Grupos Finitos de Automorfismos da Esfera de Riemann

Alexander Arbieto
Instituto de Matemática Pura e Aplicada
Rio de Janeiro, Brasil
email: alexande@impa.br

July 18, 2005

1 Introdução

Desde a Antiguidade são conhecidos os cinco poliedros regulares de $\mathbb{R}^3$: o tetraedro, o cubo, o octaedro, o dodecaedro e o icosaedro. Tão importantes o são, que muitos acreditam que eles teriam sido a motivação principal de Euclides em escrever os "Elementos".

Um bom mecanismo para estudar as simetrias de cada poliedro regular é o seguinte: imaginamos que os vértices do poliedro estão situados na esfera de Riemann e perguntamos pelo grupo de automorfismos da esfera de Riemann que permutam os vértices. Todos estes grupos são compostos de rotações. Vˆse que o grupo do tetraedro é isomorfo a A_4 (permutações pares dos seu 4 vértices, logo contendo 12 elementos), o grupo do octaedro é isomorfo a S_4 (permutações das 4 retas que unem os baricentros das faces opostas) e o grupo do icosaedro é isomorfo ao grupo alternado A_5 (permutações pares dos 5 octaedros obtidos pelos pontos médios das arestas).

Aqui, classificamos os grupos finitos de automorfismos da esfera de Riemann. E o resultado central é que existem somente 5 tipos de grupos: cíclicos, diedrais, do tetraedro, do octaedro e do icosaedro.

A idéia central é usar a fórmula de Riemann-Hurwitz no corpo $K(x)|K(x)^G$, onde K é um corpo algebricamente fechado, G é um grupo finito de automorfismos de $K(x)|K$ (generalizando assim o caso da esfera de Riemann, que pode ser vista como a superfície de Riemann do corpo de funções racionais $\mathbb{C}(x)|\mathbb{C}$). Note que pelo teorema de Lüroth **[Endler, pg. 171]** $K(x)^G$ é racional, e pelo teorema de Artin **[Endler, pg. 87]** $K(x)^G|K$ é finita, normal e sepraável com grupo de Galois G, assim podemos usar a fórmula de Riemann-Hurwitz.

Uma vez que sabemos os casos possíveis, fazemos uma ánalise detalhada das valorizações de $K(x)|K$ ramificadas sobre $K(x)^G$, que no fim correspondem aos pontos médios das arestas, aos vértices e aos baricentros das faces dos poliedros em questão.

2 Preliminares

Nesta seção apresentamos certos resultados, muito úteis, que serão usados para determinar o grupo dos automorfismos de $K(x)|K$.

Lema 1 *Seja K um corpo, t uma transcendente sobre K, $z := \frac{f(t)}{g(t)} \in K(t)\backslash K$, onde $f(X), g(X) \in K[X]$, $g(X) \neq 0$ e $mdc(f(X), g(X)) = 1$. Então z é transcendente sobre*

K e $[K(t):K(z)] = \max\{deg(f(X)), deg(g(X))\}$. Além disso, $K(t) = K(z)$, se e só se $z = \frac{at+b}{ct+d}$ onde $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$.

Com este lema vemos que $Aut(K(x)|K)$ (automorfismos de um corpo de funções racionais) é isomorfo a $PGL_2(K)$ (grupo projetivo linear). Pois dado $\sigma \in Aut(K(x)|K)$, pelo Lema 1, temos que $\sigma(x) = \frac{ax+b}{cx+d}$ onde $ad - bc \neq 0$, a menos de uma constante, isto é , $\frac{ax+b}{cx+d} = \frac{Ax+B}{Cx+D}$ se e só se $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ onde $\lambda \in K^*$. Donde:

$$Aut(K(x)|K) \approx \frac{GL_2(K)}{K^*} = PGL_2(K)$$

Vamos supor agora (que será nosso caso) que K é algebricamente fechado. Então temos uma aplicação (vista em aula) $\Psi : S_{K(x)|K} \to K \cup \{\infty\}$, dada por:

$$\Psi(v) = \begin{cases} r & \text{quando } v(x-r) = 1 \\ \infty & \text{quando } v(\frac{1}{x}) = 1 \end{cases}$$

Definimos para cada $r \in K \cup \{\infty\}$, $v_r = v$ onde r é a imagem de v pela bijeção dada acima.

Além disso, sabemos que se $\sigma \in Aut(K(x)|K)$ então σ induz bijeção em $S_{K(x)|K}$:

$$v \longmapsto v \circ \sigma^{-1}$$

E portanto induz uma bijeção em $K \cup \{\infty\}$. De fato, ao usar o expoente -1, temos que $Aut(K(x)|K)$ age a esquerda sobre a superfície de Riemann, já a ação sobre a reta projetiva é dada pelo:

Lema 2 *Seja K um corpo algebricamente fechado e $\sigma \in Aut(K(x)|K)$, isto é $\sigma(x) = \frac{ax+b}{cx+d}$ onde $ad - bc \neq 0$. Então $v_r \circ \sigma = v_{\frac{ar+b}{cr+d}}$ para cada $r \in K \cup \{\infty\}$.*

Note que se z_1, z_2 e z_3 são pontos distintos da reta projetiva $\mathbb{P}(K)$ diferentes de ∞ então o seguinte automorfismo:

$$\tau(z) = \frac{(z - z_1)(z_2 - z_3)}{(z_1 - z_2)(z_3 - z)}$$

leva z_1, z_2 e z_3 em 0, 1 e ∞ respectivamente (de fato, τ é composta por uma translação, uma homotetia e uma inversão). Caso algum $z_j = \infty$ então tomamos τ como na fórmula acima porém fazendo $z_j \to \infty$ (p.ex: se $z_1 = \infty$ então $\tau = \frac{(z_3 - z_2)}{(z_3 - z)}$. Novamente os pontos z_1, z_2 e z_3 são levados em 0, 1 e ∞. Note que τ é única pois se outro automorfismo ρ leva os mesmos pontos em 0, 1 e ∞ então $\rho \circ \tau$ fixa 0, 1 e ∞ e por verificação imediata vê-se que $\rho \circ \tau = id$.

Em particular dados (z_1, z_2, z_3) e (w_1, w_2, w_3) em $(\mathbb{P}^1(K))^3$, por transitividade, existe um único automorfismo τ que leva z_j em w_j. Além disso se τ é automorfismo que fixa 3 pontos, $\tau = id$.

Resumindo tudo isso e usando o Lema 2 para traduzir na linguagem de valorizações temos:

Lema 3 *Seja K um corpo algebricamente fechado, (v_1, v_2, v_3) e (w_1, w_2, w_3) triplas de valorizações distintas de $S_{K(x)|K}$. Então existe um único automorfismo $\sigma \in Aut(K(x)|K)$ tal que $v_j \circ \sigma^{-1} = w_j$ para $j = 1, 2, 3$.*

2.1 A Fórmula de Riemann-Hurwitz

Usaremos aqui a fórmula de Riemann-Hurwitz (vista na palestra do João e do Matheus e também nas notas de aula) para encontrar os casos a serem tratados no cálculo dos subgrupos finitos de automorfismos na esfera de Riemann.

Antes, recordemos a fórmula de Riemann-Hurwitz:

Teorema 4 (A Fórmula de Riemann-Hurwitz) *Seja $F|K$ um corpo de funções em uma variável, K algebricamente fechado. Seja também $G < Aut(F|K)$, finito com n elementos e $v_1, \cdots, v_r$ as valorizações de $S_{F^G|K}$ que se ramificam em $F|F^G$. Fixado $j = 1, \cdots, r$ seja w_j um prolongamento de v_j a F, e_j o índice de ramificação de w_j sobre F^G e d_j o coeficiente de $F|F^G$. Então*

$$2g_F - 2 = n(2g_{F^G} - 2 + \sum_{j=1}^{r} \frac{d_j}{e_j})$$

Em particular se $F = K(x)$ é um corpo de funções racionais então

$$2 - \frac{2}{n} = \sum_{j=1}^{r} \frac{d_j}{e_j}.$$

Neste caso particular temos que: $K(x)|K(x)^G$ é separável, usando o:

Teorema 5 (Lüroth) *Seja K um copro e x uma transcendente sobre K. Então todo subcorpo L de $K(x)$ com $K \subsetneq L$ é uma extensão transcendente de K do tipo $L = K(y)$.*

Para mostrar que $K(x)^G$ é racional e depois usando o teorema de Artin, conforme foi dito na introdução.

Além disso, $K_{w_j} = K_{v_j}$ para todo $j = 1, \cdots r$. Supondo $car(K) \dagger e_j$ temos pelo teorema da Diferente de Dedekind **(ver palestra do João)** que $d_j = e_j - 1$, donde:

$$2 - \frac{2}{n} = \sum_{j=1}^{r} \frac{e_j - 1}{e_j}.$$

Ou ainda:

$$2(1 - \frac{1}{n}) = \sum_{j=1}^{r} (1 - \frac{1}{e_j}).$$

Podemos supor que $e_1 \leq e_2 \leq \cdots \leq e_r$. Seja $1 \leq j \leq r$.

Como $n \geq 2$ e $e_j \geq 2$ temos $2 - \frac{2}{n} \geq 1$ e $\frac{e_j - 1}{e_j} < 1$ e portanto $r \geq 2$.

Como $2 - \frac{2}{n} < 2$ e $\frac{e_j-1}{e_j} \geq \frac{1}{2}$ temos que $r \leq 3$.

Por exemplo, seja $r = 2$ então: $\frac{2}{n} = \frac{1}{e_1} + \frac{1}{e_2}$. Assim:

$$\frac{n}{e_1} + \frac{n}{e_2} = 2$$

E como $\frac{n}{e_1}$ é inteiro positivo, vemos que $e_1 = e_2 = n$.

Se $r = 3$ então $e_1 = 2$ pois senão $e_1^{-1} + e_2^{-1} + e_3^{-1} \leq 1$ e portanto $\frac{2}{n} \leq (\sum e_i) - 1 \leq 0$ absurdo.

Analisando os casos temos o seguinte (detalhes, ver **[Jones, Singerman, pg. 47, 48]**):

Corolário 6 *Suponha que* $car(K) = 0$ *ou* $car(K)\dagger n$, $F = K(x)$ *corpo de funções racionais. Então* $r = 2$ *ou* 3. *Além disso existem 5 possibilidades para os índices de ramificação:*

1. $(r = 2)$ *e* $e_1 = e_2 = n$.
2. $(r = 3)$, $e_1 = e_2 = 2$ *e* $e_3 = \frac{n}{2}$ *(n par).*
3. $(r = 3)$, $e_1 = 2$ *e* $e_2 = e_3 = 3$ $(n = 12)$.
4. $(r = 3)$, $e_1 = 2$ *e* $e_2 = 3$ $e_3 = 4$ $(n = 24)$.
5. $(r = 3)$, $e_1 = 2$ *e* $e_2 = 3$ $e_3 = 5$ $(n = 60)$.

3 Subgrupos Finitos de $Aut(K(x)|K)$

O resultado principal conforme anunciado na introdução é:

Teorema 7 *Seja* $K(x)|K$ *um corpo de funções racionais,* K *algebricamente fechado. seja* $G < Aut(K(x)|K)$ *de ordem* n. *Suponhamos que a característica de* K *é zero ou um primo que não divide* n, *então* G *é isomorfo a um dos seguintes grupos:*

1. *grupo cíclico.*
2. *grupo diedral* D_m *de grau* $m > 1$ *de ordem* $2m = n$.
3. *grupo alternado* A_4 *(grupo do tetraedro).*
4. *grupo simétrico* S_4 *(grupo do octaedro).*
5. *grupo alternado* A_5 *(grupo do icosaedro).*

Mais ainda, em cada um destes casos podemos encontrar explicitamente os geradores de G.

No que se segue estudaremos os casos dados pelo Corolário 6, donde tiramos as conclusões do teorema. Logo após a demonstração de cada caso, é dada uma interpretação geométrica na esfera de Riemann, para ilustrar os métodos usados.

Vale a pena notar que a ação de $Aut(K(x)|K)$ sobre $S_{K(x)|K}$ (Lema 2) se extende linearmente aos divisores de $K(x)|K$ via:

$$\sigma(\sum_w n_w w) = \sum_w n_w w\sigma^{-1}$$

onde $\sigma \in Aut(K(x)|K)$ e $\sum\limits_w n_w w$ é divisor de $K(x)|K$.

Em particular, se $z \in K$ e $div(z) = \sum\limits_w w(z)w$ então:

$$\sigma(div(z)) = \sum_w n_w w\sigma^{-1} = \sum_w n_w w\sigma^{-1}(\sigma(z))w\sigma^{-1} = div(\sigma(z)).$$

Usando a notação e os casos do corolário 6, demonstremos o teorema:

3.1 Subgrupos Cíclicos (Caso 1)

Neste caso $r = 2$ e $e_1 = e_2 = n$, portanto v_1 e v_2 são totalmente ramificadas em $K(x)|K(x)^G$. Sejam w_1 e w_2 as respectivas extensões de v_1 e v_2 a $K(x)$. Tome $y \in K(x)$ tal que $div(y) = w_1 - w_2$ e seja $\sigma \in G$.

Usando a igualdade fundamental, temos que $[K(x) : K(y)] = deg(w_2) = 1$, ou seja $K(x) = K(y)$. G age transistivamente sobre os prolongamentos de v_1 e v_2, logo σ fixa w_1 e w_2 e portanto $\sigma(y) = cy$ com $c \in K^*$. Agora $\sigma^n = id$, logo c é raíz n-ésima da unidade. Logo G é cíclico e σ gera G se e só se c é raíz n-ésima *primitiva* da unidade. Note que $K(x)^G = K(y^n)$ pois $y^n \in K(x)^G$ e $[K(x) : K(y^n)] = n$.

Na esfera de Riemann $S_{\mathbb{C}(y)|\mathbb{C}}$, y é o gerador de $\mathbb{C}(x)|\mathbb{C}$ encontrado acima, w_1 e w_2 correspondem aos pólos da esfera. Como c é raíz n-ésima da unidade, temos que $\sigma(y) = e^{\frac{2\pi i m}{n}} y$ para algum m inteiro. Logo pelo Lema 2, σ induz na esfera uma rotação de ângulo $\frac{2\pi m}{n}$ com eixo de rotação passando pelos dois pólos.

3.2 Subgrupos Diedrais (Caso 2)

Neste caso $r = 3$, $e_1 = e_2 = 2$ e $e_3 = \frac{n}{2} = m$. Ora, $n = 2e_3$ diz que existem 2 extensões de v_3 a $K(x)$, digamos $w_3^{(1)}$ e $w_3^{(2)}$.

Definição 8 *Seja $F|K$ extensão Galoisiana onde K é algebricamente fechado com grupo de Galois $G = Aut(F|K)$. Seja $v \in S_{K|k}$ e w uma prolongamento de v a F. Definimos então:*

$$G(w|v) := \{\sigma \in Aut(F|K) \ ; w\sigma = w\}$$

o **grupo de decomposição de** *w* **sobre** *v e*

$$F(w|v) := \{\sigma \in Aut(F|K) \ ; w(\sigma z - z) > 0 \text{ para cada } z \in \mathcal{O}_w\}$$

o **grupo de inércia de** *w* **sobre** *v.Note que estes são subgrupos de $G = aut(F|K)$.*

Assim, $G(w_3^{(1)})$ é cíclico de ordem m. Na verdade, segundo um resultado em **[Serre, pg. 67]**, como K é algebricamente fechado e sua ordem m não é divisível por p então $G(w_3^{(1)})$ coincide com $F(w_3^{(1)})$.

Seja $y \in K(x)$ tal que $div(y) = w_3^{(1)} - w_3^{(2)}$. Novamento (como no caso cíclico) $K(y) = K(x)$, $K(x)^{<\sigma>} = K(y^m)$ e $\sigma(y) = cy$ onde c é raíz n-ésima primitva da unidade.

Agora, o grupo de Galois G age transitivamente sobre os prolongamentos de v_3, logo existe $\tau \in G$ tal que $w_3^{(2)} = w_3^{(1)}\tau$ e portanto $\tau(y) = \frac{a}{y}$ para algum $a \in K^*$ (podemos supor $\tau(y) = \frac{1}{y}$ multiplicando y por $a^{\frac{-1}{2}}$).

Como $< \sigma >= G(w_3^{(1)}) < G$ tem índice 2 e não contêm τ, temos que $G =< \sigma, \tau >$. Finalmente, as relações: $\sigma^m = \tau^2 = (\sigma\tau)^2 = id$ implicam que G é isomorfo ao grupo diedral de ordem $2m$. Note que $K(x)^{<\sigma>} = K(y + y^{-1})$ e $K(x)^G = K(y^m + y^{-m})$.

Na esfera de Riemann, novamente $w_3^{(1)}$ corresponde ao pólo sul e $w_3^{(2)}$ corresponde ao pólo norte da esfera. Tomamos $\sigma = e^{\frac{2\pi i}{m}}$. Logo pelo Lema 2, σ induz uma rotação na esfera de ângulo $\frac{2\pi}{m}$, com eixo de rotação passando pelos pólos. Agora $\tau = \frac{1}{y}$ induz um automorfismo que permuta os pólos e deixa o equador invariante. Como as extensões $w_1^{(1)}, \cdots, w_1^{(m)}$ de v_1 e $w_2^{(1)}, \cdots, w_2^{(m)}$ são caracterizadas pela propriedade da G-órbita ter comprimento m, elas correspondem bijetivamente as raízes $(2m)$-ésimas da unidade em $\mathbb{C} \cup \{\infty\}$ logo a pontos no equador da esfera. Trocando v_1 por v_2 eventualmente podemos supor que as extensões de v_1 correspondem bijetivamente as raízes m-ésimas da unidade.

3.3 O grupo do Tetraedro

Neste caso $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 3$, $n = 12$. Ora, $n = 4e_2$, logo temos 4 prolongamentos de v_2 a $K(x)$. Assim como este número é maior ou igual a 3, pelo Lema 3 temos que dado um automorfismo que fixa cada prolongamento de v_2 então ele é a identidade, isto é, a ação de G sobre estes prolongamentos é **fiel** [**AschBacher**]. Assim G tem representação fiel em S_4. Como somente A_4 é subgrupo de ordem 12 de S_4, temos que G é isomorfo a A_4.

Vamos descrever os geradores de G. Seja N o subgrupo normal de G de ordem 4. Como $e_1 = 2 \dagger 3$ e $K(x)^N | K(x)^G$ é normal temos que v_1 de $K(x)^G$ se decompõe em 3 valorizações em $K(x)^N$ (pois tem índice de ramificação e_1). Cada uma destas valorizações tem 2 prolongamentos a $K(x)$: $w_1^{(j)}, \tilde{w}_1^{(j)}$ com $j = 1, 2, 3$ e com índice de ramificação igual a 2. Ora então em $K(x)|K(x)^N$ temos o caso anterior (diedral), portanto temos $y \in K(x)$ tal que $K(y) = K(x)$, $div(y) = w_1^{(1)} - \tilde{w}_1^{(2)}$ e temos σ e τ geradores de N tal que $\sigma(y) = -y$ e $\tau(y) = \frac{1}{y}$.

Como vimos no caso anterior, as valorizações $w_1^{(1)}$ e $\tilde{w}_1^{(1)}$ correspondem aos pontos 0 e ∞ da reta projetiva enquanto $w_1^{(2)}$, $\tilde{w}_1^{(2)}$, $w_1^{(3)}$ e $\tilde{w}_1^{(3)}$ correspondem aos pontos $1, -1, i$ e $-i$. Como G age transitivamente sobre os prolongamentos de v_1, existe $\rho \in G$ tal que $w_1^{(1)}\rho^{-1} = w_1^{(2)}$. Já que N é normal em G, existe $\tau' \in N$ tal que $\rho\tau\rho^{-1} = \tau'$, assim:

$$\tilde{w}_1^{(1)}\rho^{-1} = w_1^{(1)}\tau^{-1}\rho^{-1} = w_1^{(1)}\rho^{-1}\tau'^{-1} = w_1^{(2)}\tau'^{-1} \in \{w_1^{(2)}, \tilde{w}_1^{(1)}\}$$

já que N age transitivamente sobre os prolongamentos de cada uma das 3 extensões de v_1 a $K(x)^N$. Porém $\tilde{w}_1^{(1)}\rho^{-1} \neq w_1^{(2)}$, pois $w_1^{(1)}\rho^{-1} = w_1^{(2)}$. Donde $\tilde{w}_1^{(1)}\rho^{-1} = \tilde{w}_1^{(2)}$.

Assim pelo Lema 2, temos que $\rho^{-1} = \frac{1+ay}{1-ay}$ para algum $a \in K^*$. Agora como a ordem de ρ é 3 (pois $\rho \in G \backslash N$), analisando a equação $y = \rho^3(y) (= \frac{(a^{-3}-2a^{-2}-a^{-1})y-(a^{-3}+a^{-1})}{(a^{-2}+1)y-(a^{-2}+2a^{-1}-1)})$, obtemos $a^{-2} = -1$ assim podemos supor $a = i$. E daí $\rho(y) = (-i)\frac{y-1}{y+1}$.

Finalmente, por substituição direta, vale $\tau = \rho^{-1}\sigma\rho$. Donde $G = <\sigma, \tau, \rho> = <\sigma, \rho>$.

Na esfera de Riemann, como foi visto, os prolongamentos de v_1 correspondem aos pontos 0, ∞, 1, -1, i e $-i$ de $\mathbb{C} \cup \{\infty\}$, e portanto definem um octaedro regular. Já os prolongamentos de v_2 e v_3 correspondem aos pontos fixos dos automorfismos induzidos pelos elementos de G de ordem 3. Assim, os prolongamentos de v_2 definem na esfera os vértices de um tetraedro regular e G é isomorfo ao grupo de permutações pares dos vértices desse tetraedro. Agora projete este tetraedro na esfera (centrada no centro da esfera), como o conjunto dos prolongamentos de v_1 é o único subconjunto de $S_{\mathbb{C}(y)|\mathbb{C}}$ de ordem 6 onde G opera transitivamente, temos somente mais 2 conjuntos de ordem 4 onde G opera transitivamente, os prolongamentos de v_2 e v_3 . Donde:

- Os prolongamentos de v_1 correspondem aos pontos médios das arestas do tetraedro.
- Os prolongamentos de v_3 correspondem aos baricentros das faces do tetraedro.

3.4 O Grupo do Octaedro

Neste caso $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 4$ e $n = 24$.

Novamente a idéia é "quebrar" o grupo G e analisar cada parte. Seja então U um 3-Sylow de G. Como $\#U = 3$, pelo corolário 6, temos 2 valorizações de $K(x)^U$ que se ramificam (totalmente) em $K(x)$ e como $3 \nmid e_1$, $3 \nmid e_3$ e $3 | e_2$ elas são prolongamentos de v_2 a $K(x)^U$.

Agora v_2 tem 8 prolongamentos a $K(x)$, logo G possui 4 3-Sylows, e pelo teorema de Sylow, G opera transitivamente sobre eles (via representação). Seja V o núcleo dessa representação, V está contido no normalizador de U que tem índice 4 em G. Logo V é um subgrupo normal de ordem $1, 2, 3$, ou 6.

- Se a ordem é 3 ou 6 então V possui um 3-Sylow e como V é normal em G, seria o único 3-Sylow de G, absurdo.
- Se a ordem é 2 então $K(x)^V | K(x)^G$ é Galoisiana de grau 12. Novamente pelo corolário 6 v_1 e v_3 se ramificam em $K(x)^V$ com índice de ramificação 2. Como $e_3 = 4$ temos que os $(r =)6$ prolongamentos de v_3 a $K(x)^V$ se ramificam em $K(x)$ com índice de ramificação 2. Mas $r \leq 3$ absurdo.

Logo resta somente o caso de ordem 1 e com isso G é isomorfo a S_4.

Identifiquemos os geradores. Seja N correspondente a A_4 (normal de índice 2), então v_1 e v_3 se ramificam em $K(x)^N | K(x)^G$ e v_2 se decompõe em $K(x)^N$.

Assim, a valorização que prolonga v_3 em $K(x)^N$ se ramifica em $K(x)|K(x)^N$ com índice 2 e os dois prolongamentos de v_2 a $K(x)^N$ se ramificam com índice 3. Que é isso? É o caso do tetraedro em $K(x)|K(X)^N$! Logo se w_3 é um prolongamento de v_3 a K(x) temos (como antes) $y \in K(x)$, σ e ρ automorfismos em N tais que: $div(y) = w_3 - \tilde{w}_3$, $w_3(y) > 0$ e $\tilde{w}_3(y) < 0$ e $N =< \sigma, \rho >$ onde $\sigma(y) = -y$ e $\rho(y) = a\frac{y-1}{y+1}$ com $a^2 = -1$.

Como σ é permutação de ordem 2 em A_4, ela é um quadrado em S_4, logo $\sigma = \mu^2$ para algum $\mu \in G$. Pelo caso cíclico, como $K(x)|K(x)^{<\mu>}$ tem grau 4 temos 3 valorizações totalmente ramificadas. Ora, $w_3\sigma^{-1} = w_3$, logo w_3 é uma delas e portanto $w_3\mu^{-1} = w_3$, donde $\mu(y) = cy + d$, usando $\mu^2 = \sigma$, $c^2 = -1$ e $d = 0$.

- Se $a = c$ então tome $\mu(y) = ay$, $\sigma(y) = -y$ e $\rho(y) = a\frac{y-1}{y+1}$. Logo, $G =< N, \mu >=< \sigma, \rho, \mu >=< \rho, \mu >$.
- Se $a \neq c$ então seja $\rho' = \rho\sigma$, $c = -a$. Com isso temos $\mu(y) = cy$, $\sigma(y) = -y$ e $\rho' = c\frac{y-1}{1+y}$. Logo $G =< N, \mu >=< \sigma, \rho', \mu >=< \rho', \mu >$.

Na esfera, como vimos, os prolongamentos de v_3 correspondem aos pontos 0, ∞, 1, -1, i e $-i$ de $\mathbb{C} \cup \{\infty\}$ e estes definem um octaedro regular na esfera. Agora, o conjunto dos prolongamentos de v_1 é o único subconjunto de $S_{\mathbb{C}(y)|\mathbb{C}}$ com 12 elementos, onde G age transitivamente. E os prolongamentos de v_2 formam o único subconjunto com 8 elementos de $S_{\mathbb{C}(y)|\mathbb{C}}$ onde G age transitivamente. Logo:

- Os prolongamentos de v_1 correspondem aos pontos médios das arestas.
- Os prolongamentos de v_2 correspondem aos baricentros das faces do octaedro.

3.5 O Grupo do Icosaedro

Neste caso $r = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 5$ e $n = 60$.

Primeiro verifica-se que G é simples, pois se existe N subrgupo normal próprio então $K(x)|K(x)^N$ e $K(x)^N|K(x)^G$ são Galoisianas e se enquadram nas 3 primeiras possibilidades do corolário 6. Em cada caso, ocorre uma contradição, assim existe $f : G \to A_5$ isomorfismo.

Como $A_5 =< \tilde{\sigma}, \tilde{\mu} >$ onde $\tilde{\sigma} = (12345)$ e $\tilde{\mu} = (12)(45)$ com as relações $\tilde{\sigma}^2 = \tilde{\tau}^2 = (\tilde{\sigma}\tilde{\tau})^2 = \tilde{\mu}^2 = (\tilde{\mu}\tilde{\tau})^2 = (\tilde{\mu}\tilde{\sigma})^3 = id$ e $\tilde{\tau} = (15)(24)$. O mesmo acontece com G, tomando imagens inversas pela f. Logo $G =< \sigma, \mu >$ com as mesmas relações.

Agora $U =< \sigma, \tau >$ é subgrupo isomorfo ao grupo diedral D_5 de ordem 10. Logo em $K(x)|K(x)^U$ estamos no caso diedral e portanto temos $y \in K(x)$ tal que $\sigma(y) = cy$ e $\tau(y) = \frac{1}{y}$ com c raíz 5-primitiva da unidade em K.

Seja $\mu(y) = \frac{ay+b}{ey+d}$, como $\mu^2 = id$ temos $b(a+d) = e(a+d) = 0$, assim:

- Se $(a+d) \neq 0$ então $b = e = 0$ e $\mu(y) = \tilde{a}y$ onde $\tilde{a}^2 = 1$, mas $\mu \neq id$ logo $\tilde{a} = -1$. Com isso, $(\mu\sigma)(y) = -cy$ onde c é raíz 10 primitiva da unidade e $(\mu\sigma)^3 = id$ contradição. Logo $a + d = 0$.

- Se $a = d = 0$ então $\mu(y) = \frac{\tilde{b}}{y}$, donde $(\mu\sigma)(y) = \frac{\tilde{b}c}{y}$ e $(\mu\sigma)^2 = id$. Contradição com $(\mu\sigma)^3 = id$. Logo $a = -d \neq 0$.

- Segue que $\mu(y) = \frac{y+b}{ey-1}$. Logo $(\mu\tau)(y) = \mu(\frac{1}{y}) = \frac{ey-1}{y+b}$. Como $(\mu\tau)^2 = id$ temos $\mu(y) = \frac{y+b}{-by-1}$.

- Finalmente, como $(\mu\sigma)(y) = \frac{cy+bc}{-by-1}$ e $(\mu\sigma)^3 = id$ temos $c^2 - b^2c - c + 1 = 0$. Logo $b = \pm i(c + c^4)$ e μ está determinada.

Na esfera, vamos tomar $c = e^{\frac{2\pi i}{5}}$. Agora um prolongamento de v_3 a $\mathbb{C}(y)$ corresponde ao ponto 0 de $\mathbb{C} \cup \{\infty\}$. Seguindo a órbita pelo grupo G (usando $b = -i(c + c^4)$), temos que os 12 prolongamentos de v_3 correspondem aos pontos

$$0, \ \infty, \ i(c + c^4)c^j, \ i(c^2 + c^3)c^j, \text{ onde } j = 0, 1, 2, 3, 4$$

Mas estes pontos definem um icosaedro na esfera. Novamente analisando a quantidade dos subconjuntos onde G age transitivamente temos:

- Os prolongamentos de v_1 correspondem aos pontos médios das arestas do icosaedro.

- Os prolongamentos de v_2 correspondem aos baricentros das faces do icosaedro.

Nota: Para verificar se os poliedros são realmente regulares use as seguintes fórmulas sobre distâncias na esfera de Riemann:

$$d(w, w') = \frac{2|z - z'|}{\sqrt{(1 + |z|^2)(1 + |z'|^2)}} \text{ se } z' \neq \infty$$

e

$$d(w, w') = \frac{2}{\sqrt{1 + |z|^2}} \text{ se } z' = \infty$$

onde z e z' são as projeções estereográficas de w e w'.

References

[1] Aschbacher (1986) Finite Group Theory. Cambridge Studies in Advanced Mathematics.

[2] Garcia, A. Lequain, Y. (1980) Curso de Álgebra. Projeto Euclides.

[3] João Pedro e Matheus. Notas de Seminário.

[4] Jones,G. Singerman, D. Complex Functions an algebraic and geometric viewpoint.

[5] Kaleff, A.M. Rei, D.M. Varetas, Canudos, Arestas e Sólidos Geométricos. RPM 28. pg. 29-36.

[6] Mondek, P. (1988) Os Grupos Finitos de Automorfismos da Esfera de Riemann. Dissertação de Mestrado.

[7] Serre JP. Local Fields. Springer-Verlag.

[8] Stichtenoth, H. (1993) Algebraic Function Fields and Codes. Springer-Verlag.

[9] Stöhr, K.O. (2002) Curso de Corpos de Funções Algébricas, Notas de Aula. IMPA.