1, \ldots, \lambda_r$ de $RSO(2r+1) \subset RT$ em termos destas funções simétricas elementares.

Consideremos C^{2r+1} como T-módulo com a atuação

$$\begin{aligned} &\mathrm{Diag}(A(\theta_1), \ldots, A(\theta_r), 1).(z_1, \ldots, z_{2r+1}) = \\ &= \cos\theta_1 z_1 + \mathrm{sen}\theta_1 z_2, -\mathrm{sen}\theta_1 z_1 + \cos\theta_1 z_2, \ldots, \cos\theta_r z_{2r-1} + \mathrm{sen}\theta_r z_{2r}, \\ &\quad -\mathrm{sen}\theta_r z_{2r-1} + \cos\theta_r z_{2r}, z_{2r+1}) . \end{aligned}$$

Vamos mostrar que $[C^{2r+1}] = \alpha_1 + \alpha_1^{-1} + \ldots + \alpha_r + \alpha_r^{-1} + 1$.

Como dois G-módulos são isomorfos se e somente se possuirem o mesmo caráter (teoremas 3.13 e 3.16 do capítulo I), calculemos os caracteres χ e χ' de $[C^{2r+1}]$ e de $\alpha_1+\alpha_1^{-1}+\ldots+\alpha_r+\alpha_r^{-1}+1$, respectivamente.

Façamos $A = \mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$. A matriz representativa,em relação a base canônica de C^{2r+1}, da aplicação linear que a cada $(z_1,\ldots,z_{2r+1}) \in C^{2r+1}$ associa $A.(z_1,\ldots,z_{2r+1}) \in C^{2r+1}$ é a própria A , e portanto

$$\chi(A) = 2\cos\theta_1 + \ldots + 2\cos\theta_r + 1 .$$

Como $\chi'(A) = \chi_{\alpha_1}(A) + \chi_{\alpha_1^{-1}}(A) + \ldots + \chi_{\alpha_r}(A) + \chi_{\alpha_r^{-1}}(A) + \chi_1(A) =$ $= e^{i\theta_1} + e^{-i\theta_1} + \ldots + e^{i\theta_r} + e^{-i\theta_r} + 1 = 2\cos\theta_1 + \ldots + 2\cos\theta_r + 1$, concluimos que $\chi = \chi'$ e que $[C^{2r+1}] = \alpha_1 + \alpha_1^{-1}+\ldots+ \alpha_r + \alpha_r^{-1} + 1$.

O lema 2.7 do capítulo I mostra que $\lambda_k = [\Lambda^k C^{2r+1}]$ é a k-ésima função simétrica elementar em $\alpha_1, \alpha_1^{-1},\ldots, \alpha_r, \alpha_r^{-1}, 1$, para $k = 1,\ldots,r$.

Então $\lambda_1 = \alpha_1 + \alpha_1^{-1} + \ldots + \alpha_r + \alpha_r^{-1} + 1 = \tau_1 + 1$,

$$\lambda_2 = \alpha_1\alpha_1^{-1} + \alpha_1\alpha_2 + \ldots + \alpha_r^{-1}1 = \tau_2 + \tau_1 + r$$

e

$$\lambda_3 = \tau_3 + \tau_2 + (r-1)\tau_1 + r .$$

Queremos mostrar que λ_k é polinômio em $\tau_1,\ldots,\tau_r$.É um simples problema de análise combinatória .

Temos $\tau_k = \sum_{1\le i_1<\cdots<i_k\le r} (\alpha_{i_1}^{\pm 1}\ldots\alpha_{i_k}^{\pm 1})$ e λ_k é a soma de todos os produtos de k elementos dentre $\alpha_1,\alpha_1^{-1},\ldots,\alpha_r$, α_r^{-1},1.

Então todo somando $\alpha_{i_1}^{\pm 1}\ldots\alpha_{i_k}^{\pm 1}$ de τ_k comparece como somando de λ_k exatamente uma vez.

Consideremos um somando α de $\lambda_k - \tau_k$. Então α é um produto de k elementos dentre $\alpha_1, \alpha_1^{-1}, \ldots, \alpha_r, \alpha_r^{-1}, 1$ e após cancelamentos obtemos $\alpha = \alpha_{i_1}^{\pm 1} \ldots \alpha_{i_s}^{\pm 1}$, com $s<k$ e os $\alpha_{i_1}, \ldots, \alpha_{i_s}$ são todos distintos, ou obtemos $\alpha = 1$.

Suponhamos $\alpha \neq 1$. Então α é somando de τ_s.

Procuremos determinar o número de somandos de λ_k que, após cancelamento, fornecem $\alpha_{i_1}^{\pm 1} \ldots \alpha_{i_s}^{\pm 1}$.

Se $k-s$ for par, podemos escrever $\alpha_{i_1}^{\pm 1} \ldots \alpha_{i_s}^{\pm 1}$ como somando de λ_k multiplicando-o por $(k-s)/2$ produtos do tipo $\alpha_j \alpha_j^{-1}$, com os α_j todos distintos entre si e dos α_i anteriores.

Então o número de somandos de λ_k que após cancelamento fornecem $\alpha_{i_1}^{\pm 1} \ldots \alpha_{i_s}^{\pm 1}$ é exatamente igual ao número binomial $\binom{r-s}{(k-s)/2}$.

Se $k-s$ for ímpar, $\alpha_{i_1}^{\pm 1} \ldots \alpha_{i_s}^{\pm 1}$ pode ser escrito como somando de λ_k multiplicando-o por 1 e por $(k-s-1)/2$ produtos do tipo $\alpha_j \alpha_j^{-1}$, com os α_j todos distintos entre si e dos α_i anteriores.

Então o número de somandos de λ_k desejados é exatamente igual a $\binom{r-s}{(k-s-1)/2}$.

Caso $\alpha = 1$, suponhamos k par. Seja β um somando de λ_k tal que $\beta = 1$. Então o elemento 1 não pode aparecer como fator de β.

Como se α_i for fator de β, α_i^{-1} também o será, temos exatamente $\binom{r}{k/2}$ tais somandos.

Se k for ímpar, o elemento 1 aparece forçosamente como fator de β, e portanto temos exatamente $\binom{r}{(k-1)/2}$ tais somandos.

$$\text{Logo}\quad \lambda_k = \tau_k + \sum_{s=1}^{k-1} a_s\tau_s + \begin{cases} \binom{r}{k/2} & \text{se } k \text{ for par,} \\ \binom{r}{(k-1)/2} & \text{se } k \text{ for ímpar} \end{cases}$$

$$\text{e} \quad a_s = \begin{cases} \binom{r-s}{(k-s)/2} & \text{se } k-s \text{ for par ,} \\ \binom{r-s}{(k-s-1)/2} & \text{se } k-s \text{ for ímpar} \end{cases}$$

Então mostramos que $\lambda_k = \tau_k$ + (combinação linear dos $\tau_1,\ldots,\tau_{k-1},1)$.

Deste modo, cada polinômio em $\tau_1,\ldots,\tau_{r-1},\tau_r$ pode se expresso como polinômio em $\lambda_1,\ldots,\lambda_r$ e reciprocamente.

Provamos assim que

$$Z[\lambda_1,\ldots,\lambda_r] \subset RSO(2r+1) \subset RT_W = Z[\lambda_1,\ldots,\lambda_r] \quad .$$

Isto completa a prova do teorema 3.2 para n ímpar, a menos do lema 3.3.

Provemos agora o teorema quando $n = 2r$.

Seja $T \subset SO(2r)$ o toro constituido por todas as matrizes do tipo $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r))$.

Suponhamos que todo elemento de $SO(2r)$ seja conjugado em $SO(2r)$ a algum elemento de T. Isto será demonstrado juntamente com o lema 3.3.

Determinemos o grupo de Weyl W de $SO(2r)$ em relação a T.

Como $\mathrm{Diag}(-1,1,-1,1,1,\ldots,1)$ pertence ao normalizador N_T e $\mathrm{Diag}(-1,1,-1,1,1,\ldots,1)\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r))\mathrm{Diag}(-1,1,-1,1,1,\ldots,1)$ =

$$= \mathrm{Diag}(A(-\theta_1),A(-\theta_2),A(\theta_3),\ldots,A(\theta_r)) \quad ,$$

vemos que o automorfismo de T que troca θ_1 por $-\theta_1$, θ_2 por $-\theta_2$ e deixa invariantes os demais pertence a W.

De modo análogo ao que foi feito para $SO(2r+1)$, prova-se que os automorfismos de T que permutam os índices de $\theta_1,\ldots,\theta_r$ também pertencem a W.

Então, por composição, todos os automorfismos de T que trocam θ_i por $\varepsilon_i\theta_i$, com $\varepsilon_i = \pm 1$, $i = 1,\ldots,r$, e $\varepsilon_1 \cdot \ldots \cdot \varepsilon_r = 1$, também estão em W.

Com o mesmo raciocínio utilizado para $n = 2r+1$, mostra-se que os $2^{r-1}r!$ automorfismos acima são exatamente os elementos de W.

Então $RSO(2r)$ é subanel de RT_W e vamos calculá-lo.

É claro que RT_W contém as funções simétricas elementares τ_1, $\ldots$, τ_r relativas a $\alpha_1+\alpha_1^{-1},\ldots,\alpha_r+\alpha_r^{-1}$.

Como $\tau_r = (\alpha_1+\alpha_1^{-1})\ldots(\alpha_r+\alpha_r^{-1}) =$

$$= \sum_{\varepsilon_1\cdots\varepsilon_r=1} \alpha_1^{\varepsilon_1}\ldots\alpha_r^{\varepsilon_r} + \sum_{\varepsilon_1\cdots\varepsilon_r=-1} \alpha_1^{\varepsilon_1}\ldots\alpha_r^{\varepsilon_r} \quad , \text{ com } \varepsilon_i = \pm 1 \ ,$$

temos $\tau_r = \tau_r^+ + \tau_r^-$, onde

$$\tau_r^+ = \sum_{\varepsilon_1\cdots\varepsilon_r=1} \alpha_1^{\varepsilon_1}\ldots\alpha_r^{\varepsilon} \quad \text{e} \quad \tau_r^- = \sum_{\varepsilon_1\cdots\varepsilon_r=-1} \alpha_1^{\varepsilon_1}\ldots\alpha_r^{\varepsilon}$$

pertencem a RT_W.

Podemos mostrar, como no caso anterior, que todo polinômio de RT_W pode se escrito como polinômio em $\alpha_1+\alpha_1^{-1},\ldots,\alpha_r+\alpha_r^{-1}$, e como deve ser invariante por permutações de $\alpha_1,\ldots,\alpha_r$, temos

$$RT_W = Z[\tau_1,\ldots,\tau_{r-1},\tau_r^+,\tau_r^-] \quad .$$

Lembremos que $\lambda_1,\ldots,\lambda_r$ são as funções simétricas elementares em $\alpha_1,\ldots,\alpha_r$ e que $\lambda_r = [V] + [W]$.

Temos $\lambda_1 = \tau_1$ e $\lambda_2 = \tau_2 + r$. Vamos mostrar que λ_k é polinômio em $\tau_1,\ldots,\tau_r$.

Os somandos de τ_k aparecem exatamente uma vez como somandos de λ_k. Repetiremos o raciocínio anterior.

Seja α um somando de $\lambda_k - \tau_k$. Após cancelamentos, obtemos $\alpha = \alpha_{i_1}^{\pm 1}\cdots\alpha_{i_s}^{\pm 1}$, com os α_i todos distintos, $s < k$, e notemos que $k-s$ é par, ou $\alpha = 1$.

Se $\alpha \neq 1$, certamente α é somando de τ_s.

O número de somandos de λ_k que, após cancelamentos, fornecem $\alpha_{i_1}^{\pm 1}\cdots\alpha_{i_s}^{\pm 1}$ é então $\binom{r-s}{(k-s)/2}$ pois tais somandos podem ser obtidos multiplicando-se $\alpha_{i_1}^{\pm 1}\cdots\alpha_{i_s}^{\pm 1}$ por $(k-s)/2$ fatores do tipo $\alpha_j\alpha_j^{-1}$, com os α_j distintos entre si e dos α_i anteriores.

Se $\alpha = 1$, o número de somandos de λ_k que o fornecem é $\binom{r}{k/2}$ se k for par e zero se k for ímpar.

Logo $\lambda_k = \tau_k + \sum_{s=2,4,\ldots,k-2} a_s\tau_s + \binom{r}{k/2}$ se k for par

e $\lambda_k = \tau_k + \sum_{s=1,3,\ldots,k-2} a_s\tau_s$ se k for ímpar,

onde $a_s = \binom{r-s}{(k-s)/2}$.

Em particular,

$$\lambda_r = \tau_r + \binom{2}{1}\tau_{r-2} + \binom{4}{2}\tau_{r-4} + \binom{6}{3}\tau_{r-6} + \cdots \quad .$$

Por outro lado, $\lambda_r = [V] + [W]$, e $[V]$ e $[W]$ são combinações lineares com coeficientes inteiros não negativos das funções simétricas elementares $\tau_1,\dots,\tau_{r-1}$ e de τ_r^+,τ_r^- e 1. Temos, por exemplo,

$$V = a\tau_r^+ + b\tau_r^- + \sigma \quad ,$$

onde a e b são inteiros iguais a 0 ou 1 e σ é combinação linear de $\tau_{r-1},\dots,\tau_1,1$.

Sejam B a matriz $\mathrm{Diag}(1,\dots,1,-1)$ de $U(2r)$ e $\{e_1,\dots,e_{2r}\}$ a base canônica de C^{2r}. Temos $B.e_i = e_i$ se $i \neq 2r$, $B.e_{2r} = -e_{2r}$ e B atua sobre $\Lambda^r C^{2r}$ através de $B.e_{i_1}\wedge\dots\wedge e_{i_r} = B.e_{i_1}\wedge\dots\wedge B.e_{i_r}$.

Então B troca V por W.

De fato, se $v \in V$, podemos escrever

$$v = v_1 + v_2 \ ,$$

onde $v_1 = \sum_{1\le i_1<\dots<i_r<2r} a_{i_1\dots i_r} e_{i_1}\wedge\dots\wedge e_{i_r}$ e

$$v_2 = \sum_{1\le i_1<\dots<i_{r-1}<2r} a_{i_1\dots i_r} e_{i_1}\wedge\dots\wedge e_{i_{r-1}}\wedge e_{2r} \ ,$$

obtendo $\quad B.v = B.v_1 + B.v_2 = v_1 - v_2$,

donde $\quad f_r(B.v) = f_r(v_1) - f_r(v_2)$.

Por outro lado,

$$B.f_r(v_1) = -f_r(v_1) \quad \text{e} \quad B.f_r(v_2) = f_r(v_2)$$

e portanto
$$\begin{aligned} f_r(B.v) &= -B.f_r(v_1) - B.f_r(v_2) = \\ &= -(B.f_r(v_1) + B.f_r(v_2)) = -B.(f_r(v_1) + f_r(v_2)). \end{aligned}$$

Como $\quad v \text{ (ou } iv) = f_r(v) = f_r(v_1) + f_r(v_2)$,

concluimos que $\quad f_r(B.v) = -B.v \text{ (ou } -iB.v)$,

donde $\quad B.v \in W$.

Da mesma forma mostramos que $B.w \in V$ para qualquer $w \in W$.

Então $h: V \longrightarrow W$ dado por $h(v) = B.v$ é um isomorfismo de espaços vetoriais.

Consideremos agora o espaço vetorial V com a atuação

$$\begin{aligned} *: SO(2r) \times V &\dashrightarrow V \\ (A,v) &\longmapsto BAB.v \end{aligned}$$

Então
$$\begin{aligned} h(A*v) &= h(BAB.v) = B.((BAB).v) = (BBAB).v = (AB).v = \\ &= A.(B.v) = A.h(v) \end{aligned},$$

mostrando assim que h é na verdade um isomorfismo de $SO(2r)$-módulos.

O homomorfismo de grupos

$$\begin{aligned} b: SO(2r) &\dashrightarrow SO(2r) \\ A &\longmapsto BAB \end{aligned}$$

induz um homomorfismo de anéis $Rb: RSO(2r) \dashrightarrow RSO(2r)$ de tal modo que $Rb(\alpha_i) = \alpha_i$ se $i \neq r$ e $Rb(\alpha_r) = \alpha_r^{-1}$ pois, para qualquer matriz $A = \text{Diag}(A(\theta_1),\dots,A(\theta_r))$, temos $BAB = \text{Diag}(A(\theta_1),\dots A(\theta_{r-1}),A(-\theta_r))$.

Pelo que foi visto acima,

$$Rb([V]) = [W] .$$

Então
$$\begin{aligned} [W] &= Rb([V]) = Rb(a\tau_r^+ + b\tau_r^- + \sigma) = \\ &= aRb(\tau_r^+) + bRb(\tau_r^-) + Rb(\sigma) = a\tau_r^- + b\tau_r^+ + \sigma, \end{aligned}$$

e
$$\lambda_r = [V] + [W] = (a + b)(\tau_r^+ + \tau_r^-) + 2\sigma ,$$

com $a + b = 1$.

Logo, denotando $[V]$ e $[W]$ convenientemente por λ_r^+ e λ_r^-, temos

$$\lambda_r^+ = \tau_r^+ + \tau_{r-2} + 3\,\tau_{r-4} + 5\,\tau_{r-6} + \dots$$

e

$$\lambda_r^- = \tau_r^- + \tau_{r-2} + 3\,\tau_{r-4} + 5\,\tau_{r-6} + \dots .$$

Isto mostra que qualquer polinômio em $\tau_1,\dots,\tau_{r-1},\tau_r^+,\tau_r^-$ pode ser expresso como polinômio em $\lambda_1,\dots,\lambda_{r-1},\lambda_r^+,\lambda_r^-$ e reciprocamente.

Logo $RSO(2r) = Z[\lambda_1,\ldots,\lambda_{r-1},\lambda_r^+,\lambda_r^-]$.

O cálculo da relação polinomial entre os geradores será feito na próxima secção.

Vamos agora demonstrar o lema 3.3 .

Seja $U \in SO(n)$. A matriz real U pode não possuir nenhum autovalor em R, mas certamente possui um autovalor $c_1 = a_1 + ib_1 \in C$ não nulo, com $|c_1| = 1$, que admite um autovetor $z_1 = x_1 + iy_1$ pertencente ao espaço vetorial complexificado $R^n \otimes C$, com $x_1, y_1 \in R^n$.

Se $c_1 \in R$, podemos escolher z_1 em R^n.

Como $Uz_1 = Ux_1 + iUy_1 = c_1(x_1 + iy_1) = (a_1 + ib_1)(x_1 + iy_1) =$

$$= (a_1x_1 - b_1y_1) + i(a_1y_1 + b_1x_1) \quad ,$$

temos
$$Ux_1 = a_1x_1 - b_1y_1 \quad e \quad Uy_1 = b_1x_1 + a_1y_1 \quad .$$

Seja V_1 o subespaço de R^n gerado por x_1 e y_1, e seja $V_1^\perp$ seu complemento ortogonal relativo ao produto interno canônico:

$$V_1^\perp = \{w \in R^n : \langle w, \alpha x_1 + \beta y_1\rangle = 0,\ \forall\ \alpha,\beta \in R\} \quad .$$

Então $U(V_1) \subset V_1$ e como para qualquer $w \in V_1^\perp$ temos

$$\langle Uw, \alpha x_1 + \beta y_1\rangle = \langle w, \alpha U^t x_1 + \beta U^t y_1\rangle =$$
$$= \langle w, \alpha\,(a_1x_1 + b_1y_1)/(a_1^2 + b_1^2) + \beta(a_1y_1 - b_1x_1)/(a_1^2 + b_1^2)\rangle = 0 \ ,$$

para quaisquer $\alpha,\beta \in R$, concluimos que $U(V_1^\perp) \subset V_1^\perp$.

Por indução sobre n, podemos decompor $V_1^\perp$ em soma direta

$$V_1^\perp = V_2 \oplus \ldots \oplus V_k$$

de subespaços invariantes em relação a U, de dimensões não maiores que 2, mutuamente ortogonais.

Logo $R^n = V_1 \oplus \ldots \oplus V_k$, com $U(V_i) \subset V_i$ e $\dim V_i \leq 2$, para $i = 1,\dots,k$, sendo V_i gerado por elementos x_i e y_i em R^n, como acima.

Consideremos agora o operador linear ortogonal $h: R^n \longrightarrow R^n$ cuja matriz em relação a base canônica do R^n é U.

Seja h_i a restrição de h a V_i, para $i = 1,\dots,k$. Se a dimensão de V_i for 1, V_i é gerado pelo autovetor x_i em R^n, que pode ser considerado com norma 1, e $h_i(x_i) = \pm x_i$. Se a dimensão de V_i for dois, V_i é gerado pelos vetores x_i e y_i do R^n e a matriz de h_i em relação a esta base é

$$\begin{bmatrix} a_i & b_i \\ -b_i & a_i \end{bmatrix}$$

com $a_i^2 + b_i^2 = 1$. Podemos fazer $a_i = \cos\theta_i$, $b_i = \operatorname{sen}\theta_i$, para algum $\theta_i \varepsilon R$.

Como h_i é ortogonal, temos

$$\begin{aligned}\langle h_i(x_i), h_i(y_i)\rangle &= \langle x_i, y_i\rangle = \\ &= a_i b_i \langle x_i, x_i\rangle - a_i b_i \langle y_i, y_i\rangle + (a_i^2 - b_i^2)\langle x_i, y_i\rangle\end{aligned}$$

ou

$$\text{(I)} \quad a_i b_i(\langle x_i, x_i\rangle - \langle y_i, y_i\rangle) = 2b_i^2\langle x_i, y_i\rangle \quad .$$

Se $z_i = x_i + iy_i$, $z_i + iz_i$ também é autovetor correspondente a $a_i + ib_i$, donde

$$a_i b_i(\langle x_i - y_i, x_i - y_i\rangle - \langle x_i + y_i, x_i + y_i\rangle) = 2b_i^2\langle x_i - y_i, x_i + y_i\rangle \ ,$$

e portanto

$$\text{(II)} \quad -2a_i b_i\langle x_i, y_i\rangle = b_i^2(\langle x_i, x_i\rangle - \langle y_i, y_i\rangle) \quad .$$

Desde que neste caso b_i não é nulo, a comparação de (I) e (II) resulta

$$-a_i^2\langle x_i, y_i\rangle = b_i^2\langle x_i, y_i\rangle \quad ,$$

e portanto $\langle x_i, y_i\rangle = 0$. Também $\langle x_i, x_i\rangle = \langle y_i, y_i\rangle$, e podemos considerar $\{x_i, y_i\}$ como base ortonormal de V_i, talvez dividindo x_i e y_i por sua norma.

Então, após talvez reenumerarmos os somandos da decomposição $R^n = V_1 \oplus \ldots \oplus V_k$, a matriz de h em relação a base ortonormal formada pela união das bases consideradas dos somandos diretos será

$$B = \mathrm{Diag}(A(\theta_1),\ldots,A(\theta_s),-1,\ldots,-1,1,\ldots,1) \quad ,$$

onde o número de vezes que o elemento -1 aparece na diagonal é par, uma vez que $\det U = 1$.

Como $\mathrm{Diag}(-1,-1) = A(\pi)$ e $\mathrm{Diag}(1,1) = A(2\pi)$, vemos que B pertence a T. e como B e U são matrizes do mesmo operador h em relação a bases ortonormais, existe $D \in O(n)$ tal que $B = DUD^{-1}$.

Resta mostrar que D pertence a $SO(n)$, ou seja, que $\det U$ é positivo.

As colunas da matriz U (respectivamente B), consideradas como vetores do R^n, formam uma base para o R^n, que denotaremos por $\mathcal{U}$ (respectivamente $\mathcal{B}$).

Se $\mathcal{U}$ e $\mathcal{B}$ tiverem a mesma orientação, o determinante da matriz mudança de base D será positivo.

Se $\mathcal{U}$ e $\mathcal{B}$ não possuirem a mesma orientação, como o operador h preserva orientação, trocamos os dois primeiros vetores da base formada por $x_1,y_1,\ldots,x_k,y_k$ do R^n, obtendo uma nova base em relação a qual a matriz de h é $B' = \mathrm{Diag}(A(-\theta_1),A(\theta_2),\ldots,A(\theta_s),-1,\ldots,-1,1,\ldots,1)$.

Como $\mathcal{U}$ e esta nova base possuem a mesma orientação, existe D' em $SO(n)$ tal que $B' = D'UD'^{-1}$.

Isto demonstra o lema.

4. O grupo Spin(n)

Elie Cartan desenvolveu um método geral para construir representações irredutíveis de O(n) (ou qualquer outro grupo semi-simples) considerando "operações infinitésimais" e encontrou, como alicerces de sua teoria, as representações tensoriais e uma representação independente destas cujos elementos atuantes foram denominados "spinors".

"Spinors" no espaço de quatro dimensões ocorrem nas equações de Dirac para o elétron, sendo as quatro equações de onda as componentes de um "spinor". Dirac mostrou também a conexão entre "spinors" e o grupo de Lorentz, mais tarde tratada matematicamente por van der Waerden.

Cartan estabeleceu as propriedades dos "spinors" estudando apenas ar "rotações infinitesimais". Brauer e Weyl, em 1935, em seu artigo [2], conseguiram simplificar a construção do grupo Spin(n) e a demonstração de suas propriedades, utilizando-se da álgebra de Clifford,obtendo, a partir disto, que as equações de Dirac do movimento de um elétron e a expressão da corrente elétrica são univocamente determinadas, mesmo no caso de dimensão arbitrária.

Definiremos o grupo Spin(n) através da álgebra de Clifford sobre R ou C.

4.1 A álgebra de Clifford An

Consideremos o espaço vetorial real R^n munido da forma quadrática

$$(u,v) = -(u_1v_1 + \dots + u_nv_n) ,$$

onde u_i e v_i são as coordenadas dos vetores u e v do R^n, respectiva mente, em relação a base canônica do R^n.

Tudo o que segue pode também ser feito em relação a qualquer outra forma quadrática.

Sejam $T(R^n)$ a álgebra tensorial de R^n e I o ideal gerado por todos os elementos da forma $u \otimes u - (u,u)$, com $u \in R^n$.

Denotemos por A_n a álgebra quociente $T(R^n)/I$ e seja $\theta\colon R^n \longrightarrow A_n$ a composição da inclusão $i\colon R^n \longrightarrow T^1(R^n) \subset T(R^n)$ com a projeção $p\colon T(R^n) \longrightarrow A_n$.

Então A_n é gerada pela imagem $\theta(R^n)$ e $\theta^2(u) = (u,u)1$, para qualquer $u \in R^n$, onde 1 é a unidade de A_n.

A álgebra real A_n goza da seguinte propriedade universal : para qualquer aplicação linear $h\colon R^n \longrightarrow A$, onde A é uma álgebra real qualquer, tal que

$$h^2(u) = (u,u)1, \quad \forall\, u \in R^n,$$

existe um único homomorfismo de álgebras $h'\colon A_n \longrightarrow A$ com $h' \circ \theta = h$.

De fato, existe $h''\colon T(R^n) \longrightarrow A$, homomorfismo de álgebras reais, tal que $h'' \circ i = h$, por propriedade de $T(R^n)$. Uma vez que $h''(I) = \{0\}$, existe um homomorfismo de álgebras $h'\colon A_n \longrightarrow A$ tal que $h' \circ \theta = h$, como queríamos.

A unicidade de h' decorre do fato de $\theta(R^n)$ gerar A_n.

4.1.1 Definição:

A álgebra A_n, juntamente com a aplicação θ, construida acima, é denominada n-ésima álgebra de Clifford (ou simplesmente álgebra de Clifford) associada a forma quadrática $(\ ,\ )$.

Observemos que a álgebra de Clifford é essencialmente única, uma uma vez que para qualquer outra álgebra A_n' real e qualquer aplicação linear $\theta': R^n \longrightarrow A_n'$ tal que $\theta'^2(u) = (u,u)1$, satisfazendo a propriedade universal considerada acima, existe um isomorfismo de álgebras $f: A_n \longrightarrow A_n'$ tal que $\theta' = f \circ \theta$.

Identifiquemos $\theta(e_i)$ com e_i, para $i = 1,\ldots,n$. Então A_n é gerada por $e_1,\ldots,e_n$, e valem as relações

$$e_i^2 = -1 \ , \quad e_ie_j + e_je_i = 0 \quad (i \neq j) \ ,$$

pois $\quad e_i^2 = \theta^2(e_i) = (e_i,e_i)1 = -1$, e como

$$\theta^2(e_i+e_j) = \theta^2(e_i) + \theta^2(e_j) + \theta(e_i)\theta(e_j) + \theta(e_j)\theta(e_i)$$

e $\quad \theta^2(e_i+e_j) = (e_i+e_j,e_i+e_j)1 = \theta^2(e_i) + \theta^2(e_j)$,

vemos que $\quad e_ie_j + e_je_i = 0$.

Considerada como espaço vetorial sobre R, A_n tem uma base constituida pelos 2^n monômios $e_1^{i_1}\ldots e_n^{i_n}$, onde os expoentes valem 0 ou 1.

A demonstração deste resultado não será apresentada aqui. Encontra-se, por exemplo, em [6].

Mais tarde desejaremos utilizar a álgebra de Clifford sobre os complexos e então denotaremos por $A_n \otimes C$ a álgebra complexificada.

Denotemos por A_n^+ o subespaço vetorial de A_n gerado por 1 e por todos os monômios $e_{i_1}\ldots e_{i_k}$, com k par, e por A_n^- o subespaço vetorial de A_n gerado por todos os monômios $e_{i_1}\ldots e_{i_k}$, com k ímpar.

Então $A_n = A_n^+ \oplus A_n^-$ e dizemos que A_n é uma álgebra graduada.

Na verdade, A_n^+ é subálgebra de A_n e A_{n-1} é isomorfa a A_n^+. Um isomorfismo de álgebras é dado por

$$A_{n-1} = A_{n-1}^{+} \oplus A_{n-1}^{-} \longrightarrow A_n^{+}$$
$$a \oplus b \longmapsto a + be_n$$

Fixemos os 2^n elementos básicos $e_1^{i_1}\ldots e_n^{i_n}$ de A_n numa certa ordem. Então, para cada $x \in A_n$, podemos representar o operador linear

$$L(x): A_n \longrightarrow A_n$$
$$y \longmapsto xy$$

por uma matriz real de ordem 2^n, que denotaremos também por $L(x)$.

Como espaço vetorial real, A_n é isomorfa a R^{2^n}, e então podemos muni-la de uma topologia simplesmente transportando a A_n a topologia usual do R^{2^n}, de modo que o isomorfismo se torne um homeomorfismo.

As operações de adição, multiplicação e produto por escalar são contínuas e se denotarmos A_n^* o grupo multiplicativo dos elementos inversíveis de A_n, com a topologia induzida, então a operação que a cada x em A_n^* associa seu inverso x^{-1} em A_n^* também é contínua.

Esta última afirmação pode ser verificada considerando, para cada $x \in A_n^*$, o isomorfismo de espaços vetoriais $L(x): A_n \longrightarrow A_n$, e verificando que x^{-1} é solução única da equação matricial

$$L(x).[y] = [1] \ ,$$

onde $[y]$ e $[1]$ representam as matrizes de y e 1 em relação a base de A_n considerada acima, respectivamente.

Então A_n^* é grupo topológico.

4.1.2 A exponencial em A_n

A aplicação L que a cada $x \in A_n$ associa a matriz real $L(x)$ é homeomorfismo de A_n sobre algum subespaço do espaço vetorial de todas as matrizes reais de ordem 2^n, pois $L(x).1 = x$, mostrando que os coeficientes de x também são coeficientes de alguma coluna da matriz $L(x)$.

Temos $L(1 + x + x^2/2 + \ldots + x^m/m!) =$

$$= L(1) + L(x) + (1/2)L(x)^2 + \ldots + (1/m!)L(x)^m \quad .$$

Se m tende ao infinito, o lado direito da igualdade acima tende a $\exp L(x)$. Para a definição e propriedades da exponencial de matrizes, vide, por exemplo, [4] .

Desta forma, como L é homeomorfismo de A_n sobre sua imagem, $1 + x + x^2/2 + \ldots + x^m/m!$, para qualquer x em A_n, tende a um único elemento de A_n, que denotaremos por $\exp x$, satisfazendo a

$$L(\exp x) = \exp L(x) \quad .$$

Temos $\exp(x + y) = \exp x \exp y$, para quaisquer x e y em A_n com $xy = yx$. Em particular, $\exp(-x) = (\exp x)^{-1}$, donde $\exp x \in A_n^*$.

Para cada $x \in A_n^*$, o operador linear $\psi(x)$ de A_n que a cada $y \in A_n$ associa $xyx^{-1} \in A_n$ pode ser representado por uma matriz real de ordem 2^n que denotaremos também por $\psi(x)$.

4.1.3. Lema:

Para qualquer $x \in A_n$, $\psi(\exp x) = \exp X(x)$, onde $X(x)$ é a matriz do operador linear

$$\begin{aligned} X(x):\ & A_n \longrightarrow A_n \\ & y \longmapsto xy-yx \end{aligned} \quad .$$

Prova:

Sejam $y_0 \in A_n$ e $y(t) = (\exp tx)y_0\exp(-tx)$, para qualquer $t \in R$.

Temos $y(t + h) = \exp(hx)y(t)\exp(-hx) = (1+hx+\ldots)y(t)(1-hx+\ldots)$, donde $dy/dt = \lim_{h \to 0} (1/h)(y(t+h) - y(t)) = xy(t) - y(t)x = X(x)y(t)$.

Esta equação diferencial é equivalente a um sistema de 2^n equações diferenciais lineares homogêneas nos coeficientes de $y(t)$ cuja solução é dada por $y(t) = (\exp tX(x))y_0$.

Logo $\exp tx = \exp tX(x)$, para qualquer $t \in R$.

Isto demonstra o lema.

4.1.4 Lema:

Um elemento $a \in A_n^+$ comuta com todos os elementos de A_n se e somente se for múltiplo real da unidade 1 de A_n.

Prova:

Seja $a = \Sigma\, t_{i_1 \ldots i_n} e_1^{i_1} \ldots e_n^{i_n}$, onde a somatória é efetuada sobre todas as n-uplas $i_1, \ldots, i_n$, com i_j igual a 0 ou 1 e $i_1 + \ldots + i_n$ é par.

Temos $e_r a e_r^{-1} = \Sigma\, (-1)^{i_r}\, t_{i_1 \ldots i_n} e_1^{i_1} \ldots e_n^{i_n}$ pois

$$e_r e_1^{i_1} \ldots e_n^{i_n} e_r^{-1} = (-1)^{i_1 + \ldots + i_{r-1} + i_{r+1} + \ldots + i_n} e_1^{i_1} \ldots e_{r-1}^{i_{r-1}} e_r^{i_r} e_{r+1}^{i_{r+1}} \ldots e_n^{i_n}$$
$$= (-1)^{i_r} e_1^{i_1} \ldots e_n^{i_n} \quad ,$$

já que $i_1 + \ldots + i_n$ é par.

Então se a comuta com $e_1, \ldots, e_n$, devemos ter

$$t_{i_1 \ldots i_n} = (-1)^{i_1} t_{i_1 \ldots i_n} = \ldots = (-1)^{i_n} t_{i_1 \ldots i_n}$$

e portanto $t_{i_1 \ldots i_n} = 0$ para $(i_1, \ldots, i_n) \neq (0, \ldots, 0)$.

Logo $a = t_{0 \ldots 0}\, 1$.

A recíproca é trivial.

4.2 O grupo Spin(n)

Denotemos por R^n o subespaço vetorial de A_n gerado por e_1, ..., e_n.

Seja $S^{n-1} \subset A_n^-$ a esfera unitária constituida por todos os elementos da forma $t_1e_1+\ldots+t_ne_n$, com os reais t_i satisfazendo a condição $t_1^2+\ldots+t_n^2 = 1$.

Se $u = t_1e_1 +\ldots+ t_ne_n$ e $v = s_1e_1 +\ldots+ s_ne_n$ são elementos de A_n^-, a identidade $uv+vu = -2(t_1s_1+\ldots+t_ns_n)\,1$ mostra que u e v anticomutam se e somente se são ortogonais no sentido de que $t_1s_1+\ldots+t_ns_n= 0$.

Se u pertencer a S^{n-1}, a igualdade acima para $u = v$ reduz-se a $u^2 = -1$, e portanto u é inversível com inverso igual a $-u$.

Estamos agora em condições de definir o grupo Spin(n). É conveniente definir antes um grupo maior denominado pin(n).

4.2.1 Definição:

Denominaremos pin(n) ao subgrupo multiplicativo de A_n^* gerado por todos os elementos da esfera unitária S^{n-1}.

Cada elemento a pin(n) pode ser escrito como um produto de elementos de S^{n-1}:

$$a = u_1\ldots u_k \quad .$$

Se $x = \Sigma\, t_{i_1\ldots i_n} e_1^{i_1}\ldots e_n^{i_n}$ é um elemento genérico de A_n, denotamos por x^* o elemento $\Sigma\, t_{i_1\ldots i_n} e_n^{i_1}\ldots e_1^{i_n}$.

No caso de $a = u_1\ldots u_k$ pertencer a pin(n), com $u_i \in S^{n-1}$, temos $a^*= u_k\ldots u_1$, donde concluimos que $a \in A_n^+$ se e somente se $aa^*= 1$ e $a \in A_n^-$ se e somente se $aa^*= -1$.

4.2.2. Definição:

4.2.2 Definição:

O grupo Spin(n) é o subgrupo de pin(n) constituido por todos os elementos $a \in pin(n)$ com $aa^* = 1$.

Em outros termos, $Spin(n) = A_n^+ \cap pin(n)$.

A topologia induzida de A_n^* torna Spin(n) um grupo topológico.

4.2.3 Proposição:

O grupo Spin(n) é conexo por caminhos, para $n \geq 2$.

Prova:

Se $n = 1$, S^0 é o conjunto $\{-e_1, e_1\}$ e Spin(1) é igual a $\{-1,1\}$, ambos desconexos.

Para $n \geq 2$, claramente S^{n-1} é conexo por caminhos, implicando no resultado.

De fato, se $a = u_1 \ldots u_{2r}$ pertence a Spin(n), com $u_i \in S^{n-1}$, suponhamos r par. Então existem caminhos contínuos $\alpha_1, \ldots, \alpha_{2r} : [0,1] \longrightarrow S^{n-1}$ ligando $u_1, \ldots, u_{2r}$ a e_1, respectivamente.

O caminho $\alpha : [0,1] \longrightarrow Spin(n)$ dado por $\alpha(t) = \alpha_1(t) \ldots \alpha_{2r}(t)$ é contínuo e liga $u_1 \ldots u_{2r}$ a $(-1)^r 1 = 1$.

No caso de r ser ímpar, existem caminhos contínuos $\alpha_2, \ldots, \alpha_{2r} : [0,1] \longrightarrow S^{n-1}$ unindo $u_2, \ldots, u_{2r}$ a e_1, respectivamente, e $\alpha_1 : [0,1] \longrightarrow S^{n-1}$ unindo u_1 a $-e_1$.

O mesmo procedimento do caso anterior fornece um caminho unindo $u_1 \ldots u_{2r}$ a $-(-1)^r 1 = 1$, como queríamos.

Nosso objetivo agora será mostrar que Spin(n) é espaço de re - vestimento de SO(n).

Para cada $a \in pin(n)$ e $v \in R^n$, mostremos que ava^* pertence a R^n. Basta considerar $a = u = u_1e_1+\ldots+u_ne_n$ em S^{n-1}.

Pensando em R^n como espaço vetorial euclidiano com o produto interno canônico, podemos decompor qualquer elemento $v = v_1e_1+\ldots+v_ne_n$ do R^n como uma soma $v = tu + v'$, com t real e v' em R^n. Basta fazer $t = u_1v_1+\ldots+u_nv_n$ e $v' = v - tu$.

Logo $uvu^* = uvu = u(tu + v')u = u(tu^2 + v'u) =$

$$= u(tu^2 - uv') = u^2(tu - v') = -tu + v' ,$$

mostrando que uvu^* pertence a R^n .

Podemos então, para cada a em pin(n), definir o operador linear

$$\begin{aligned} \phi_1(a): R^n &\longrightarrow R^n \\ v &\longmapsto ava^* \end{aligned} .$$

Mostramos acima que, para $u \in S^{n-1}$, $\phi_1(u)$ é uma reflexão do R^n em relação ao hiperplano perpendicular a u.

Seja $O(n)$ o grupo topológico de todas as transformações ortogonais do R^n. Como composição de reflexões é uma transformação ortogonal, $\phi_1(a)$ pertence a $O(n)$, para qualquer a em pin(n).

Definimos então o homomorfismo contínuo de grupos ϕ_1 de pin(n) em $O(n)$ que a cada a em pin(n) associa a transformação ortogonal $\phi_1(a)$.

Como cada transformação ortogonal do R^n pode ser expressa como produto de reflexões, o argumento anterior mostra que ϕ_1 é um epimorfismo.

Se $a = u_1\ldots u_k$ pertence a pin(n), temos $\det \phi_1(a) = (-1)^k$, uma vez que $\det \phi_1(u) = -1$ para todo u em S^{n-1}.

Isto mostra que $a \in Spin(n)$ se e somente se $\phi_1(a) \in SO(n)$. Logo $\phi_1^{-1}(SO(n)) = Spin(n)$.

Denotemos por ϕ a restrição de ϕ_1 a $Spin(n)$:

$$\phi \colon Spin(n) \longrightarrow SO(n) \qquad .$$

É claro que, para todo $a \in Spin(n)$, $\phi(a)$ é a retrição a R^n do operador $\psi(a)$.

Determinemos agora o núcleo do epimorfismo ϕ.

Temos $a \in \ker\phi$ se e somente se $\phi(a)e_i = e_i$, ou seja, $ae_i a^* = e_i$, para todo $i = 1,\ldots,n$. Como $a^* = a^{-1}$, isto é equivalente a $ae_i = e_i a$, ou seja, a comuta com todos os elementos de A_n .

Pelo lema 4.1.4, $a \in \ker\phi$ se e somente se $a = t1$, com $t \in R$. Como $aa^* = 1$, temos $t^2 = 1$, ou seja, $a = \pm 1$.

Então $\ker\phi = \{-1,+1\}$.

Voltemos ao estudo da exponencial.

Seja M o subespaço vetorial de A_n gerado por todos os elementos $e_i e_j$, com $i \neq j$. Sua dimensão é $n(n-1)/2$. Como todo subespaço vetorial de R^{2^n} é completo, exp x pertence a A_n^+ para todo x em A_n^+ .

Seja $x = \sum_{i<j} a_{ij} e_i e_j$ em M. Temos $X(x)\colon A_n \longrightarrow A_n$ dado por $X(x)(y) = xy - yx$ e como

$$X(e_i e_j)e_k = \begin{cases} 0 & \text{se } k \neq i,j \\ 2e_j & \text{se } k = i \\ -2e_i & \text{se } k = j \end{cases}$$

concluimos que

$$X(x)(R^n) \subset R^n, \quad \forall\, x \in M \quad .$$

Um cálculo direto mostra que, neste caso, a matriz de $X(x)$ em relação a base canônica do R^n é

$$[X(x)|R^n] = \begin{bmatrix} 0 & -2a_{12} & -2a_{13} & \dots & -2a_{1n} \\ 2a_{12} & 0 & -2a_{23} & \dots & -2a_{2n} \\ 2a_{13} & 2a_{23} & 0 & \dots & -2a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 2a_{1n} & 2a_{2n} & 2a_{3n} & \dots & 0 \end{bmatrix} .$$

Como $\psi(\exp x) = \exp X(x)$, segue-se que para todo x em M temos $\psi(\exp x)(R^n) \subset R^n$. Ainda $\det(\psi(\exp x)|R^n) = \det(\exp X(x)|R^n) =$

$$= \exp \text{traço}(X(x)|R^n) = 1 .$$

O operador linear $\psi(\exp x)|R^n\colon R^n \dashrightarrow R^n$ é ortogonal.

De fato, se $\psi(\exp x)(e_i) = \sum_{j=1}^{n} b_{ji} e_j$, temos

$$\psi(\exp x)\Big(\sum_{i=1}^{n} x_i e_i\Big) = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} x_i b_{ji}\Big) e_j .$$

Por outro lado,

$$\psi(\exp x)\Big(\Big(\sum_{i=1}^{n} x_i e_i\Big)^2\Big) = \psi(\exp x)\Big(\sum_{i=1}^{n} x_i e_i\Big) . \psi(\exp x)\Big(\sum_{i=1}^{n} x_i e_i\Big)$$

$$= -\sum_{j=1}^{n}\Big(\sum_{i=1}^{n} x_i a_{ji}\Big)^2 1)$$

e como $\psi(\exp x)\Big(\Big(\sum_{i=1}^{n} x_i e_i\Big)^2\Big) = \psi(\exp x)\Big(-\sum_{i=1}^{n} x_i^2 1\Big) = -\sum_{i=1}^{n} x_i^2\, 1$,

concluimos que

$$\sum_{i=1}^{n} x_i^2 = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} x_i b_{ji}\Big)^2 .$$

Como a última igualdade se verifica para qualquer valor de x_i, $i = 1,\dots,n$, temos

$$\sum_{j=1}^{n} b_{ji}^2 = 1 \quad \text{e} \quad \sum_{j=1}^{n} b_{ji} b_{jk} = 0 \quad \text{para} \quad i \neq k ,$$

mostrando que realmente $\psi(\exp x)|R^n$ é ortogonal.

Logo $\psi(\exp x)|R^n \in SO(n)$, para qualquer $x \in M$.

Como $\phi\colon Spin(n) \dashrightarrow SO(n)$ é sobre, existe $a \in Spin(n)$ tal que $\phi(a) = \psi(\exp x)|R^n$, ou seja, tal que

$$a e_i a^* = (\exp x) e_i (\exp -x) , \quad i = 1,\dots,n .$$

Como $(a^*\exp x)e_i = e_i(a^*\exp x)$, $a^*\exp x$ pertencente a A_n^+ comuta com todos os elementos de A_n, Pelo lema 4.1.4, existe k real com $a^*\exp x = k1$, ou seja, $\exp x = ka$, e como

$$1 = \exp x \exp -x = \exp x \exp x^* = (\exp x)(\exp x)^* =$$
$$= ka\, ka^* = k^2\, 1,$$

concluimos que $k = \pm 1$, donde $\exp x$ pertence a $\mathrm{Spin}(n)$, para qualquer $x \varepsilon M$.

Seja $X_1(x)$ a restrição de $X(x)$ a R^n, para x em M.Temos $X_1^t(x) = -X_1(x)$ e $X_1(x) = 0$ implica em $x = 0$.

Então a aplicação X_1 de M no espaço das matrizes reais anti-simétricas de grau n que a cada $x \varepsilon M$ associa $X_1(x)$ é linear injetora e portanto um isomorfismo bicontínuo, pois a dimensão do espaço vetorial das matrizes anti-simétricas de grau n é também $n(n-1)/2$.

Mostremos que ϕ: $\mathrm{Spin}(n) \dashrightarrow SO(n)$ é aberta.

Seja V uma vizinhança de 1 em A_n. Então $V \cap \mathrm{Spin}(n)$ é vizinhança de 1 em $\mathrm{Spin}(n)$. Como $\exp$ é contínua, existe U, vizinhança de 0 em M, tal que $\exp U \subset V \cap \mathrm{Spin}(n)$.

Como $\exp X_1(U)$ é vizinhança do elemento neutro de $SO(n)$, por propriedade da exponencial de matrizes e por X_1 ser homeomorfismo, concluimos que $\phi(V \cap \mathrm{Spin}(n))$ é vizinhança do elemento neutro do $SO(n)$, uma vez que $\exp X_1(U) = \phi(\exp U) \subset (V \cap \mathrm{Spin}(n))$.

Consequentemente ϕ é aberta.

4.2.4 Teorema:

A aplicação $\phi: \mathrm{Spin}(n) \dashrightarrow SO(n)$ é aplicação de revestimento.

Prova:

Para qualquer $y \in SO(n)$, existe $x \in Spin(n)$ com $\phi(x) = y$, e podemos encontrar um aberto U em $Spin(n)$ com $x \in U$ e $U \cap (-U) = \Phi$.

Como $\phi|U: U \longrightarrow \phi(U)$ e $\phi|-U: -U \longrightarrow \phi(U)$ são homeomorfismos de U e de $-U$ sobre o aberto $\phi(U)$, respectivamente, concluimos que ϕ é aplicação de revestimento.

4.2.5 Corolário:

O grupo $Spin(n)$ é compacto.

Prova:

Seja $\{x_n\}$ um conjunto infinito de pontos de $Spin(n)$. Então $\{\phi(x_n)\}$ é um conjunto infinito de pontos de $SO(n)$ e portanto tem ponto de acumulação y pois $SO(n)$ é compacto.

Existe x em $Spin(n)$ com $\phi(y)^{-1} = \{x,-x\}$. Se ambos x e $-x$ não forem pontos de acumulação de $\{x_n\}$, podemos encontrar uma vizinhança aberta V de x em $Spin(n)$ tal que V e $-V$ não contenham pontos de $\{x_n\}$ distintos de x e de $-x$.

Logo $\phi(V)$ é vizinhança aberta de y que não contém nenhum ponto de $\{\phi(x_n)\}$ distinto de $\phi(x)$, o que é absurdo.

4.3 O anel de representação de Spin(n)

Vamos agora estudar as representações do grupo $Spin(n)$.

Como $\phi: Spin(n) \longrightarrow SO(n)$ induz um homomorfismo de anéis $R\phi: RSO(n) \longrightarrow RSpin(n)$, cada $SO(n)$-módulo origina um $Spin(n)$-módulo, com $+1$ e -1 atuando como identidade.

Por outro lado, fazendo $Spin(n)$ atuar sobre o espaço vetorial real A_n^+ por multiplicação a esquerda

$$\begin{aligned} \mathrm{Spin}(n) \times A_n^+ &\longrightarrow A_n^+ \\ (u\ ,\ v) &\longmapsto uv \end{aligned}$$

obtemos uma representação real que não provém de $SO(n)$, uma vez que -1 em $\mathrm{Spin}(n)$ é representado por uma aplicação linear não trivial.

Vamos agora classificar os módulos a esquerda sobre a álgebra de Clifford, definidos como usualmente.

Como A_n^+ é isomorfo a A_{n-1}, podemos considerar A_n^+-módulos, e qualquer A_n^+-módulo origina, de modo natural, um $\mathrm{Spin}(n)$-módulo.

Em tudo o que segue, $A_n \otimes C$ será a álgebra de Clifford complexificada.

4.3.1 Teorema:

Cada $A_n \otimes C$-módulo M se decompõe como soma direta de $A_n \otimes C$-módulos irredutíveis.

Para $n = 2k$, existe exatamente um $A_n \otimes C$-módulo irredutível, a menos de isomorfismos. Tem dimensão complexa 2^k.

Para $n = 2k - 1$, existem dois $A_n \otimes C$-módulos irredutíveis distintos, cada qual com dimensão 2^{k-1}.

Prova:

Vamos utilizar indução sobre n.

Para $n = 0$, é claro que todo $A_0 \otimes C$-módulo irredutível é isomorfo a C.

Seja $n = 2k - 1$ e suponhamos por hipótese de indução, que o teorema se verifique para $n - 1$:
existe exatamente um $A_{n-1} \otimes C$-módulo irredutível, a menos de isomorfismos, com dimensão complexa 2^{k-1}.

Seja M um $A_n \otimes C$-módulo. O elemento $t = i^k e_1 \dots e_n$ pertence ao centro da álgebra $A_n \otimes C$, pois

$$e_j t = -(-1)^{j-1} i^k e_1 \dots e_{j-1} e_{j+1} \dots e_n \qquad \text{e}$$
$$t e_j = -(-1)^{n-j} i^k e_1 \dots e_{j-1} e_{j+1} \dots e_n \qquad .$$

Como n é ímpar, temos $e_j t = t\, e_j$. Ainda $t^2 = 1$.

Podemos então decompor M como soma direta $M = M^+ \oplus M^-$, onde M^+ e M^- são submódulos de M com t atuando como identidade em M^+ e como multiplicação por -1 em M^-.

Pensando em M^+ e M^- como $A_{n-1} \otimes C$-módulos, a hipótese de indução garante que M^+ e M^- são somas diretas de $A_{n-1} \otimes C$-submódulos irredutíveis, todos isomorfos entre si e de dimensão 2^{k-1}:

$$M^+ = I_1^+ \oplus \dots \oplus I_r^+ \quad \text{e} \quad M^- = I_1^- \oplus \dots \oplus I_s^- \qquad .$$

Como para $m \in M^{\pm}$ temos

$$\begin{aligned} e_n m &= e_n 1 m = e_n t(tm) = i^k e_n e_1 \dots e_n (tm) = \\ &= i^k (-1)^n e_1 \dots e_{n-1}(tm) = -i^k e_1 \dots e_{n-1}(tm) = \\ &= \mp i^k e_1 \dots e_{n-1} m \,, \end{aligned}$$

concluimos que cada $I_j^{\pm}$ é também um $A_n \otimes C$-módulo irredutível.

É claro que I_j^+ (respec. I_j^-) é isomorfo como $A_n \otimes C$-módulo a I_i^+(respec. I_i^+), mas o mesmo não acontece com I_j^+ e I_i^-, uma vez que

$$e_n m = -\, i^k e_1 \dots e_{n-1} m \,, \text{ se } m \in I_j^+$$
e
$$e_n m = +\, i^k e_1 \dots e_{n-1} m \,, \text{ se } m \in I_i^- \qquad .$$

Agora consideremos um $A_{n+1} \otimes C$-módulo M.

Pensando em M como um $A_n \otimes C$-módulo, podemos decompô-lo em $M = M^+ \oplus M^-$, como acima.

O elemento $e_{n+1} \in A_{n+1} \otimes C$ anti-comuta com $t = i^k e_1 \ldots e_n$, donde $e_{n+1} M^+ \subset M^-$ e $e_{n+1} M^- \subset M^+$.

Seja $M^+ = I_1^+ \oplus \ldots \oplus I_r^+$ a decomposição de M^+ em $A_n \otimes C$- módulos irredutíveis.

Como todo $m \in M^-$ pode ser escrito como

$$m = e_{n+1}(-e_{n+1} m) ,$$

com $(-e_{n+1} m) \in M^+$, vemos que $e_{n+1} M^+ = M^-$.

Fazendo $I_j = I_j^+ \oplus e_{n+1} I_j^+$, obtemos um $A_{n+1} \otimes C$-módulo irredutível de dimensão 2^k, e $M = I_1 \oplus \ldots \oplus I_r$. É claro que os módulos $I_1, \ldots, I_r$ são isomorfos entre si como $A_{n+1} \times C$-módulos, uma vez que $I_1^+, \ldots, I_r^+$ o são como $A_n \times C$-módulos.

Isto completa a indução, demonstrando o teorema.

Como Spin(2r+1) está contido em $A_{2r+1}^+ \otimes C$, que é isomorfa a $A_{2r} \otimes C$, cada $A_{2r} \otimes C$-módulo determina um Spin(2r+1)-módulo.

Pelo teorema anterior, existe exatamente um módulo irredutível sobre $A_{2r+1}^+ \otimes C$ e a representação proveniente deste módulo em RSpin(2r+1) será denotada por Δ.

Da mesma forma, Spin(2r) está contido em $A_{2r}^+ \otimes C$, que é isomorfa a $A_{2r-1} \otimes C$, e existem exatamente dois $A_{2r-1} \otimes C$-módulos irredutíveis. Os elementos de RSpin(2r) provenientes destes dois módulos serão denotados por Δ^+ e Δ^-.

Mais especificamente, Δ^+ corresponde ao módulo onde $i^r e_1 \ldots e_{2r}$ pertencente a Spin(2r) (que corresponde a $t = i^r e_1 \ldots e_{2r-1} \in A_{2r-1} \otimes C$ através do isomorfismo entre $A_{2r-1} \otimes C$ e $A_{2r}^+ \otimes C$ dado na página 61) atu a como multiplicação por $+1$, e Δ^- corresponde ao módulo onde $i^r e_1 \ldots e_{2r}$ atua como multiplicação por -1.

Vamos agora determinar um toro maximal em $Spin(n)$ e seu grupo de Weyl.

Consideremos $n = 2r$ ou $2r+1$.

Para cada $j = 1,\ldots,r$, seja $w_j: R/2\pi Z \longrightarrow Spin(n)$ o homomorfismo de grupos dado por

$$w_j(\overline{\theta}) = \cos\theta \; 1 - \operatorname{sen}\theta \; e_{2j-1}e_{2j} \quad , \quad \forall\, \overline{\theta} \in R/2\pi Z.$$

É trivial verificar que w_j está bem definido e é realmente um homomorfismo.

Um cálculo direto mostra que

$$w_j(\overline{\theta})\, e_k\, w_j(\overline{\theta})^* = \begin{cases} e_k & \text{se } k \neq 2j-1, 2j \\ \cos 2\theta\; e_{2j-1} - \operatorname{sen} 2\theta\; e_{2j} & \text{se } k = 2j-1 \\ \operatorname{sen} 2\theta\; e_{2j-1} + \cos 2\theta\; e_{2j} & \text{se } k = 2j \end{cases}.$$

Isto mostra que $\phi w_j(\overline{\theta}) = \operatorname{Diag}(\underbrace{1,\ldots,1}_{2j-2}, A(2\theta), 1, \ldots, 1)$, pertencente a $SO(n)$.

Temos também $w_j(\overline{\theta+\pi}) = -w_j(\overline{\theta})$.

Podemos então definir um homomorfismo w do r-ésimo toro Tr em $Spin(n)$ através de

$$w(\overline{\theta}_1,\ldots,\overline{\theta}_r) = w_1(\overline{\theta}_1)\ldots w_r(\overline{\theta}_r),$$

e obtemos $\phi w(\overline{\theta}_1,\ldots,\overline{\theta}_r)$ igual a $\operatorname{Diag}(A(2\theta_1),\ldots,A(2\theta_r))$ se $n = 2r$, ou $\operatorname{Diag}(A(2\theta_1),\ldots,A(2\theta_r),1)$ se $n = 2r+1$.

Usaremos a notação $\operatorname{Diag}(A(\theta_1),\ldots,A(\theta_r),*)$ indistintamente para $\operatorname{Diag}(A(\theta_1),\ldots,A(\theta_r))$ e $\operatorname{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$.

Calculemos o núcleo de w. Temos $w(\overline{\theta}_1,\ldots,\overline{\theta}_r) = 1$ se e somente se

$$(\cos\theta_1\, 1 - \operatorname{sen}\theta_1 e_1 e_2)\ldots(\cos\theta_r\, 1 - \operatorname{sen}\theta_r e_{2r-1}e_{2r}) = 1 =$$

$$= \cos\theta_1\cos\theta_2\ldots\cos\theta_r\, 1 - \operatorname{sen}\theta_1\cos\theta_2\ldots\cos\theta_r e_1 e_2 -$$

$$- \cos\theta_1\operatorname{sen}\theta_2\cos\theta_3\ldots\cos\theta_r e_3 e_4 - \ldots - \cos\theta_1\ldots\cos\theta_{r-1}\operatorname{sen}\theta_r e_{2r-1}e_{2r} + \ldots$$

e portanto se e somente se

$$\cos\theta_1\cos\theta_2\ldots\cos\theta_r = 1 \quad \text{e} \quad \operatorname{sen}\theta_1 = \ldots = \operatorname{sen}\theta_r = 0.$$

Concluimos então que $w(\overline{\theta}_1,\ldots,\overline{\theta}_r) = 1$ se e somente se existem inteiros $k_1,\ldots,k_r$ tais que $\theta_i = 2k_i\pi$, $i = 1,\ldots,r$, ou $\theta_i = k_i\pi$, $i = 1,\ldots,r$, com $k_1+\ldots+k_r$ par.

Do mesmo modo, $w(\overline{\theta}_1,\ldots,\overline{\theta}_r) = -1$ se e somente se existem inteiros $k_1,\ldots,k_r$ tais que $\theta_i = k_i\pi$, $i = 1,\ldots,r$, com $k_1+\ldots+k_r$ ímpar.

Seja $T' = w(Tr)$. Então T' é abeliano, e como w é contínuo, T' é compacto e conexo. Uma vez que $\mathrm{Spin}(n)$ é um grupo de Lie, pode-se mostrar que T' é um toro. (Vide [4].)

4.3.2 Proposição:

O subgrupo $T' = w(Tr)$ é um toro maximal de $\mathrm{Spin}(n)$.

Prova:

Seja $T_{SO(n)}$ o toro maximal de $SO(n)$ considerado em §3.

Vimos que $\phi\circ w(Tr) \subset T_{SO(n)}$.

Mostremos que $\phi^{-1}(T_{SO(n)}) \subset T'$. Então, como ϕ é sobre, teremos $\phi(T') = T_{SO(n)}$.

Se $y \in \phi^{-1}(T_{SO(n)})$, temos $\phi(y) \in T_{SO(n)}$ e então $\phi(y) = \mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r))$ se $n = 2r$ ou $\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),1)$ se $n = 2r+1$. Portanto existe $(\overline{\theta}_1/2,\ldots,\overline{\theta}_r/2) \in Tr$ tal que

$$\phi\circ w(\overline{\theta}_1/2,\ldots,\overline{\theta}_r/2) = \phi(y) .$$

Seja $x = w(\overline{\theta}_1/2,\ldots,\overline{\theta}_r/2) \in T'$. Como $\ker\phi = \{-1,+1\}$, temos

$$y = x \quad \text{ou } y = -x = w(\overline{\theta}_1/2 + \pi, \overline{\theta}_2/2,\ldots,\overline{\theta}_r/2)$$

e portanto em qualquer caso y pertence a T'.

Isto mostra que $\phi(T') = T_{SO(n)}$.

Como $x \in T'$ implica $-x \in T'$, dado $y \in SO(n)$, temos $\phi^{-1}(yT_{SO(n)}y^{-1}) = uT'u^{-1}$, com $u \in \phi^{-1}(y)$, e portanto

$$\begin{aligned} Spin(n) &= \phi^{-1}(SO(n)) = \phi^{-1}\Big(\bigcup_{y\in SO(n)} yT_{SO(n)}y^{-1}\Big) = \\ &= \bigcup_{y\in SO(n)} \phi^{-1}(yT_{SO(n)}y^{-1}) = \bigcup_{u\in Spin(n)} uT'u^{-1} . \end{aligned}$$

Isto completa a demonstração.

4.3.3 Proposição:

O grupo de Weyl de Spin(n) em relação a T' é o mesmo que de $SO(n)$ em relação a $T_{SO(n)}$.

Prova:

Seja $N_{T'}$ o normalizador de T' em Spin(n). Se $x \in N_{T'}$, temos $\phi(x)\phi(T')\phi(x^{-1}) = \phi(T')$, donde $\phi(x)T_{SO(n)}\phi^{-1}(x) = T_{SO(n)}$,ou seja, $\phi(x)$ pertence a $N_{T_{SO(n)}}$. Assim $\phi(N_{T'}) \subset N_{T_{SO(n)}}$, ou $N_{T'} \subset \phi^{-1}(N_{T_{SO(n)}})$.

Como $\phi(uT'u^{-1}) = \phi(T')$ implica em $uT'u^{-1} = T'$, concluimos que $\phi^{-1}(N_{T_{SO(n)}}) \subset N_{T'}$. Mostramos assim que $N_{T'} = \phi^{-1}(N_{T_{SO(n)}})$, ou $N_{T_{SO(n)}} = \phi(N_{T'})$.

Considerando os epimorfismos restrições de ϕ a T' e a $N_{T'}$, temos

$$T'/\ker\phi \cong T_{SO(n)} \quad \text{e} \quad N_{T'}/\ker\phi \cong N_{T_{SO(n)}} .$$

Então $N_{T_{SO(n)}}/T_{SO(n)} \cong N_{T'}/T'$,mostrando que os grupos de Weyl coincidem.

Os homomorfismos de grupos $w\colon Tr \dashrightarrow T'$ e $\phi\colon T' \dashrightarrow T_{SO(n)}$ induzem os homomorfismos de anéis $R\phi\colon RT_{SO(n)} \dashrightarrow RT'$ e $Rw\colon RT' \dashrightarrow RTr$.

Como w e ϕ são epimorfismos, o teorema 3.17 do capítulo I garante que Rw, $R\phi$ e $R(\phi\circ w)$ têm núcleo nulo.

Sabemos que $RT_{SO(n)} = Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}]$, onde α_j é a classe dos $T_{SO(n)}$-módulos isomorfos a C com a atuação que a cada par $(\mathrm{Diag}(A(\theta_1),\ldots,A(\theta_r),*),z)$ em $T_{SO(n)} \times C$ associa $e^{i\theta_j}z$ em C.

Então $R(\phi\circ w)(\alpha_j)$ é o Tr-módulo C com a atuação que a cada par $((\overline{\theta}_1,\ldots,\overline{\theta}_r),z)$ em $Tr \times C$ associa o elemento

$$(\overline{\theta}_1,\ldots,\overline{\theta}_r).z = (\phi\circ w)(\overline{\theta}_1,\ldots,\overline{\theta}_r).z = \mathrm{Diag}(A(2\theta_1),\ldots,A(2\theta_r),*).z = \\ = e^{i2\theta_j}\, z \quad .$$

Podemos então considerar $R(\phi\circ w)$ como a inclusão

$$R(\phi\circ w)\colon RT_{SO(n)}=Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}] \dashrightarrow RT_r=Z[\alpha_1^{1/2},\alpha_1^{-1/2},\ldots,\alpha_r^{1/2},\alpha_r^{-1/2}].$$

Como Rw é injetor, podemos considerar RT' como subanel de $RTr = Z[\alpha_1^{1/2},\alpha_1^{-1/2},\ldots,\alpha_r^{1/2},\alpha_r^{-1/2}]$.

4.3.4 Proposição:

O anel RT' é igual a $Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1},(\alpha_1\ldots\alpha_r)^{1/2}]$.

Prova:

Lembremos que $\ker w$ é o conjunto de todos os elementos $(\overline{\theta}_1,\ldots,\overline{\theta}_r)$ em Tr tais que existem $k_1,\ldots,k_r$ inteiros com $\theta_i = k_i\pi$ e $k_1 + \ldots + k_r$ par. Então qualquer elemento de $\ker w$ atua como identidade em qualquer Tr-módulo representante de α_j, $j=1,\ldots,r$, ou de $(\alpha_1\ldots\alpha_r)^{1/2}$.

Logo o T'-módulo C com a atuação que a cada par (x,z) de $T'\times C$ associa $e^{i2\theta_j} z$, onde θ_j é qualquer real satisfazendo a $w(\overline{\theta}_1,\ldots,\overline{\theta}_j,\ldots,\overline{\theta}_r) = x$ está bem definido e é levado por Rw em α_j .

Da mesma forma, o T'-módulo C com a atuação que a cada par (x,z) de $T'xC$ associa $e^{i(\theta_1+\ldots+\theta_r)}z$, onde $(\theta_1,\ldots,\theta_r)$ é tal que $w(\overline{\theta}_1,\ldots,\overline{\theta}_r) = x$, é levado por Rw em $(\alpha_1\ldots\alpha_r)^{1/2}$.

Isto mostra que $\alpha_1,\ldots,\alpha_r$ e $(\alpha_1\ldots\alpha_r)^{1/2}$ pertencem a RT'. Analogamente mostramos que $\alpha_1^{-1},\ldots,\alpha_r^{-1}$ pertencem a RT'.

Então $Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1},(\alpha_1\ldots\alpha_r)^{1/2}]$ está contido em RT'. Como $R\phi(\alpha_j) = \alpha_j$, ϕ induz a inclusão $R\phi$ de $Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}]=RT_{SO(n)}$ em $Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1},(\alpha_1\ldots\alpha_r)^{1/2}]\subset RT'\subset RTr$.

Seja agora M um T'-módulo. Se $-1 \varepsilon T'$ atuar em M como identidade, podemos considerar M como $T_{SO(n)}$-módulo definindo a atuação

$$T_{SO(n)} \times M \dashrightarrow M$$
$$(x,m) \mapsto x'm$$

onde x' é qualquer elemento pertencente a $\phi^{-1}(x)$.

Então $R\phi$ leva o $T_{SO(n)}$-módulo M acima definido no T'-módulo M.

Isto mostra que todo elemento de RT' onde -1 atua como identidade pertence a $RT_{SO(n)}$, ou seja, é polinômio em $\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}$.

Se M for um T'-módulo arbitrário, podemos escrevê-lo como soma direta $M = M_1 \oplus M_2$ de T'-submódulos M_1 e M_2 onde $-1 \varepsilon T'$ atua como identidade e como multiplicação por -1, repectivamente, já que o operador que leva $m \varepsilon M$ em $-1.m$ é idempotente.

Então $[M_1]$ e $[M_2 \otimes M_2]$ pertencem a $Z[\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}]$, uma vez que -1 atua como identidade sobre M_1 e $M_2 \times M_2$.

Como RT' é subanel de RTr, podemos considerar $[M_2] \varepsilon RTr$ e en tão $[M_2]$ é combinação linear de monômios do tipo $\alpha_1^{n_1/2}\dots\alpha_r^{n_r/2}$ pertencentes a RT' e aonde -1 atua como multiplicação por -1, uma vez que, como T' é comutativo, M_2 se decompõe como soma direta de T'-submódulos de dimensão 1.

Como $w^{-1}(-1)$ é o conjunto de todos os elementos $(\bar{\theta}_1,\dots,\bar{\theta}_r)$ de Tr para os quais existem inteiros $k_1,\dots,k_r$ tais que $\theta_j = k_j\pi$, com $k_1+\dots+k_r$ ímpar, devemos ter $n_1\theta_1+\dots+n_r\theta_r = \pi+2k\pi$, para $(\bar{\theta}_1,\dots,\bar{\theta}_r)$ em $w^{-1}(-1)$, devido a identificação $Rw(\alpha_j) = \alpha_j$.

Logo $n_1k_1+\dots+n_rk_r$ deve ser ímpar para todos $k_1,\dots,k_r$ inteiros com $k_1+\dots+k_r$ ímpar. Então $n_1,\dots,n_r$ são todos ímpares.

De fato, se, digamos, n_1 fosse par, teríamos $n_1\,1+n_2 0+\dots+n_r 0=n_1$ que é par, contrariando nossa hipótese.

Portanto $\alpha_1^{n_1/2}\dots\alpha_r^{n_r/2}$ pode ser escrito como $\alpha_1^{t_1}\dots\alpha_r^{t_r}(\alpha_1\dots\alpha_r)^{1/2}$, com $t_1,\dots,t_r$ inteiros.

Mostramos com isto que $RT' \subset Z[\alpha_1,\alpha_1^{-1},\dots,\alpha_r,\alpha_r^{-1},(\alpha_1\dots\alpha_r)^{1/2}]$.

Segue-se a tese.

4.3.5 Lema:

O elemento $\Delta \in RSpin(2r+1) \subset RT'$ é igual a

$$(\alpha_1^{1/2}+\alpha_1^{-1/2})\dots(\alpha_r^{1/2}+\alpha_r^{-1/2}) = \sum_{\varepsilon_i=\pm 1} \alpha_1^{\varepsilon_1/2}\dots\alpha_r^{\varepsilon_r/2} .$$

Os elementos Δ^+ e Δ^- $\in RSpin(2r)$ RT' são dados por

$$\Delta^+ = \sum_{\varepsilon_1\cdots\varepsilon_r=+1} \alpha_1^{\varepsilon_1/2}\dots\alpha_r^{\varepsilon_r/2} \quad \text{e}$$

$$\Delta^- = \sum_{\varepsilon_1\cdots\varepsilon_r=-1} \alpha_1^{\varepsilon_1/2}\dots\alpha_r^{\varepsilon_r/2} .$$

Prova:

Consideremos o toro $T' \subset Spin(2r+1)$ atuando por multiplicação a esquerda sobre o espaço vetorial $A^+_{2r+1} \otimes C$.

O teorema 4.3.1 mostra que a representação assim obtida se decompõe como soma direta de $2^{2r}/2^r$ cópias de Δ. Em relação a base fixada de $A^+_{2r+1} \otimes C$, a atuação de cada elemento de T' é representada por uma matriz $2^{2r} x 2^{2r}$. Como $T' = w(\mathbb{T}r)$ e cada elemento de T' é da forma

$$x = (\cos\theta_1\, 1 - \operatorname{sen}\theta_1 e_1 e_2)\ldots(\cos\theta_r\, 1 - \operatorname{sen}\theta_r e_{2r-1} e_{2r}) \ ,$$

temos
$$x.e_{i_1}\ldots e_{i_{2k}} = \cos\theta_1\ldots\cos\theta_r e_{i_1}\ldots e_{i_{2k}} + \ldots \ ,$$
e portanto os elementos diagonais desta matriz são todos iguais a $\cos\theta_1\ldots\cos\theta_r$, donde o caráter da representação $2^r\Delta$ em x é igual a $2^{2r}\cos\theta_1\ldots\cos\theta_r$.

Em outros termos, o caráter de Δ em x é igual a

$$2^r\cos\theta_1\ldots\cos\theta_r = (e^{i\theta_1} + e^{-i\theta_1})\ldots(e^{i\theta_r} + e^{-i\theta_r}) \ .$$

Como este é precisamente o caráter em x de $(\alpha_1^{1/2} + \alpha_1^{-1/2})\ldots(\alpha_r^{1/2} + \alpha_r^{-1/2})$, concluimos, pelo teorema 3.16 do capítulo I, que

$$\Delta = \prod_{j=1}^{r} (\alpha_j^{1/2} + \alpha_j^{-1/2}) \ .$$

Se $n = 2r$, para calcularmos Δ^+ e Δ^-, notemos que $\Delta = \Delta^+ + \Delta^-$ e que ambos são não nulos e invariantes sob a ação do grupo de Weyl. Então Δ^+ e Δ^- devem ser dados por uma das expressões

$$\sum_{\varepsilon_1\ldots\varepsilon_r=1} \alpha_1^{\varepsilon_1/2}\ldots\alpha_r^{\varepsilon_r/2} \quad \text{e} \quad \sum_{\varepsilon_1\ldots\varepsilon_r=-1} \alpha_1^{\varepsilon_1/2}\ldots\alpha_r^{\varepsilon_r/2} \ .$$

Resta saber qual corresponde a Δ^+ e qual a Δ^-.

Para isto, consideremos o elemento

$$y = w(\pi/2,\ldots,\pi/2) = (-1)^r e_1 e_2\ldots e_{2r-1} e_{2r} \ .$$

Em Δ^+, y atua como multiplicação por i^r, uma vez $t = i^r e_1\ldots e_{2r}$ atua como identidade. Então o caráter de Δ^+, calculado em y, é igual a $2^{r-1} i^r$.

Como o caráter de $\sum_{\varepsilon_1\ldots\varepsilon_r=\pm1}\alpha_1^{\varepsilon_1/2}\ldots\alpha_r^{\varepsilon_r/2}$, calculado em y, é igual a $\sum_{\varepsilon_1\ldots\varepsilon_r=\pm1} e^{i\pi/2(\varepsilon_1+\ldots+\varepsilon_r)} = \sum_{\varepsilon_1\ldots\varepsilon_r=\pm1} i^{\varepsilon_1+\ldots+\varepsilon_r} = \sum_{\varepsilon_1\ldots\varepsilon_r=\pm1}\varepsilon_1\ldots\varepsilon_r i^r = \pm 2^{r-1} i^r$, concluimos que

$$\Delta^+ = \sum_{\varepsilon_1\ldots\varepsilon_r=1}\alpha_1^{\varepsilon_1/2}\ldots\alpha_r^{\varepsilon_r/2} \quad \text{e} \quad \Delta^- = \sum_{\varepsilon_1\ldots\varepsilon_r=-1}\alpha_1^{\varepsilon_1/2}\ldots\alpha_r^{\varepsilon_r/2} .$$

Isto demonstra o lema.

4.3.6 Teorema:

O anel de representação $RSpin(2r+1)$ é o anel de polinômios $Z[\lambda_1,\ldots,\lambda_{r-1},\Delta]$. O elemento λ_r deste anel é determinado por

$$\Delta\Delta = \lambda_r+\lambda_{r-1}+\ldots+\lambda_1+1 .$$

O anel $RSpin(2r)$ é o anel de polinômios $Z[\lambda_1,\ldots,\lambda_{r-2},\Delta^+,\Delta^-]$ onde valem as relações

$$\Delta^+\Delta^+ = \lambda_r^+ + \lambda_{r-2} + \lambda_{r-4} + \ldots$$
$$\Delta^+\Delta^- = \lambda_{r-1} + \lambda_{r-3} + \lambda_{r-5} + \ldots$$

e

$$\Delta^-\Delta^- = \lambda_r^- + \lambda_{r-2} + \lambda_{r-4} + \ldots ,$$

com cada soma terminando em $\lambda_4 + \lambda_2 + 1$ ou $\lambda_3 + \lambda_1$.

Observação:

A relação polinomial do teorema 3.2 segue de $\Delta^+\Delta^+.\Delta^-\Delta^- = (\Delta^+\Delta^-)^2$.

Prova:

Comecemos com o caso $n = 2r+1$.

Provemos a fórmula $\Delta\Delta = \lambda_r + \lambda_{r-1} + \ldots + \lambda_1 + 1$.

Consideremos o polinômio

$$f(t) = (1 + \alpha_1 t)(1 + \alpha_1^{-1}t)\ldots(1 + \alpha_r t)(1 + \alpha_r^{-1}t)(1 + t) .$$

Como os λ_j são as funções simétricas elementares em $\alpha_1,\alpha_1^{-1},\ldots,\alpha_r,\alpha_r^{-1}$, 1, o coeficiente de t^j em $f(t)$ é λ_j, para $j \neq 0$, e temos

$$f(1) = 1 + \lambda_1 + \ldots + \lambda_{2r+1} = 2(\lambda_r + \lambda_{r-1} + \ldots + \lambda_1 + 1) ,$$

pois $\lambda_j = \lambda_{2r+1-j}$.

Como $(1 + \alpha_j)(1 + \alpha_j^{-1}) = \alpha_j + 2 + \alpha_j^{-1} = (\alpha_j^{1/2} + \alpha_j^{-1/2})^2$,

temos $\lambda_r + \lambda_{r-1} + \ldots + 1 = 1/2\ f(1) = \prod_{j=1}^{r} (\alpha_j^{1/2} + \alpha_j^{-1/2})^2 = \Delta\Delta$,

pelo lema 4.3.5 .

Temos $Z[\lambda_1, \ldots, \lambda_r] = RSO(n) \subset RSpin(n) \subset RT' = Z[\alpha_1, \alpha_1^{-1}, \ldots, \alpha_r, \alpha_r^{-1}, (\alpha_1 \cdots \alpha_r)^{1/2}]$.

Seja M um Spin(n)-módulo. Como -1 pertence a Spin(n) e $(-1)^2 = 1$, podemos decompor M como soma direta de Spin(n)-submódulos M_1 e M_2, onde -1 atua como identidade e como multiplicação por -1, respectivamente.

Já vimos que $[M_1]$ pertence a RSO(n).

A atuação de $u_i = e_i e_n \in \text{Spin}(n)$ para $i = 1, \ldots, n-1$ sobre M_2 satisfaz as relações

$$u_i^2 = -1 , \quad u_i u_j = -u_j u_i , \text{ para } j \neq i .$$

Isto define uma estrutura de módulo a esquerda em M_2 sobre $A_{n-1} \otimes C$ compatível com a atuação de Spin(n) .

Então $[M] \in RSpin(2r+1)$ pode ser escrito de maneira única como

$$[M] = a + b\Delta \quad , \quad \text{com } a \in RSO(n) \text{ e } b \in Z .$$

Como $\Delta^2 = \lambda_r + \lambda_{r-1} + \ldots + \lambda_1 + 1$, os elementos de RSpin(2r+1) são polinômios em $\lambda_1, \ldots, \lambda_{r-1}, \Delta$.

Seja T: $RTr = Z[\alpha_1^{1/2}, \alpha_1^{-1/2}, \ldots, \alpha_r^{1/2}, \alpha_r^{-1/2}] \dashrightarrow RTr$ o homomorfismo de anéis dado por $T(\alpha_1^{\pm 1/2}) = -\alpha_1^{\pm 1/2}$ e $T(\alpha_i^{\pm 1/2}) = \alpha_i^{\pm 1/2}$, para $i \neq 1$.

Então $T(\Delta) = -\Delta$ e $T(g) = g$ para todo $g \in RSO(2r+1)$.

Como todo polinômio f em $\lambda_1,\ldots,\lambda_{r-1},\Delta$ se decompõe como $f = f_1 + \Delta f_2$, com f_1 e f_2 polinômios em $\lambda_1,\ldots,\lambda_{r-1},\lambda_r$, vemos que $f = 0$ implica $T(f) = 0 = T(f_1 + \Delta f_2) = f_1 - \Delta f_2$, e portanto $f_1 = f_2 = 0$.

Isto mostra que $RSpin(2r+1) = Z[\lambda_1,\ldots,\lambda_{r-1},\Delta]$ e que os geradores $\lambda_1,\ldots,\lambda_{r-1},\Delta$ são algebricamente independentes.

Se $n = 2r$, um argumento semelhante ao da primeira parte do caso anterior mostra que, se denotarmos $\Delta' = \Delta^+ + \Delta^-$, para evitar confusões com o caso n ímpar, teremos

$$\Delta'\Delta' = 2 + 2\lambda_1 + \ldots + 2\lambda_{r-1} + \lambda_r^+ + \lambda_r^- .$$

De fato, o polinômio

$$g(t) = (1 + \alpha_1 t)(1 + \alpha_1^{-1} t)\ldots(1 + \alpha_r t)(1 + \alpha_r^{-1} t)$$

tem λ_j por coeficiente de t^j e

$$\begin{aligned} g(1) &= 1 + \lambda_1 + \ldots + \lambda_r + \lambda_{r+1} + \ldots + \lambda_{2r} = \\ &= 2 + 2\lambda_1 + \ldots + 2\lambda_{r-1} + \lambda_r^+ + \lambda_r^- \qquad (\text{pois } \lambda_k = \lambda_{n-k} \text{ e } \lambda_n = 1) \\ &= (\alpha_1^{1/2} + \alpha_1^{-1/2})^2 \ldots (\alpha_r^{1/2} + \alpha_r^{-1/2})^2 = (\sum_{\varepsilon_j = \pm 1} \alpha_1^{\varepsilon_1/2} \ldots \alpha_r^{\varepsilon_r/2})^2 = \\ &= (\sum_{\varepsilon_1 \cdots \varepsilon_r = 1} \alpha_1^{\varepsilon_1/2} \ldots \alpha_r^{\varepsilon_r/2} + \sum_{\varepsilon_1 \cdots \varepsilon_r = -1} \alpha_1^{\varepsilon_1/2} \ldots \alpha_r^{\varepsilon_r/2})^2 = \\ &= (\Delta^+ + \Delta^-)^2 = (\Delta')^2 , \end{aligned}$$

pelo lema 4.3.5 .

Escrevamos $(\Delta')^2 = \sum_{\varepsilon_j, \delta_j = \pm 1} \alpha_1^{(\varepsilon_1 + \delta_1)/2} \ldots \alpha_r^{(\varepsilon_r + \delta_r)/2}$.

Para um dado termo

$$z = \alpha_1^{(\varepsilon_1 + \delta_1)/2} \ldots \alpha_r^{(\varepsilon_r + \delta_r)/2} ,$$

sejam
u o número de índices j com $\varepsilon_j = \delta_j = 1$,
a " " " " " " $\varepsilon_j = 1$ e $\delta_j = -1$,
b " " " " " " $\varepsilon_j = -1$ e $\delta_j = 1$ e
v " " " " " " $\varepsilon_j = \delta_j = -1$.

Então $r = u + a + b + v$.

O termo dado é somando de $\Delta^+\Delta^+$ se e somente se $b+v$ e $a+v$ são ambos pares; é somando de $\Delta^+\Delta^-$ se e somente se exatamente um dos números $b+v$ ou $a+v$ é ímpar; e é somando de $\Delta^-\Delta^-$ se e somente se $b+v$ e $a+v$ são ambos ímpares.

O monômio $z = \alpha_1^{(\varepsilon_1+\delta_1)/2} \ldots \alpha_r^{(\varepsilon_r+\delta_r)/2}$ é somando de λ_{r-i} se e somente se $u+v \equiv r-i \pmod 2$.

Temos $u+v = r-a-b = r+2v-(b+v)-(a+v) \equiv r-(b+v)-(a+v) \pmod 2$, onde $b+v$ é o número de índices j com $\varepsilon_j = -1$ e $a+v$ é o número de índices j com $\delta_j = -1$.

Consequentemente, o monômio z aparece em λ_{r-i} se e somente se $i \equiv (b+v) + (a+v) \pmod 2$.

Como z é somando de $\Delta^+\Delta^-$ se e somente se exatamente um dos números $b+v$ ou $a+v$ for ímpar e isto equivale a i ser ímpar, concluímos que

$$\Delta^+\Delta^- = \lambda_{r-1} + \lambda_{r-3} + \cdots \quad .$$

Logo $$\Delta^+\Delta^+ + \Delta^-\Delta^- = \lambda_r^+ + \lambda_r^- + 2\lambda_{r-2} + 2\lambda_{r-4} + \cdots \quad .$$

Em qualquer $Spin(2r)$-módulo representante de $\Delta^+\Delta^+$ ou $\Delta^-\Delta^-$, $-1 \in Spin(2r)$ atua como identidade, e portanto $\Delta^+\Delta^+$ e $\Delta^-\Delta^-$ pertencem a $RSO(2r)$.

Então $\Delta^+\Delta^+ = a\lambda_r^+ + b\lambda_r^- + \tau$, onde τ é combinação linear de $\lambda_{r-2}, \lambda_{r-4}, \ldots$, e a e b valem 0 ou 1.

Seja $H: RTr \longrightarrow RTr$ o homomorfismo de anéis dado por $H(\alpha_1^{\pm 1/2}) = \alpha_1^{\mp 1/2}$ e $H(\alpha_j^{\pm 1/2}) = \alpha_j^{\pm 1/2}$, para $j \neq 1$. Temos

$$H(\Delta^+) = \Delta^- \ , \ H(\Delta^-) = \Delta^+ \ ,$$

$$H(\lambda_k) = \lambda_k \ , \ k = 1,\dots,r-1 \qquad \text{e}$$

$$H(\lambda_r^+) = \lambda_r^- \ , \ H(\lambda_r^-) = \lambda_r^+ \qquad .$$

Logo $\quad H(\Delta^+\Delta^+) = b\lambda_r^+ + a\lambda_r^- + \tau = \Delta^-\Delta^-$,

donde

$$\Delta^+\Delta^+ + \Delta^-\Delta^- = \lambda_r^+ + \lambda_r^- + 2(\lambda_{r-2} + \lambda_{r-4} + \dots) =$$

$$= (a+b)(\lambda_r^+ + \lambda_r^-) + 2\tau \ ,$$

e portanto $\Delta^+\Delta^+$ e $\Delta^-\Delta^-$ têm a forma $\lambda_r^\pm + \lambda_{r-2} + \lambda_{r-4} + \dots$.

Para ver qual a expressão correspondente a $\Delta^+\Delta^+$, notemos que o monômio $\alpha_1 \dots \alpha_r$ é somando de λ_r^+ mas não de λ_r^-, e como ele aparece em $\Delta^+\Delta^+$ e não em $\Delta^-\Delta^-$, concluimos que

$$\Delta^+\Delta^+ = \lambda_r^+ + \lambda_{r-2} + \lambda_{r-4} + \dots \qquad \text{e}$$

$$\Delta^-\Delta^- = \lambda_r^- + \lambda_{r-2} + \lambda_{r-4} + \dots \qquad .$$

Como todo Spin(2r)-módulo se decompõe como soma direta de um SO(2r)-módulo e de um $A_{2r-1} \otimes C$-módulo, vemos que qualquer polinômio de RSpin(2r) é polinômio em $\lambda_1,\dots,\lambda_{r-2},\Delta^+$ e Δ^- .

Resta mostrar que estes são algebricamente independentes.

Um procedimento inteiramente análogo ao caso anterior mostra que $\lambda_1,\dots,\lambda_{r-1},\Delta^+ + \Delta^-$ o são.

Denotemos por $\lambda_1^{(r-1)},\dots,\lambda_{r-1}^{(r-1)}$ as funções simétricas elementares em $\alpha_1,\alpha_1^{-1},\dots,\alpha_{r-1},\alpha_{r-1}^{-1}$ e $\Delta_{r-1}^+, \Delta_{r-1}^-$ dadas por

$$\Delta_{r-1}^+ = \sum_{\varepsilon_1 \dots \varepsilon_{r-1} = 1} \alpha_1^{\varepsilon_1/2} \dots \alpha_{r-1}^{\varepsilon_{r-1}/2} \quad \text{e} \quad \Delta_{r-1}^- = \sum_{\varepsilon_1 \dots \varepsilon_{r-1} = -1} \alpha_1^{\varepsilon_1/2} \dots \alpha_{r-1}^{\varepsilon_{r-1}/2} \ .$$

Claramente $\lambda_1^{(r-1)},\dots,\lambda_{r-1}^{(r-1)}$, $\Delta_{r-1}^+ + \Delta_{r-1}^-$ são algebricamente independentes.

Seja $\Psi\colon Z[\alpha_1^{1/2},\alpha_1^{-1/2},\dots,\alpha_r^{1/2},\alpha_r^{-1/2}] \longrightarrow Z[\alpha_1^{1/2},\alpha_1^{-1/2},\dots,\alpha_{r-1}^{1/2},\alpha_{r-1}^{-1/2}]$

o homomorfismo de anéis dado por $\Psi(\alpha_j^{\pm 1/2}) = \alpha_j^{\pm 1/2}$, para $j = 1,\ldots,r-1$, e $\Psi(\alpha_r^{\pm 1/2}) = 1$.

Temos $\Psi(\lambda_1) = \lambda_1^{(r-1)} + 2$,

$\Psi(\lambda_j) = \lambda_j^{(r-1)} + 2\lambda_{j-1}^{(r-1)}$, para $j = 1,\ldots,r-1$,

e $\Psi(\Delta^{\pm}) = \Delta_{r-1}^{+} + \Delta_{r-1}^{-}$.

Se existir uma relação polinomial não identicamente nula f com $f(\lambda_1,\ldots,\lambda_{r-2},\Delta^+,\Delta^-) = 0$, então

$0 = \Psi(f(\lambda_1,\ldots,\lambda_{r-2},\Delta^+,\Delta^-) = f(\lambda_1^{(r-1)} + 2,\ldots,\lambda_{r-2}^{(r-1)} + 2\lambda_{r-3}^{(r-1)},$
$\Delta_{r-1}^{+} + \Delta_{r-1}^{-},\Delta_{r-1}^{+} + \Delta_{r-1}^{-})$,

o que é absurdo.

Isto mostra que $RSpin(2r) = Z[\lambda_1,\ldots,\lambda_{r-2},\Delta^+,\Delta^-]$, com $\lambda_1,\ldots,\lambda_{r-2},\Delta^+,\Delta^-$ algebricamente independentes.

BIBLIOGRAFIA

1. Adams, J. F., Lectures on Lie Groups, Benjamin, New York, 1969.
2. Brauer, R., H. Weyl, Spinors in n Dimensions, A.J.M., 57, 425-449, (1935).
3. Cartan, E., The Theory of Spinors, The M.I.T. Press, Cambridge, 1966.
4. Chevalley, C., Theory of Lie Groups I, Princeton University, Princeton, 1946.
5. ____________, The Algebraic Theory of Spinors, Columbia University, New York, 1955.
6. ____________, The Construction and Study of Certain Important Algebras, The Math. Society of Japan, Japan, 1955.
7. Husemoller, D., Fibre Bundles, Mc Graw-Hill, New York, 1966.
8. Mac Lane, S., G. Birkhoff, Algebra, Mac Millan, New York, 1968.
9. Milnor, J., The Representation Rings of Some Classical Groups, (mimeographed), Princeton University, Princeton, 1963.
10. Nachbin, L., The Haar Integral, Van Nostrand, Princeton, 1965.
11. Van der Waerden, B.L., Álgebra Moderna, Soc. Portuguesa de Matemática, Lisboa, 1955.
12. Weyl, H., Classical Groups, Princeton University, Princeton, 1946.