Edney Augusto Jesus de Oliveira

Singularidades de Curvas Definidas por Anéis de Representações

Belo Horizonte

2016

Edney Augusto Jesus de Oliveira

Singularidades de Curvas Definidas por Anéis de Representações

Este exemplar corresponde à redação final da tese defendida por **Edney Augusto Jesus de Oliveira.** Tese apresentada ao Instituto de Ciências Exatas, ICEX, como requisito parcial para obtenção do título de **DOUTOR EM MATEMÁTICA**.

Universidade Federal de Minas Gerais – UFMG

Instituto de Ciências Exatas

Departamento de Matemática

Orientador: Renato Vidal da Silva Martins

Coorientador: André Gimenez Bueno

Belo Horizonte

2016

Edney Augusto Jesus de Oliveira

Singularidades de Curvas Definidas por Anéis de Representações

Este exemplar corresponde à redação final da tese defendida por **Edney Augusto Jesus de Oliveira.** Tese apresentada ao Instituto de Ciências Exatas, ICEX, como requisito parcial para obtenção do título de **DOUTOR EM MATEMÁTICA**.

Belo Horizonte, 07 de outubro de 2016:

Renato Vidal da Silva Martins
Orientador

André Gimenez Bueno
Coorientador

Csaba Schneider

Eduardo Tengan

Ethan Guy Cotterill

André Luís Contiero

Belo Horizonte
2016

Agradecimentos

Agradeço aos professores Renato Vidal da Silva Martins e André Gimenez Bueno pela orientação competente e ao mesmo tempo companheira, por acreditarem em mim, até mesmo quando eu duvidava de minhas capacidades.

Aos colegas do programa de pós-graduação em Matemática da UFMG, em especial à Gheyza Ferreira da Silva.

Às secretárias Andrea e Kelli da secretaria do PGMAT por toda paciência e gentileza.

À todos os professores do DMAT-UFMG que fizeram parte desta jornada.

Ao DEMAT-UFOP pelo apoio.

Agradeço a minha amada esposa Monique pelo apoio e paciência necessária no dia a dia deste doutoramento.

Aos meus pais Lourdes e Geraldo (*in memorian*) por serem meus heróis.

Resumo

Seja G um grupo finito de ordem n e ξ uma raiz n-ésima primitiva da unidade. Considere a curva afim $C := \mathrm{Spec}\,(\mathbb{Z}[\xi] \otimes R(G))$ onde$R(G)$ é o anel de representação de G. Estudamos as fibras do feixe tangente formal de C estimando a sua dimensão e determinando (e medindo) as singularidades de C. Lidamos cuidadosamente com três exemplos simples de grupos não-comutativos, tendo como alvo um algoritmo para calcular estes invariantes em geral.

Abstract

Let G be a finite group of order n, and ξ an n-th primitive root of the unity. Consider the affine curve $C := \mathrm{Spec}(\mathbb{Z}[\xi] \otimes R(G))$ where $R(G)$ is the representation ring of G. We study the fibers of the formal tangent sheaf of C by estimating their dimension and also finding (and measuring) the singularities of C. We carefully deal with three simple examples of noncommutative groups, targeting an algorithm to compute these invariants in general.

Sumário

Introdução

Seja G um grupo, A um anel comutativo, e $A[G]$ o anel de grupo associado. É bem conhecido que $A[G]$ é uma álgebra de Hopf que representa um esquema afim diagonalizável sobre A (veja, por exemplo, [CS, Ch. 3], [D] and [Wa]). Se G é abeliano, então $A[G]$ é comutativo e é natural o estudo do esquema afim $X := \mathrm{Spec}(A[G])$. Este estudo é bastante simples quando A é um corpo, especialmente quando G é finito, caso em que as componentes irredutíveis de X são pontos.

Então, o próximo passo é considerar o caso em que $A = \mathbb{Z}$, o que aumenta consideravelmente a complexidade, mesmo que o interesse seja apenas conjuntista. De fato, a estrutura topológica de $\mathrm{Spec}(\mathbb{Z}[G])$ é não-trivial no sentido de que as suas componentes irredutíveis podem se intersectar em vários pontos. Se levado ao nível esquemático, o assunto ganha vários aspectos adicionais a serem abordados. Um deles é identificar e descrever as singularidades por meio de seus invariantes naturais: espaços tangentes, dimensões de mergulho formais, índices de ramificação, etc.. Percebe-se um comportamento, de certo modo, inesperado de tais esquemas aritméticos se comparados com esquemas sobre corpos. Tal estudo foi feito por A. Bueno e M. Dokuchaev em [BD] (baseado em [B]), onde é dada uma completa descrição do esquema $\mathrm{Spec}(\mathbb{Z}[G])$ e seus pontos singulares.

Remover a hipótese de G ser abeliano é o ponto de partida do presente trabalho e o objetivo é obter resultados semelhantes aos de [BD] no caso em que G é não-comutativo. Mas, para isso, note que temos de preservar a comutatividade do anel resultante, por isso, naturalmente, substituímos $\mathbb{Z}[G]$ por $R(G)$, seu *anel de representação* (ou *anel de Green*), já que ambos coincidem quando G é abeliano. Na verdade, uma descrição topológica de $\mathrm{Spec}(R(G))$ pode ser encontrada, por exemplo, em M. Atiyah [A], em G. Segal [Sg] e JP Serre [Sr]. Em tais referências torna-se claro que é melhor lidar com $C := \mathrm{Spec}(\mathbb{Z}[\xi_n] \otimes R(G))$, onde ξ_n é uma raiz primitiva n-ésima da unidade e n é a ordem de G, em vez de $C' := \mathrm{Spec}(R(G))$. Assim, o estudo de C como um esquema é precisamente o que fazemos aqui.

No primeiro capítulo definimos o que uma representação linear de um grupo, apresentamos a definição formal do anel de representação de um grupo, encontramos os caráteres de representações irredutíveis de alguns grupos que serão úteis a posteriori. Ainda neste capitulo reservamos uma seção para o estudo de elementos $p-$regulares de um grupo com p um número primo.

No segundo capítulo estudamos o caso geral e reunimos os resultados que obtivemos em dois teoremas. No Teorema 2.1, analisamos a decomposição de C em componentes irredutíveis, que é a versão esquemática de resultados topológicos dos artigos acima

mencionados. Na segunda parte estudamos os pontos singulares de C. E aí é importante destacar a diferença entre a dimensão do espaço tangente de Zarisky (definido via fibra do feixe tangente) e a dimensão de mergulho formal de um ponto. Estes conceitos concordam se o esquema de base é o espectro de um corpo, o que não é o nosso caso. Então tentamos obter afirmações sobre esses invariantes. Na Teorema 2.2, os pontos de C, ou ao menos de C', são racionais e reduzimos o problema a estudar um esquema zero-dimensional sobre corpos finitos. Em comparação com [B], em ambos os Teoremas 2.1 e 2.2, às vezes obtemos cotas ao invés de igualdades. Isto porque não temos similares da decomposição de G (não abeliano) em grupos cíclicos, então os argumentos são baseados em princípios gerais de feixes, diferenciais e álgebras locais. Por outro lado, note que o nosso Teorema 2.2.(iii) generaliza [B, Teo. 4.1.2, Cor. 4.1.5] no caso racional. A saber, [B, Teo. 4.1.2] é enunciado como segue:

Teorema 4.1.2 (André Gimenez Bueno)**.** Seja G um grupo abeliano finitamente gerado e escreva $G = t(G)\times F$, onde F é a parte livre de G, ie, um grupo abeliano finitamente gerado, cujo posto denotamos por r. Dado um subgrupo H de G, denotamos sua ordem por h. Para um primo $\mathfrak{p}$ de $\mathbb{Z}[G]$, escreva $\mathfrak{m}_\mathfrak{p}$ para o ideal maximal de $(\mathbb{Z}[G])_\mathfrak{p}$ e $\kappa(\mathfrak{p}) = (\mathbb{Z}[G])_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$.

(i) Há uma correspondência biunívoca entre subgrupos cíclicos finitos $H \subseteq G$ e ideais primos minimais aH (os pontos genéricos das componentes) de $\mathbb{Z}[G]$ tal que:

$$\mathrm{Spec}(Z[G]) = \bigcup_H V(\mathfrak{a}_H) \tag{1}$$

é a decomposição de $\mathrm{Spec}(Z[G])$ em componentes irredutíveis. Além disso,

$$V(\mathfrak{a}_H) \cong \mathrm{Spec}(Z[\zeta_h][F]), \tag{2}$$

onde ζ_h é uma $h-$ésima raiz primitiva da unidade, e

$$\mathbb{Q}[t(G)] \cong \prod_H \mathbb{Q}(\zeta_h), \tag{3}$$

é a decomposição de Wedderburn de $\mathbb{Q}[t(G)]$. Para um h fixo dividindo o expoente de $t(G)$, o número de componentes irredutíveis satifazendo (2) é igual ao número de subgrupos cíclicos de G de ordem h. Se $\mathfrak{p}$ é um ponto de interseção, i.e, se pertence ao menos a duas componentes, então $\mathfrak{p}$ está acima de um divisor primo de $|t(G)|$.

(ii) Se $\mathfrak{q} \in \mathrm{Spec}(Z[G])$ pertence a somente uma componente de $\mathrm{Spec}(Z[G])$, digamos $V = \mathrm{Spec}(Z[\zeta_h][F])$, então $\mathrm{Spec}(Z[G])_\mathfrak{q} \cong (Z[\zeta_h][F])_{\tilde{\mathfrak{q}}}$, onde $\tilde{\mathfrak{q}} \in \mathrm{Spec}(Z[\zeta_h][F])$ é o primo correspondente a $\mathfrak{q}$. Em particular, $\mathfrak{q}$ é regular.

(iii) Os pontos singulares fechados de $\mathrm{Spec}(Z[G])$ são exatamente os ideais maximais $\mathfrak{p} \in \mathrm{Spec}(Z[G])$ acima dos divisores primos de $|t(G)|$. Em particular, cada ponto (fechado) singular é um ponto de interseção, i. e. pertence ao menos a duas componentes irredutíveis.

No capítulo 3 estudamos os casos onde G é, respectivamente, o grupo simétrico S_3, o grupo diedral D_4 e o grupo alternado A_4. Encontramos as singularidades, dimensões do espaço tangente e de mergulho das curvas definidas pelos anéis de representação destes grupos usando os vários itens dos Teoremas 2.1 e 2.2 e mesmo de sua prova. As contas são feitas dentro de uma forma sistemática para que o leitor possa entender o que fazer em um caso diferente. O método, no entanto, funciona sob certas condições.

No capítulo 4 esboçamos um algoritmo para encontrar os pontos singulares de C e seus invariantes. Os primeiros passos são muito baseados nos resultados obtidos nos Teoremas 2.1 e 2.2. Para o caso geral em que eventualmente um ponto singular é não racional utilizamos dois métodos a saber: um deles baseado na eliminação de divisores de zero e o outro criando uma correspondência entre o anel que define a curva e um grafo orientado com número finito de vértices.

Por fim deixamos algumas perguntas pertinentes, tais como: (1) No caso em que G é abeliano, ℓ_p representa o número minimal de geradores do $p-$subgrupo de Sylow; o que ℓ_p representaria no caso não abeliano?; (2) Nos casos em que estudamos, todos os pontos singulares de C projetavam sobre pontos racionais de C'. Fica a pergunta se isso sempre ocorre. (3) Seria interessante tentar adaptar os argumentos contidos em [B] e [BD] para grupos não abelianos finitos cuja decomposição racional do anel de representação é conhecida. São assuntos que temos estudado embora sigam em aberto para nós.

1 Preliminares

Neste capítulo, temos como principal objetivo apresentar as definições e resultados da Teoria de Representações necessários para a definição do Anel de Representação do grupo G, o qual denotamos por $R(G)$. Ainda, para ilustrar esses resultados construiremos efetivamente os Anéis de representação dos grupos S_3, D_4 e A_4, os quais serão utilizados no capítulo 3, quando apresentaremos algumas aplicações dos Teoremas 2.1 e 2.2.

Consideraremos ao longo deste capítulo que G sempre representará um grupo finito com identidade e, V um espaço vetorial sobre o corpo dos números complexos $\mathbb{C}$ de dimensão finita m e $GL(V)$ o grupo dos automorfismos de V.

1.1 O Anel de Representações de um Grupo

Definição 1.1. Uma *representação linear* do grupo G no espaço vetorial V é um homomorfismo de grupos

$$\begin{array}{rccc} \rho: & G & \to & GL(V) \\ & g & \mapsto & \rho(g) =: \rho_g \end{array} \tag{1.1}$$

Se é dado ρ uma representação linear de G em V, dizemos que V *é um espaço de representação de* G, ou simplesmente que V é uma *representação* de G, e se a dimensão de V for m, dizemos que m é o grau da representação V.

Observação 1.1. *Note que ρ_g pode ser descrito por uma matriz quadrada $m \times m$ com entradas em $\mathbb{C}$, a qual denotaremos por R_g. Daí,*

$$\det(R_g) \neq 0\,,\ R_{gh} = R_g \cdot R_h, \qquad \forall g,\, h \in G.$$

Com isso, $GL(V) \cong GL_m(\mathbb{C})$. Duas representações lineares ρ_1 e ρ_2 de um mesmo grupo G em dois espaços vetoriais V_1 e V_2 serão ditas isomorfas se existir um isomorfismo linear $\sigma : V_1 \to V_2$ tal que para todo $g \in G$, $\sigma \circ \rho_1(g) = \rho_2(g) \circ \sigma$.

Equivalentemente, dada uma representação ρ, temos uma ação associada de G em V definida da seguinte forma

$$\begin{array}{rccc} \psi_\rho: & G \times V & \to & V \\ & (g, v) & \mapsto & \psi_\rho(g, v) := \rho_g(v) \end{array}$$

note que a construção acima define uma correspondência biunívoca entre representações de G e ações de G em V.

Sejam $\rho : G \to GL(V)$ uma representação linear de G em V e W um subespaço vetorial de V. Suponha que W seja estável sobre a ação de G, isto é, se $w \in W$, então $\forall g \in G$, $\rho_g w \in W$. Com isso, temos que a restrição ρ_g^W de ρ_g em W é um isomorfismo de W em si mesmo, e portanto, temos que $\rho^W : G \to GL(W)$ é uma representação linear de G em W. Neste caso W é dita uma *subrepresentação* de V.

Uma representação linear ρ de G em V é dita *irredutível* se nenhum subespaço vetorial de V é estável sob G, com excessão é claro de $\{0\}$ e do próprio V.

Definição 1.2. Dado ρ uma representação de G em V, definimos o *caráter da representação* ρ, denotado por χ_ρ, como uma função de G em $\mathbb{C}$ dada por

$$\chi_\rho(g) = \mathrm{Tr}(R_g)$$

onde $\mathrm{Tr}(R_g)$ é o traço da matriz R_g da representação ρ em $g \in G$.

Quando uma representação ρ de G em V for irredutível, diremos que χ_ρ é um caráter irredutível de G.

Se χ_ρ um caractere da representação ρ de grau n, temos que para todos $s, t \in G$ são válidas

1. $\chi_\rho(1) = n$.
2. $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$;
3. $\chi_\rho(tst^{-1}) = \chi_\rho(s)$.

Uma função f sobre G que atende a condição (3) acima é também chamada de *função de classe.*

Sejam $\rho_1 : G \to GL(V_1)$ e $\rho_2 : G \to GL(V_2)$ duas representações (lineares) de G tais que R_s^1 e R_s^2 são suas formas matriciais (para cada $s \in G$). Denote por χ_1 e χ_2 os caracteres de ρ_1 e ρ_2 respectivamente. Uma representação para a soma direta entre V_1 e V_2 terá matriz

$$R_s = \begin{pmatrix} R_s^1 & 0 \\ 0 & R_s^2 \end{pmatrix}$$

donde

$$\chi(s) := \mathrm{Tr}\,(R_s) = \mathrm{Tr}\left(R_s^1\right) + \mathrm{Tr}\left(R_s^2\right) := \chi_1(s) + \chi_2(s). \tag{1.2}$$

Com isso, temos que se χ é o caractere da soma direta $V_1 \oplus V_2$, temos que $\chi = \chi_1 + \chi_2$. É possível demonstrar que se temos que se χ é o caractere do produto $V_1 \otimes V_2$, temos que $\chi = \chi_1 \cdot \chi_2$ (onde este produto denota o produto ponto a ponto.).

A seguir, alguns resultados relevantes para esse trabalho.

Proposição 1.2. *Duas representações com o mesmo caráter são isomorfas.*

Uma prova para a proposição acima pode ser obtida em [Sr, Corolário 2, Teo. 4, pág 16].

A seguir, dois resultados sobre a teoria de caráteres, cujas demonstrações podem ser consultadas, por exemplo, em [BC, Teo. 2.3.2].

Proposição 1.3. *Sejam $\chi_1, \ldots, \chi_h$ os caráteres irredutíveis de G, e sejam n_i, $i = 1, \ldots, h$ seus respectivos graus. Então*

$$|G| = \sum_{i=1}^{h} n_i^2. \tag{1.3}$$

Proposição 1.4. *Seja G um grupo finito. O número de representações irredutíveis não isomórifcas do grupo G é igual ao número de classes de conjugações de G.*

Note que a proposição acima nos garante que o número de caráteres irredutíveis de um grupo finito G é finito. Se G for um grupo abeliano finito, temos que $|\mathrm{Cl}(G)| = |G|$, ou seja, cada elemento $x \in G$ define a classe de conjugação $\{x\}$ de G, e neste caso temos que existem $|G|$ caráteres irredutíveis do grupo G, todos eles de grau 1.

O resultado abaixo relaciona o conjunto de caráteres irredutíveis distintos de um grupo G com as funções de classes sobre G:

Proposição 1.5. *Os caráteres irredutíveis distintos de G forma uma base ortonormal para o espaço das funções de classes sobre G.*

Demonstração. Veja [Sr, Teo. 6, pág. 19]. □

Como visto acima, todo caractere de G é uma função de classe sobre G, e portanto, é descrito de forma única como uma combinação linear dos caráteres irredutíveis de G com coeficientes inteiros (e tais coeficientes devem ser inteiros não-negativos, mas tal fato não é necessário para nossos objetivos – para mais consulte [Sr, Cap. 2 e 9]), o qual denotaremos por $R^+(G)$.

Definição 1.3. Sejam G um grupo e $\chi_1, \chi_2, \ldots, \chi_s$ todos os seus caráteres irredutíveis distintos. O *Anel de Representação de G*, ou o *anel dos caracteres virtuais* de G, ou ainda, o *anel de Green* de G, denotado por $R(G)$, é o grupo gerado por

$$R^+(G) := \{a_1\chi_1 + \ldots + a_s\chi_s | 0 \leq a_i \in \mathbb{Z}, \text{ e } \{\chi_1, \ldots, \chi_s\} \text{ os caráteres irredutíveis de } G\}$$

ou seja,

$$R(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_s \tag{1.4}$$

onde $s := |\mathrm{Cl}(G)|$ e a multiplicação em $R(G)$ é induzida pelo produto de caráteres irredutíveis, o qual é feito ponto-a-ponto, ou seja,

$$\chi_i\chi_j(g) := \chi_i(g)\chi_j(g)$$

para todo $g \in G$ e $i, j \in \{1, \ldots, s\}$. Por convenção, adotaremos χ_1 como sendo o carátere tal que $\chi_1(g) = 1$ para todo $g \in G$.

A título de curiosidade, podemos construir o anel $R(G)$ de forma mais geral do seguinte modo: cada representação de $G \to GL(V)$ nos fornece uma ação de G em V, que por sua vez faz de V um $\mathbb{C}[G]$-módulo finitamente gerado cuja ação é definida da seguinte forma:

$$\left(\sum_{g\in G} \lambda_g g\right) \cdot v := \sum_{g\in G} \lambda_g (g \cdot v) := \sum_{g\in G} \lambda_g \rho_g(v)$$

Reciprocamente, dado um $\mathbb{C}[G]$-módulo finitamente gerado obtemos por restrição uma representação de G.

Com isso, pode-se definir formalmente o anel $R(G)$ como o grupo de Grothendieck da categoria de $\mathbb{C}[G]$-módulos finitamente gerados munido da operação de multiplicação induzida pelo produto tensorial, e tendo em vista a completa redutibilidade dos $\mathbb{C}[G]$-módulos pode-se verificar que o anel de representação de um grupo tem a descrição via caráteres irredutíveis dada acima em (1.4).

Para ilustrar as definições acima, apresentamos abaixo o conjunto de caráteres irredutíveis dos grupos S_3, A_4 e D_4, os quais são bem conhecidos na literatura seus conjuntos de caráteres (consulte por exemplo [We], [Sr] e [Mr]), e por esse motivo não exibimos os detalhes de como tais caráteres são obtidos. A escolha de tais exemplos é estratégica para o desenvolvimento do Capítulo 3.

O Grupo Simétrico S_3

Considere o grupo das permutações de três elementos

$$\begin{array}{ccc} \sigma_1 = e & \sigma_2 = (1\,2) & \sigma_3 = (1\,3) \\ \sigma_4 = (2\,3) & \sigma_5 = (1\,2\,3) & \sigma_6 = (1\,3\,2) \end{array}$$

onde e é a permutação identidade. Tomando $\sigma = (1\,2\,3)$ e $\tau = (1\,2)$ podemos reescrever S_3 como

$$S_3 = \left[\{\sigma, \tau \,|\, \sigma\tau = \tau\sigma^2\}\right] = \{e,\, \sigma,\, \sigma^2,\, \tau,\, \tau\sigma,\, \tau\sigma^2\},$$

donde

$$\mathrm{Cl}\,(S_3) = \{c_1 = \{e\}, c_2 = \{\sigma, \sigma^2\}, c_3 = \{\tau, \tau\sigma, \tau\sigma^2\}\}.$$

Com a notação acima, temos que o conjunto de caráteres de S_3, $\{\chi_1,\, \chi_2\, \chi_3\}$ é descrito pela tabela

	c_1	c_2	c_3
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

(1.5)

Note que o número de caráteres e os seus respectivos graus estão em concordância com os resultados citados acima (Proposição 1.4, Teorema 1.3 e Proposição 1.2).

O grupo Alternado A_4

Considere o grupo alternado $A_4 = \{\sigma_i\}_{i=1}^{12}$ com

$$\begin{array}{cccc} \sigma_1 = e & \sigma_2 = (1\,2)(3\,4) & \sigma_3 = (1\,3)(2\,4) & \sigma_4 = (1\,4)(2\,3) \\ \sigma_5 = (1\,2\,3) & \sigma_6 = (1\,2\,4) & \sigma_7 = (1\,3\,2) & \sigma_8 = (1\,3\,4) \\ \sigma_9 = (1\,4\,2) & \sigma_{10} = (1\,4\,3) & \sigma_{11} = (2\,3\,4) & \sigma_{12} = (2\,4\,3) \end{array}$$

donde verificamos que o conjunto das classes de conjugação de A_4 é

$$\mathrm{Cl}\,(A_4) = \{c_1 = \{\sigma_1\},\ \ c_2 = \{\sigma_2, \sigma_3, \sigma_4\},\ \ c_3 = \{\sigma_6, \sigma_7, \sigma_{10}, \sigma_{11}\},\ \ c_4 = \{\sigma_5, \sigma_8, \sigma_9, \sigma_{12}\}\}\,.$$

Com a notação acima, temos que o conjunto de caráteres de A_4, $\{\chi_1,\ \chi_2\,\chi_3, \chi_4\}$[1] é descrito pela tabela

	c_1	c_2	c_3	c_4
χ_1	1	1	1	1
χ_2	1	1	w	w^2
χ_3	1	1	w^2	w
χ_4	3	-1	0	0

(1.6)

onde $w^3 = 1$ com $w \neq 1$.

O Grupo Diedral D_4

Considere o grupo de de simetrias (coplanares) de um polígono regular de k vértices, o grupo diedral D_k. Tal grupo pode ser descrito por

$$D_k = \left[\{r,\ s | r^k = s^2 = e,\ \ sr = r^{k-1}s,\}\right]$$

onde s é uma reflexão com respeito a alguma diagonal ou diâmetro do polígono e r uma rotação (plana) em torno do centro do polígono de $2\pi/k$ radianos.

O conjunto das classes de equivalência de D_k é dado em dois casos distintos:

a) Se k for um número ímpar, então

$$\mathrm{Cl}(D_k) = \left\{\{e\}, \{r, r^{k-1}\}, \ldots, \{r^{\frac{k-1}{2}}, r^{\frac{k+1}{2}}\}, \{s, sr, sr^2, sr^3, sr^4, \ldots, sr^{k-1}\}\right\}$$

e ainda, $\#\mathrm{Cl}(D_k) = \frac{k+3}{2}$.

[1] Mesmo utilizando a mesma notação do caso S_3, não haverá risco de confusão pois estudamos cada caso separadamente.

b) Se n for um número par, então

$$\mathrm{Cl}(D_k) = \Big\{\{e\}, \{r, r^{k-1}\}, \ldots, \{r^{\frac{k-2}{2}}, r^{\frac{k+2}{2}}\}, \{r^{\frac{k}{2}}\}, \{s, sr^2, sr^4, \ldots, sr^{k-2}\}, \{sr, sr^3, \ldots, sr^{k-1}\}\Big\}$$

e ainda, $\#\mathrm{Cl}(D_k) = \frac{k+6}{2}$.

Para simplificar, optamos no caso de D_k descrever os caracteres por sua ação nos elementos de D_k r^n e sr^n $(n = 0, \ldots, k-1)$. Com isso, temos que o conjunto de caráteres de D_k, é descrito por

a) k par:

	r^n	sr^n
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^n$	$(-1)^n$
χ_4	$(-1)^n$	$(-1)^n$
χ_h	$2\cos\left(\frac{2\pi(h-4)n}{n}\right)$	0

com $4 < h < k/2$.

b) k ímpar:

	r^n	sr^n
χ_1	1	1
χ_2	1	-1
χ_h	$2\cos\left(\frac{2\pi(h-4)n}{n}\right)$	0

com $2 < h < (k-1)/2$.

Para o caso $k = 4$, temos

$$\mathrm{Cl}(D_4) = \Big\{c_1 = \{e\},\ c_2 = \{r, r^3\},\ c_3 = \{r^2\},\ c_4 = \{s, sr^2\},\ c_5 = \{sr, sr^3\}\Big\}.$$

Assim, conjunto de caráteres de D_4, $\{\chi_1,\ \chi_2\,\chi_3, \chi_4, \chi 5\}$ é descrito pela tabela

	c_1	c_2	c_3	c_4	c_5
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	0	-2	0	0

(1.7)

1.2 Elementos regulares de um grupo

Nesta seção apresentamos uma caracterização para elementos de um grupo finito G que será utilizada na demonstração do Teorema 2.1 adiante.

Definição 1.4. Sejam $p \in \mathbb{Z}$ um número primo e G um grupo finito.

(i) Dizemos que um elemento $g \in G$ é um *p-elemento* (ou um elemento *p-unipotente*) se $\text{ord}(g) = p^m$ para algum $m \in \mathbb{N}$.

(ii) Dizemos que um elemento $g \in G$ é um *p'-elemento* (ou um elemento *p-regular*) se $\text{mdc}\,(\text{ord}(g), p) = 1$.

Um fato importante é que dados $p \in \mathbb{Z}$ um número primo e $g \in G$ um elemento qualquer do grupo, podemos sempre escrever de forma única o seguinte

$$g = g_{u,p} \cdot g_{r,p} \tag{1.8}$$

tal que $\text{ord}(g_{r,p}) = p^m$ para algum $m \in \mathbb{N}$ e $p \nmid \text{ord}(g_{u,p})$ e que os elementos $g_{u,p}$ e $g_{r,p}$ comutam. De fato, tome o subgrupo cíclico gerado por g, o qual é abeliano e portanto admite decomposição única em $p-$subgrupos. Para mais detalhes veja por exemplo [BJN, Lema 3.3, cap. 8].

Neste contexto, os elementos $g_{u,p}$ e $g_{r,p}$ são respectivamente chamados de componentes *p-unipotente* e *p-regular* de g em G. Por exemplo, sejam $\sigma = (1\ 4\ 2\ 3) \in A_4$ e $p = 2$, temos

$$\sigma_{u,2} = \text{Id} \text{ e } \sigma_{r,2} = (1\ 4\ 2\ 3)$$

onde $\text{ord}(\sigma_{r,2}) = 2^2$ e $\text{ord}(\sigma_{u,2}) = 1$ o qual é coprimo com $p = 2$.

Outra importante definição é

Definição 1.5. Sejam $p \in \mathbb{Z}$ um número primo e $c \in \text{Cl}(G)$ uma classe de conjugação do grupo finito G. Definimos

$$c(p) := \{g_{r,p}\}_{g \in c}. \tag{1.9}$$

Para ilustrar a definição acima, vejamos os seguintes exemplos estratégicos para essa tese

Exemplo 1.1. *Na definição acima, considere $G = S_3$. Sejam*

$$c_1 = \{e\}, \quad c_2 = \{r, r^2\}, \quad c_3 = \{s, sr, sr^2\}$$

as classes de conjugação de S_3. Para cada p primo, determinaremos $c_i(p)$ dado em (1.9):

a) $p = 2$*:*

$c_1 = \{e\}$
assim $c_1(2) = \{e\} = c_1$*;*

$c_2 = \{r, r^2\}$
$\text{ord}\,(r) = 3$; então $(r)_{u,2} = e$, $(r)_{r,2} = r$
$\text{ord}\,(r^2) = 3$; então $(r^2)_{u,2} = e$, $(r^2)_{r,2} = r^2$
assim $c_2(2) = \{r, r^2\} = c_2$*;*

$c_3 = \{s, sr, sr^2\}$
$\text{ord}\,(s) = 2$; então $(r)_{u,2} = s$, $(r)_{r,2} = e$
$\text{ord}\,(sr) = 2$; então $(sr)_{u,2} = sr$, $(sr)_{r,2} = e$
$\text{ord}\,(sr^2) = 2$; então $(sr^2)_{u,2} = sr^2$, $(sr^2)_{r,2} = e$
assim $c_3(2) = \{e\} = c_1$*.*

b) $p = 3$*:*

$c_1 = \{e\}$
assim $c_1(3) = \{e\} = c_1$*;*

$c_2 = \{r, r^2\}$
$\text{ord}\,(r) = 3$; então $(r)_{u,3} = r$, $(r)_{r,3} = e$
$\text{ord}\,(r^2) = 3$; então $(r^2)_{u,3} = r^2$, $(r^2)_{r,3} = e$
assim $c_2(3) = \{e\} = c_1$*;*

$c_3 = \{s, sr, sr^2\}$
$\text{ord}\,(s) = 2$; então $(r)_{u,3} = e$, $(r)_{r,3} = s$
$\text{ord}\,(sr) = 2$; então $(sr)_{u,3} = e$, $(sr)_{r,3} = sr$
$\text{ord}\,(sr^2) = 6 = 2 \times 3$; então $(sr^2)_{u,3} = e$, $(sr^2)_{r,3} = sr^2$
assim $c_3(3) = \{s, sr, sr^2\} = c_3$*.*

c) $p > 3$*: Primeiro note que os únicos divisores primos de* $|S_3|$ *são* 2 *e* 3*, e pelo teorema de Lagrange, temos que dado* $p \neq 2, 3$*, não existe nenhum elemento* $x \in S_3$ *tal que* $ord(x) = p$*. Assim, para todo* $x \in S_3$*,*

$$(x)_{u,p} = e, \quad (x)_{r,p} = x$$

e portanto, $c_i(p) = c_i$ *para* $i = 1, 2, 3$*,* $p \neq 2, 3$*.*

Exemplo 1.2. *Agora, utilizando o mesmo racíocinio utilizado no exemplo anterior para os grupos* D_4 *e* A_4*, temos*

(i) Para D_4, temos:

a) Para $p = 2$ obtemos que $c_1(2) = c_2(2) = c_3(2) = c_4(2) = c_5(2) = \{e\} = c_1$.

b) Para $p \neq 2$ obtemos que $c_i(p) = c_i$, para $i = 1, 2, 3, 4, 5$.

(ii) Para A_4, temos:

a) Para $p = 2$, obtemos que $c_1(2) = c_2(2) = c_1$, $c_3(2) = c_3$ e $c_4(2) = c_4$.

b) Para $p = 3$, obtemos que $c_1(3) = c_3(3) = c_4(3) = c_1$ e $c_2(3) = c_2$.

c) Para $p \neq 2, 3$ obtemos que $c_i(p) = c_i$ para $i = 1, 2, 3, 4$.

2 O Caso Geral

O objetivo deste capítulo é estudar as singularidades da curva afim C, mas primeiro relembramos alguns conceitos importantes sobre pontos de esquemas.

2.1 Espaço Tangente, Dimensão de Mergulho e Pontos Racionais

Definição 2.1. Seja X um esquema sobre Y e $P \in X$ um ponto arbitrário. Seja também $\mathcal{O}_P$ o anel local de P sobre X e $\mathfrak{m}_P$ o seu ideal maximal. Seja $k_P := \mathcal{O}_P/\mathfrak{m}_P$ o seu corpo residual. O *espaço tangente de Zariski* de X/Y em P é definido por

$$T_P X = T_P(X/Y) := \mathrm{Hom}_{k_P}(\Omega_{X/Y} \otimes_{\mathcal{O}_X} k_P, k_P)$$

onde $\Omega_{X/Y}$ é o feixe de diferenciais. Lembre que $\Omega_{X/Y} \otimes_{\mathcal{O}_X} k_P$ é um feixe skyscrapper suportado em P e é identificado aqui com seu stalk em P, que é um k_P espaço vetorial e a definição faz sentido.

Define-se a *dimensão de mergulho formal (local)* de X em P como

$$\mathrm{edim}_P(X) := \dim_{k_P}(\mathfrak{m}_P/\mathfrak{m}_P^2).$$

O ponto P é dito *regular* (ou *suave*, ou *não singular*)[1], se $\mathcal{O}_P$ é regular, ou seja,

$$\mathrm{edim}_P(X) = \dim(\mathcal{O}_P)$$

onde $\dim(\mathcal{O}_P)$ refere-se à dimensão de Krull. O ponto é dito ser *singular* caso contrário.

Para o restante deste trabalho, consideraremos G um grupo finito, $n := |G|$ a ordem de G, $\mathrm{Cl}(G)$ o conjunto das classes de G, $s := |\mathrm{Cl}(G)|$. Consideraremos também a curva afim

$$C := \mathrm{Spec}(\mathbb{Z}[\xi_n] \otimes_{\mathbb{Z}} R(G)).$$

onde $\xi_n := e^{2\pi i/n}$ é uma raiz n-ésima primitiva da unidade, e

$$C' := \mathrm{Spec}(R(G)).$$

com o qual o seguinte diagrama comuta

$$\begin{array}{ccc} C & \xrightarrow{\pi'} & C' \\ {\scriptstyle\pi}\downarrow & \swarrow & \\ \mathrm{Spec}(\mathbb{Z}) & & \end{array}$$

onde π e π' são os morfismos de projeção natural.

[1] Aqui tais definições são coincidentes uma vez que estamos estudando um esquema unidimensional

Teorema 2.1. *As seguintes afirmações são verdaderias:*

(I) Existe uma correspondência biunívoca entre classes de conjugação $c \in \mathrm{Cl}(G)$ e ideais primos minimais I_c (os pontos genéricos das componentes) de $\mathbb{Z}[\xi_n] \otimes_{\mathbb{Z}} R(G)$ tal que

$$C = \bigcup_{c \in \mathrm{Cl}(G)} V(I_c)$$

é a decomposição de C em componentes (irredutíveis). Mais ainda,

$$V(I_c) \cong \mathrm{Spec}(\mathbb{Z}[\xi_n])$$

para cada $c \in \mathrm{Cl}(G)$.

(II) Seja $P \in C$ tal que $\pi(P) = p$. Então:

(i) P é singular se e somente se P pertence a pelo menos duas componentes de C;

(ii) se P é singular, então $p|n$;

(iii) $\dim(T_P C) \leq \mathrm{edim}_P(C)$;

(iv) se $p \notin P^2$, então $\dim(T_P C) < \mathrm{edim}_P(C)$;

(v) se existe $x \in R(G)$ com $x \not\equiv 0 \pmod p$ e $x^r \equiv 0 \pmod p$ então $\dim(T_P C) \geq 1$ para algum $P \in \pi^{-1}(p)$;

(vi) $\mathrm{edim}_P(C) \leq 1 + \log_p(\phi(n) \cdot s)$, onde ϕ é a função de Euler.

Demonstração. Considere $\xi := \xi_n$ e $\mathbb{Z}[\xi]^{\mathrm{Cl}(G)}$ o anel das funções sobre $\mathrm{Cl}(G)$ com valores em $\mathbb{Z}[\xi]$. Considere as injeções naturais

$$\mathbb{Z}[\xi] \longrightarrow \mathbb{Z}[\xi] \otimes R(G) \longrightarrow \mathbb{Z}[\xi]^{\mathrm{Cl}(G)}$$

definidas por

$$\begin{array}{ccc} \mathbb{Z}[\xi] & \longrightarrow & \mathbb{Z}[\xi] \otimes R(G) \\ \xi & \longmapsto & \xi \otimes \chi_1 \end{array} \qquad \begin{array}{ccc} \mathbb{Z}[\xi] \otimes R(G) & \longrightarrow & \mathbb{Z}[\xi]^{\mathrm{Cl}(G)} \\ \xi \otimes \chi_i & \longmapsto & \xi \chi_i \end{array}$$

então, podemos supor que $\mathbb{Z}[\xi] \subset \mathbb{Z}[\xi] \otimes R(G) \subset \mathbb{Z}[\xi]^{\mathrm{Cl}(G)}$.

Isto produz a seguinte sequência de projeções

$$\mathrm{Spec}(\mathbb{Z}[\xi]^{\mathrm{Cl}(G)}) \xrightarrow{\varphi} C \longrightarrow \mathrm{Spec}(\mathbb{Z}[\xi]).$$

Seguindo [Sr, pág. 86], pode se dar uma descrição mais detalhada do morfismo φ acima. De fato, em primeiro lugar, pode-se naturalmente identificar

$$\mathrm{Spec}(\mathbb{Z}[\xi]^{\mathrm{Cl}(G)}) = \mathrm{Cl}(G) \times \mathrm{Spec}(\mathbb{Z}[\xi])$$

da seguinte maneira: dado qualquer ideal primo $M \in \mathbb{Z}[\xi]$ e qualquer classe de conjugação $c \in \mathrm{Cl}(G)$, associamos o ideal primo $M_c \in \mathbb{Z}[\xi]^{\mathrm{Cl}(G)}$ consistindo das funções $f \in \mathbb{Z}[\xi]^{\mathrm{Cl}(G)}$ tal que $f(c) \in M$. Claramente

$$\begin{array}{rccc} \varphi: & \mathrm{Spec}(\mathbb{Z}[\xi]^{\mathrm{Cl}(G)}) & \longrightarrow & C \\ & M_c & \longmapsto & M_c \cap (\mathbb{Z}[\xi] \otimes R(G)) \end{array}$$

Como $M_c \cap \mathbb{Z}[\xi] = M$, temos que $\varphi(M_c) = \varphi(N_c)$ se e somente se $M = N$.

Assim, em nível apenas conjuntista, C é a união de s cópias de $\mathrm{Spec}(\mathbb{Z}[\xi])$ – uma para cada classe $c \in \mathrm{Cl}(G)$ – que podem, eventualmente, se interceptar, como veremos em (2.1) a seguir. Com o objetivo pôr a afirmação acima dentro de um âmbito algébrico (esquemático), para cada $c \in \mathrm{Cl}(G)$ defina

$$J_c := \{f \in \mathbb{Z}[\xi]^{\mathrm{Cl}(G)} \mid f(c) = 0\} \quad \text{e} \quad I_c := J_c \cap (\mathbb{Z}[\xi] \otimes R(G)).$$

Então,

$$C = \bigcup_{c \in \mathrm{Cl}(G)} V(I_c)$$

que é a decomposição de C em componentes irredutíveis, uma vez que, por construção, os I_c são precisamente os primos minimais de $\mathbb{Z}[\xi] \otimes R(G)$, uma vez que o morfismo φ é finito. Além disso, cada aplicação

$$\begin{array}{ccc} \mathrm{Spec}(\mathbb{Z}[\xi]) & \longrightarrow & V(I_c) \\ M & \longmapsto & M_c \cap (\mathbb{Z}[\xi] \otimes R(G)) \end{array}$$

é claramente um isomorfismo, e então (I) está provado.

Para provar (II), primeiro lembramos que dado um número primo $p \in \mathbb{Z}$, e algum $g \in G$, por (1.8), podemos escrever

$$g = g_u \cdot g_r$$

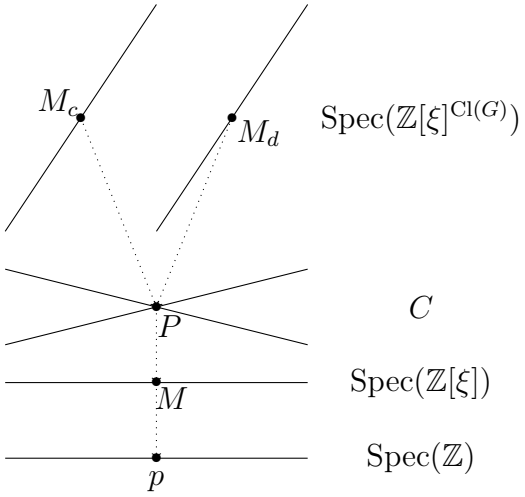
onde tal produto é único e comutativo com $\mathrm{ord}(g_u) = p^m$ para algum $m \in \mathbb{N}$ e $p \nmid \mathrm{ord}(g_r)$. Seja $c(p)$ dado na Definição 1.5. Se o corpo residual de M é de característica p segue de [Sr, Proposição 30'] que

$$\varphi(M_c) = \varphi(M_d) \iff c(p) = d(p). \tag{2.1}$$

Dado $P \in C$, tome $M \in \mathrm{Spec}(\mathbb{Z}[\xi])$ e $c \in \mathrm{Cl}(G)$ tais que $P = \varphi(M_c)$. Se $p \nmid n$, então $d(p) = d$ para todo $d \in \mathrm{Cl}(G)$; em particular, $\varphi(M_c) \neq \varphi(M_d)$ para todo $d \neq c$, assim $V(I_c)$ é a única componente irredutível a qual P pertence. Além disso, como visto no item (I), toda componente irredutível de C é isomórfica a $\mathrm{Spec}(\mathbb{Z}[\xi])$, a qual é uma curva suave, assim (II).(i) e a necessidade em (II).(ii) seguem. Agora se P pertence ao menos duas componentes, então $\mathcal{O}_P$ tem ao menos dois primos minímais, mas se é assim,

$\mathcal{O}_P$ não é um domínio. Por outro lado, por [Mt, Thm. 14.3], qualquer anel local regular (Noetheriano), então a suficiência em (II).(i) segue.

Ilustramos o que foi dito acima na imagem abaixo.



Para provar (II).(iii), note que $\mathcal{O}_P$ é uma $\mathbb{Z}$-álgebra, e assim temos a seguinte sequência exata de k_P-espaços vetoriais

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \xrightarrow{d} \Omega_{\mathcal{O}_P/\mathbb{Z}} \otimes_{\mathcal{O}_P} k_P \longrightarrow \Omega_{k_P/\mathbb{Z}} \longrightarrow 0 \tag{2.2}$$

onde "d" é a aplicação derivação; por outro lado a sequência natural de homomorfismo de anéis

$$\mathbb{Z} \longrightarrow \mathbb{F}_p \longrightarrow k_P$$

produz a seguinte sequência exata de k_P-espaços vetoriais

$$\Omega_{\mathbb{F}_p/\mathbb{Z}} \otimes_{\mathbb{F}_p} k_P \longrightarrow \Omega_{k_P/\mathbb{Z}} \longrightarrow \Omega_{k_P/\mathbb{F}_p}. \tag{2.3}$$

Seja $R := \mathbb{Z}[\xi] \otimes R(G)$. Como P é um ideal maximal, temos que $k_P \cong R/P$, e portanto k_P é uma álgebra finitamente gerada sobre $\mathbb{F}_p$. Ainda, por [Wa, A.8], $k_p \supset \mathbb{F}_p$ é uma extensão finita e, como $\mathbb{F}_p$ é um corpo perfeito, temos que k_P é uma extensão separável de $\mathbb{F}_p$, daí $\Omega_{k_P/\mathbb{F}_p} = 0$. Segue do epimorfismo $\mathbb{Z} \to \mathbb{F}_P$ que $\Omega_{\mathbb{F}_p/\mathbb{Z}} = 0$, portanto, de (2.3), deduzimos que $\Omega_{k_P/\mathbb{Z}} = 0$, e, de (2.2), obtemos a aplicação linear sobrejetiva

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \twoheadrightarrow \Omega_{\mathcal{O}_P/\mathbb{Z}} \otimes_{\mathcal{O}_P} k_P. \tag{2.4}$$

Agora

$$\begin{aligned}
\Omega_{C/\mathrm{Spec}(\mathbb{Z})} \otimes_C k_P &:= (\Omega_{C/\mathrm{Spec}(\mathbb{Z})} \otimes_{\mathcal{O}_C} k_P)_P \\
&= (\Omega_{C/\mathrm{Spec}(\mathbb{Z})})_P \otimes_{\mathcal{O}_P} (k_P)_P \\
&= (\Omega_{R/\mathbb{Z}})_P \otimes_{R_P} k_P \\
&= \Omega_{R_P/\mathbb{Z}} \otimes_{R_P} k_P \\
&= \Omega_{\mathcal{O}_P/\mathbb{Z}} \otimes_{\mathcal{O}_P} k_P.
\end{aligned}$$

Em particular

$$\dim(T_P C) = \dim(\Omega_{\mathcal{O}_P/\mathbb{Z}} \otimes_{\mathcal{O}_P} k_P) \tag{2.5}$$

e (II).(iii) segue de (2.4).

Para provar (II).(iv), note que se $p \notin P^2$ então sua classe é não nula em $\mathfrak{m}_P/\mathfrak{m}_P^2$. Mas a aplicação derivada d definida em (2.2) se anula em todos os elementos da imagem de $P \cap \mathbb{Z}$ em $\mathfrak{m}_P/\mathfrak{m}_P^2$. Em particular $d(p) = 0$, mas como p é não nulo, temos que $\ker(d) \neq 0$, e uma vez que d é sobrejetiva por (2.4), segue que $\dim(T_P C) < \operatorname{edim}_P(C)$ por (2.5).

Para provar (II).(v), tome $x \in R(G)$ com $x \not\equiv 0 \bmod p$ tal que $x^r \equiv 0 \bmod p$ para algum $r \geq 2$. Então $(1 \otimes x) \otimes 1$ é um elemento nilpotente em $A := (\mathbb{Z}[\xi] \otimes R(G)) \otimes \mathbb{F}_p$. Portanto a fibra $C_p := \operatorname{Spec} A$ do morfismo $\pi : C \to \operatorname{Spec}(\mathbb{Z})$ sobre p não pode ser uma união disjunta da forma $\bigsqcup_i k_i$ onde os k_i são extensões de corpo finitas separáveis de $\mathbb{F}_p$. De [Ml, Prp. 3.2] segue que π ramifica em p, e de [Ml, Prp. 3.5] segue que $\Omega_{C/\operatorname{Spec}(\mathbb{Z})} \otimes_{\mathcal{O}_C} k_P \neq 0$ uma vez que $\pi(P) = p$. Em particular, $\dim(T_P C) \geq 1$.

Para provar (II).(vi), seja $\ell := \phi(n) - 1$. Todo elemento $f \in R$ pode ser escrito como

$$\begin{aligned} f &= \sum_{i=1}^{l} (a_{i0} + a_{i1}\xi + a_{i2}\xi^2 + \ldots + a_{i\ell}\xi^{\ell}) \otimes (b_{i1}\chi_1 + \ldots + b_{is}\chi_s) = \sum_{i=1}^{l}\sum_{j=0}^{\ell}\sum_{k=1}^{s} a_{ij}b_{ik}\left(\xi^j \otimes \chi_k\right) \\ &= \sum_{j=0}^{\ell}\sum_{k=1}^{s} c_{jk}\left(\xi^j \otimes \chi_k\right) \end{aligned}$$

onde $a_{ij}, b_{ik} \in \mathbb{Z}$, $c_{jk} := \sum_{i=1}^{\ell} a_{ij}b_{ik} \in \mathbb{Z}$. Note que é natural supor $\mathbb{Z} \subset R$, e portanto podemos tomar congruência mod P^2 para escrever

$$\overline{f} = \sum_{j=0}^{\ell}\sum_{k=1}^{s} \overline{c_{jk}} \cdot \overline{(\xi^j \otimes \chi_k)}. \tag{2.6}$$

Como $\langle p \rangle \subset P$, segue que $\langle p^2 \rangle \subset P^2$, daí (2.6) implica

$$|R/P^2| \leq p^2 \cdot \phi(n) \cdot s. \tag{2.7}$$

Por outro lado, temos os isomorfismos naturais

$$\frac{R/P^2}{P/P^2} \cong \frac{R}{P} \cong k_P. \tag{2.8}$$

Portanto,

$$\begin{aligned} \operatorname{edim}_P(X) = \dim(P/P^2) = \log_{|k_P|} |P/P^2| &= \log_{|k_P|} \frac{|R/P^2|}{|k_P|} \\ &\leq \log_p \frac{p^2 \cdot \phi(n) \cdot s}{p} = \log_p\ p \cdot \phi(n) \cdot s = 1 + \log_p(\phi(n) \cdot s) \end{aligned}$$

onde a terceira equação vem de (2.8) e a inequação vem de (2.7) e o fato que $\mathbb{F}_p \subset k_P$. □

Agora iremos restringir a analise feita no Teorema 2.1 ao caso onde os pontos singulares são pontos racionais. Começamos pela definição de ponto racional.

Definição 2.2. Seja X um esquema e $Y = \mathrm{Spec}(A)$ um esquema afim. Denote por $X(A) := \mathrm{Hom}(T, X)$. Se A é local, então elemento de $X(A)$ corresponde a um par formado por um ponto $P \in X$ e um morfismo local $\mathcal{O}_{X,P} \to A$. Dizemos que P é *A-rational* se tal morfismo existe.

Em particular, se $A = K$, um corpo, então $X(K)$ pode ser dado por pares formados por pontos $P \in X$ e extensões de corpos $k_P \to K$. Se, além disso, X é um esquema sobre Y, então $X(K)$ é naturalmente identificado com o conjunto de pontos $P \in X$ para os quais a extensão $K \to k_P$ é um isomorfismo.

Mais geralmente, dado um esquema X sobre Y, dizemos que $P \in X$ é *Y-racional* se P é k_Q-racional onde $Q \in Y$ é a imagem de P. Se $Y = \mathrm{Spec}(\mathbb{Z})$ dizemos simplesmente que P é *racional*, por simplicidade. Neste caso, se P anula sobre $p \in \mathbb{N}$, então P é racional se e somente se $k_P \cong \mathbb{F}_p$.

Com a definição acima, temos o seguinte resultado

Teorema 2.2. *Seja $P' := \pi\prime(P)$. Se P' é racional então existe um inteiro $\ell_{P'}$ satisfazendo $0 \leq \ell_{P'} \leq s-1$ tal que*

(i) $\mathrm{edim}_P(C) \leq \ell_{P'} + 1$.

(ii) $\dim(T_P C) = \mathrm{edim}_P(C) = \ell_{P'} + 1$ *se P é racional.*

(iii) Se G é abeliano, então P' é singular se somente se $p|n$. Além disso

$$\mathrm{edim}_{P'}(C') = \ell_{P'} + 1 \qquad e \qquad \dim(T_{P'} C') = \ell_{P'},$$

e $\ell_{P'}$ coincide com o número minimal de geradores do p-Sylow subgrupo de G.

Demonstração. Seja $f(y) \in \mathbb{Z}[y]$ o n-ésimo polinômio ciclotômico, então claramente

$$P = \begin{cases} \langle p \otimes \chi_1, P' \rangle & \text{se } f \text{ é irredutível em } \mathbb{F}_p[y] \\ \langle h(\xi) \otimes \chi_1, P' \rangle & \text{se } h|f \text{ em } \mathbb{F}_p[y] \end{cases} \tag{2.9}$$

Agora note que exite uma correspondência biunívoca natural entre pontos $P \in C$ com $\pi(P) = p$ e pontos do esquema zero-dimensional

$$Z \subset \mathbb{A}^s_{\mathbb{F}_p} = \mathrm{Spec}(\mathbb{F}_p[x_2, \ldots x_s, y])$$

definido pelas equações

$$f_{ij}(x_2, \ldots, x_s) = x_i x_j - a_{ij1} - a_{ij2} x_2 - \ldots - a_{ijs} x_s = 0 \tag{2.10}$$

$$f(y) = 0 \tag{2.11}$$

onde $f_{ij} \in \mathbb{F}_p[x_2, \ldots, x_s]$ são tais que $\chi_i\chi_j = a_{ij1}\chi_1 + a_{ij2}\chi_2 + \ldots + a_{ijs}\chi_s$ para todo $i, j \in \{2, \ldots s\}$.

De fato, esta correspondência é na verdade um isomorfismo entre o esquema fibra C_p e Z e segue imediatamente do seguinte epimorfismo de anéis

$$\begin{array}{rccc} \Psi: & \mathbb{F}_p[x_2, \ldots, x_s, y] & \longrightarrow & (\mathbb{Z}[\xi] \otimes R(G))/\langle p \rangle \\ & 1 & \longmapsto & \chi_1 \\ & x_i & \longmapsto & \chi_i \\ & y & \longmapsto & \xi \end{array}$$

Sendo um isomorfismo, preserva pontos racionais, e também restringe a pontos de C' sobre p. Então P' é racional se e somente se

$$P' = \langle p, \chi_2 - c_2\chi_1, \ldots, \chi_s - c_s\chi_1 \rangle \tag{2.12}$$

onde $(c_2, \ldots, c_s) \in \mathbb{F}_p^{s-1}$ satisfaz as equações (2.10). Então podemos considerar $P' \in \mathbb{A}^{s-1}_{\mathbb{F}_p}$.

Para provar (i), seja

$$\begin{array}{rccc} J_{P'}: & \mathbb{F}_p^{s-1} & \longrightarrow & \mathbb{F}_p^{\binom{s}{2}} \\ & e_k & \longmapsto & \displaystyle\sum_{ij} \frac{\partial f_{ij}}{\partial x_k}(c_2, \ldots, c_s)e_{ij} \end{array}$$

a aplicação Jacobiana, com $\{e_k\}_{i=2}^s$ a base standard de $\mathbb{F}_p^{s-1}$ e $\{e_{ij}\}_{ij}$ a de $\mathbb{F}_p^{\binom{s}{2}}$. Defina

$$\ell_{P'} := \dim(\ker(J_{P'}))$$

Agora, sejam

$$M_P = \begin{cases} \mathfrak{m}_P/\langle p \rangle & \text{se } \Phi_n \text{ é irredutível em } \mathbb{F}_p[y] \\ \mathfrak{m}_P/\langle h(\xi) \rangle & \text{se } h|\Phi_n \text{ em } \mathbb{F}_p[y] \end{cases}$$

e seja também $\mathfrak{n}_{P'}$ o ideal maximal de $P' \in \mathbb{A}^{s-1}_{\mathbb{F}_p}$. Então Ψ fornece um epimorfismo natural

$$\begin{array}{rccc} \psi: & \mathfrak{n}_{P'}/\mathfrak{n}_{P'}^2 & \longrightarrow & M_P/M_P^2 \\ & g(x_2, \ldots, x_s) & \longmapsto & \displaystyle\sum_{k=2}^{s} \frac{\partial g}{\partial x_k}(P')(\chi_k - c_k) \end{array}$$

cujo núcleo é gerado pelas classes dos elementos f_{ij}, que a saber, são

$$\overline{f}_{ij} = \sum_{k=2}^{s} \frac{\partial f_{ij}}{\partial x_k}(P')(x_k - c_k)$$

então, claramente, o núcleo de ψ tem a mesma dimensão da imagem de $J_{P'}$. Portanto

$$\dim(M_P/M_P^2) = (s-1) - \dim(\ker(\psi)) = (s-1) - \dim(\mathrm{im}(J_{P'})) = \dim(\ker(J_{P'})).$$

Por construção, se $L_1, \ldots, L_r$ formam uma base de M_P/M_P^2 então precisamos apenas adicionar p (ou $h(\xi)$) para gerar $\mathfrak{m}_P/\mathfrak{m}_P^2$, e assim

$$\dim(\mathfrak{m}_P/\mathfrak{m}_P^2) \leqslant \dim(M_P/M_P^2) + 1 = \dim(\ker(J_{P'})) + 1 = \ell_{P'} + 1$$

onde a primeira desigualdade vem do fato de que o conjunto $\{L_1, \ldots, L_r\} \cup \{p \text{ (ou } h(\xi))\}$ pode não ser linearmente independente.

Para provar (ii), note que P é racional se e somente se $h(y)$ é um fator linear de $f(y)$, digamos $h(y) = y - c$. Então escreva $P := (c_2, \ldots, c_s, c) \in \mathbb{F}_p^s$ com P satisfazendo as equações (2.10) e (2.11). A matriz Jacobiana em P é

$$J_P = \begin{pmatrix} & & & 0 \\ & J_{P'} & & \vdots \\ & & & 0 \\ 0 & \ldots & 0 & f'(c) \end{pmatrix}$$

e $f'(c) = 0$ pois c tem multiplicidade ao menos 2. De fato, por [Mr, Teo. 17.2], temos que

$$f(y) = \prod (y - \xi^k)$$

com $1 \leq k \leq n-1$ e $(k, n) = 1$. Daí toda raiz do polinômio ciclotômico $f(y)$ é uma raiz n-ésima primitiva da unidade. Logo, c também é raiz de $y^n - 1$. Por outro lado, note que em $\mathbb{F}_p[y]$ a seguinte igualdade é válida

$$y^n - 1 = (y^m - 1)^{p^r}$$

onde $n = p^r m$ com $p \nmid m$. Com isso vemos que a raiz c de $y^n - 1$ tem multiplicidade maior ou igual p^r sobre $\mathbb{F}_p$. Agora, sejam $\alpha_1, \ldots, \alpha_n$ as n raízes de $y^n - 1$ em seu corpo de decomposição K sobre $\mathbb{F}_p$. Considere o conjunto de todas as suas raízes primitivas, digamos $R_n = \{\zeta_1, \ldots, \zeta_{\phi(n)}\}$. Defina o polinômio cujas raízes são os elementos de R_n

$$\prod_{i=1}^{\phi(n)} (y - \zeta_i)$$

o qual, por [Mr, Teo. 17.2], é o n-ésimo polinômio ciclotômico $f(y)$. Por outro lado, como $p \mid n$, temos que cada uma das raízes α_i, $i = \{1, \ldots, n\}$ tem multiplicidade igual a $p^r > 1$ sobre $\mathbb{F}_p$, em particular, cada raiz ζ_j de $f(y)$ tem multiplicidade p^r, para $j = 1, \ldots, \phi(n)$.

Agora seja $\mathfrak{n}_P$ o ideal maximal de $P \in \mathbb{A}^s_{\mathbb{F}_p}$ e estenda a aplicação ψ naturalmente para a aplicação $\widetilde{\psi} : \mathfrak{n}_P/\mathfrak{n}_P^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$. Então

$$\mathrm{edim}_P(C) = \dim(\mathrm{im}(\widetilde{\psi})) = \dim(\ker(J_P)) = \dim(\ker(J_{P'})) + 1.$$

A fim de incluir $\dim(T_P C)$ na sequência de igualdades acima, basta notar que $k_P = \mathbb{F}_p$ e que

$$\begin{array}{rccc} d \circ \widetilde{\psi} : & \mathfrak{n}_P/\mathfrak{n}_P^2 & \longrightarrow & \Omega_{\mathcal{O}_P/\mathbb{Z}} \otimes_{\mathcal{O}_P} k_P \\ & g(x_2, \ldots, x_s, y) & \longmapsto & \displaystyle\sum_{k=2}^{s} \frac{\partial g}{\partial x_k}(P) d\chi_i + \frac{\partial g}{\partial y}(P) d\xi \end{array}$$

Assim, $\dim(T_P C) = \dim(\Omega_{\mathcal{O}_P/\mathbb{Z}} \otimes_{\mathcal{O}_P} k_P) = \dim(\mathrm{im}(d \circ \widetilde{\psi})) = \dim(\ker(J_P))$ como desejado.

Para provar (iii), escreva o grupo abeliano finito como

$$G = \left((\mathbb{Z}/p_1^{\alpha_{11}}\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/p_1^{\alpha_{1r_1}}\mathbb{Z}) \right) \oplus \ldots\ldots \oplus \left((\mathbb{Z}/p_s^{\alpha_{s1}}\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/p_s^{\alpha_{sr_s}}\mathbb{Z}) \right).$$

Então existe uma correspondência biunívoca entre os pontos $P' \in C'$ que projetam sobre p e pontos do esquema zero-dimensional $Z' \subset \mathbb{A}^{r_1+\ldots+r_s}_{\mathbb{F}_p} = \mathrm{Spec}(\mathbb{F}_p[x_{ij}])$ com $i \in \{1, \ldots, s\}$ e $j \in \{1, \ldots, r_i\}$ definida pelas equações

$$f_{ij} = x_{ij}^{p_i^{\alpha_{ij}}} - 1 = 0.$$

Eles produzem a matriz Jacobiana diagonal

$$J_{Z'} = \begin{pmatrix} p_1^{\alpha_{11}} x_{11}^{p_1^{\alpha_{11}}-1} & & 0 \\ & \ddots & \\ 0 & & p_s^{\alpha_{sr_s}} x_{sr_s}^{p_s^{\alpha_{sr_s}}-1} \end{pmatrix}$$

que, computados no único ponto racional $P' = (1, \ldots, 1) \in Z'$, têm núcleo com dimensão $\ell_{P'} = r_k$ se $p = p_k$ para algum $k \in \{1, \ldots, s\}$ ou 0 em caso contrário. Depois é só seguir o que foi dito acima para concluir que $\mathrm{edim}_{P'}(C') = \ell_{P'} + 1$ e então use o fato de que $p \notin P^2$ por [B, p. 33] (assim $d(p) = 0$) para concluir que $\dim(T_{P'} C') = \ell_{P'}$. Finalmente, note que r_k é precisamente o número minimal de geradores do p_k-subgrupo de Sylow de G. □

3 Casos Particulares

Neste capítulo aplicaremos os Teoremas 2.1 e 2.2 nos casos onde G é, respectivamente, o grupo simétrico S_3, o grupo diedral D_4 e o grupo alternado A_4 obtendo explicitamente os seus pontos singulares e a sua dimensão de mergulho. Dada a importância destes casos, reservaremos uma seção para cada um e devido as explicações envolvidas, embora se trate de exemplos, optamos por colocar o texto dentro do esquema "proposição-prova".

3.1 O caso do grupo simétrico S_3

Consideremos nessa seção S_3 como o grupo das permutações apresentado no Capítulo 1 e $\xi := \xi_6$.

Proposição 3.1. *A curva afim*

$$C = Spec(\mathbb{Z}[\xi_6] \otimes_{\mathbb{Z}} R(S_3))$$

tem apenas dois pontos singulares:

(i) O ponto $P = \langle 1 \otimes 2\chi_1, 1 \otimes \chi_3 \rangle$, *com* $\dim(T_P C) = 1$ *e* $\operatorname{edim}_P(C) = 2$.

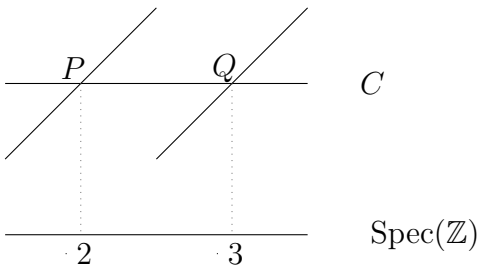
(ii) O ponto $Q = \langle (1+\xi) \otimes \chi_1, 1 \otimes \chi_3 \rangle$, *com* $\dim(T_Q C) = \operatorname{edim}_Q(C) = 2$.

Além disso, se $\pi : C \to Spec(\mathbb{Z})$ *é o morfismo natural, então* $\pi(P) = 2$ *e* $\pi(Q) = 3$.

Demonstração. Com o objetivo de calcular os pontos singulares de C, conforme a prova do Teorema 2.1, devemos inicialmente determinar os conjuntos $c_i(2)$ e $c_i(3)$ para $i \in \{1, 2, 3\}$ (veja definição (1.5)), trabalho esse que já foi realizado no Exemplo 1.1:

$$c_1(2) = c_3(2) = c_1, \quad c_2(2) = c_2; \qquad c_1(3) = c_2(3) = c_1, \quad c_3(3) = c_3.$$

Disso concluímos que a figura de C é



E assim, temos que P e Q são os únicos pontos singulares de C. Vamos determiná-los, iniciando por P. Pelo visto no primeiro capítulo,

$$R(S_3) = \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2 \oplus \mathbb{Z}\chi_3.$$

Agora, a multiplicação em $R(S_3)$ é induzida pelo produto dos caratéres iredutíveis, como veremos a seguir. Segue da tabela de multiplicação dos caráteres de S_3 dada em (1.5), por exemplo, que:

$$\begin{aligned}(\chi_3)^2(c_1) &= 2^2 = 4 = 1+1+2 = \chi_1(c_1)+\chi_2(c_1)+\chi_3(c_1)\\ (\chi_3)^2(c_2) &= (-1)^2 = 1 = 1+1-1 = \chi_1(c_2)+\chi_2(c_2)+\chi_3(c_2)\\ (\chi_3)^2(c_3) &= 0^2 = 0 = 1-1+0 = \chi_1(c_3)+\chi_2(c_3)+\chi_3(c_3)\end{aligned}$$

ou seja,

$$(\chi_3)^2(g) = \chi_1(g)+\chi_2(g)+\chi_3(g) \quad \forall g \in S_3$$

ou simplesmente, $(\chi_3)^2 = \chi_1+\chi_2+\chi_3$.

Através de verificações semelhantes obtemos a seguinte tábua de multiplicação

$$\begin{aligned}\chi_1^2 &= \chi_1 & \chi_2^2 &= \chi_1\\ \chi_1\chi_2 &= \chi_2 & \chi_2\chi_3 &= \chi_3\\ \chi_1\chi_3 &= \chi_3 & \chi_3^2 &= \chi_1+\chi_2+\chi_3\end{aligned} \tag{3.1}$$

Vamos agora determinar o ponto singular P. De (3.1) obtemos um sistema em $\mathbb{F}_2^2 = (x_2, x_3)$ dado por

$$\begin{aligned}x_2^2 &= 1\\ x_2x_3 &= x_3\\ x_3^2 &= 1+x_2+x_3\end{aligned} \tag{3.2}$$

cujas soluções são $P_1' := (1,0)$ e $P_2' := (1,1)$. A matriz Jacobiana de (3.2) é

$$J = \begin{pmatrix} 0 & 0\\ x_3 & x_2+1\\ 1 & 1\end{pmatrix}$$

e assim,

$$J_{P_1'} = \begin{pmatrix} 0 & 0\\ 0 & 0\\ 1 & 1\end{pmatrix} \qquad J_{P_2'} = \begin{pmatrix} 0 & 0\\ 1 & 0\\ 1 & 1\end{pmatrix}$$

Note que $J_{P_1'}$ pode ser identificada como uma transformação linear entre $\mathbb{F}_2^2$ em $\mathbb{F}_2^3$ dada por:

$$J_{P_1'}(x_2,x_3) := J_{P_1'}\cdot(x_2,x_3)^{\mathrm{t}} = \begin{pmatrix} 0 & 0\\ 0 & 0\\ 1 & 1\end{pmatrix}\cdot(x_2,x_3)^{\mathrm{t}} = (0,0,x_2+x_3)\,.$$

O que implica que $\ker\left(J_{P_1'}\right) = \langle(1,1)\rangle$, e disso, $\dim_{\mathbb{F}_2}\left(\ker\left(J_{P_1'}\right)\right) = 1 = \ell_{P_1'}$. Similarmente $\ell_{P_2'} = 0$.

Assim, pelo Teorema 2.2.(i), $\operatorname{edim}_{P_2}(C) = 1$, ou seja, P_2 está sobre um ponto regular de C. Ainda pelo Teorema 2.2.(i), temos que $\operatorname{edim}_{P_1}(C) = 1$ ou $\operatorname{edim}_{P_1}(C) = 2$. Portanto $P = P_1'$ pode, possivelmente, produzir um ponto singular em C.

Uma vez que $f(y) = y^2 - y + 1$ é irredutível em $\mathbb{F}_2[y]$ segue da figura acima e do Teorema 2.1.(II).(i) que existem somente dois pontos de C sobre 2, e um deles é singular. Assim, P_1' está sobre este ponto singular, o qual, por (2.9) e (2.12) que

$$P = \langle 2 \otimes \chi_1, 1 \otimes (\chi_2 + \chi_1), 1 \otimes \chi_3 \rangle \in C$$

Note que neste caso, $P \in C$ não é racional, então segue do Teorema 2.2.(i) que

$$\operatorname{edim}_P(C) \leqslant \ell_{P'} + 1 = 1 + 1 = 2. \tag{3.3}$$

Por outro lado, como P é singular, temos

$$\operatorname{edim}_P(C) \geqslant 2, \tag{3.4}$$

e portanto $\operatorname{edim}_P(C) = 2$.

Observe que

$$\chi_2 + \chi_1 = (\chi_3 - \chi_1)\chi_3$$

o que implica que

$$P = \langle 2 \otimes \chi_1, 1 \otimes \chi_3 \rangle. \tag{3.5}$$

como esperado desde que $\operatorname{edim}_P(C)$ concorda com o menor número de elementos necessários gerar P por [Mt, p. 104].

Para calcular $\dim(T_P C)$, afirmamos que

$$2 \otimes \chi_1 \notin P^2.$$

De fato, segue de (3.5) que

$$P^2 = \langle 2\chi_1, \chi_3 \rangle^2 = \langle 4 \otimes \chi_1,\ 2 \otimes \chi_3,\ 1 \otimes (\chi_1 + \chi_2 + \chi_3) \rangle.$$

Escrevendo seus geradores por

$$v_1 = 4 \otimes \chi_1,\ v_2 = 2 \otimes \chi_3,\ v_3 = 1 \otimes (\chi_1 + \chi_2 + \chi_3),$$

temos que um elemento genérico de P^2 é do tipo

$$\left(\sum_{i=1}^{3}\sum_{j=0}^{1} a_{ij}\xi^j \otimes \chi_i\right) v_1 + \left(\sum_{i=1}^{3}\sum_{j=0}^{1} b_{ij}\xi^j \otimes \chi_i\right) v_2 + \left(\sum_{i=1}^{3}\sum_{j=0}^{1} c_{ij}\xi^j \otimes \chi_i\right) v_3$$

com os coeficientes em $\mathbb{Z}$. Agora, suponha por absurdo que $2 \otimes \chi_1 \in P^2$. Daí, obtemos o seguinte sistema (Diofantino)

$$\begin{cases} 2 = & 4a_{10} + 2b_{30} + c_{10} + c_{20} + c_{30} \\ 0 = & 4a_{11} + 2b_{31} + c_{11} + c_{21} + c_{31} \\ 0 = & 4a_{20} + 2b_{30} + c_{10} + c_{20} + c_{30} \\ 0 = & 4a_{21} + 2b_{31} + c_{11} + c_{21} + c_{31} \\ 0 = & 4a_{30} + 2b_{10} + 2b_{20} + 2b_{30} + c_{10} + c_{20} + 3c_{30} \\ 0 = & 4a_{31} + 2b_{11} + 2b_{21} + 2b_{31} + c_{11} + c_{21} + 3c_{31} \end{cases}$$

Considerando somente a primeira e a terceira equações acima, temos

$$\begin{aligned} 2 = & \quad 4a_{10} + 2b_{30} + c_{10} + c_{20} + c_{30} \\ 0 = & \quad 4a_{20} + 2b_{30} + c_{10} + c_{20} + c_{30} \end{aligned}$$

de onde verificamos que

$$1 = 2(a_{10} - a_{20})$$

o que implica em 2 divide 1 em $\mathbb{Z}$, absurdo. Portanto $2 \otimes \chi_1 \notin P^2$, como afirmado, e por 2.1.(iv) temos que

$$\dim(T_P C) < \operatorname{edim}_P(C). \tag{3.6}$$

Por outro lado, note que

$$(\chi_2 - \chi_1)^2 \equiv \chi_2^2 - \chi_1 \equiv 0 \mod 2 \tag{3.7}$$

e pelo Teorema 2.1.(v), segue que

$$1 \leq \dim(T_P C). \tag{3.8}$$

Por (3.3), (3.6) e (3.8), concluímos que

$$1 \leq \dim(T_P C) < \operatorname{edim}_P(C) \leq 2.$$

Portanto $\dim(T_P C) = 1$ e $\operatorname{edim}_P(C) = 2$.

Para obter o ponto singular Q, procederemos de modo semelhante ao feito no caso anterior. Primeiro, consideraremos o sistema (3.2) em $\mathbb{F}_3^2$, cujas soluções são

$$Q_1' := (1, 2) \quad \text{e} \quad Q_2' := (2, 0)$$

Neste caso, a matriz Jacobiana de (3.2) é

$$J = \begin{pmatrix} 2x_2 & 0 \\ x_3 & x_2 + 2 \\ 2 & 2x_3 + 2 \end{pmatrix}$$

e daí

$$J_{Q'_1} = \begin{pmatrix} 2 & 0 \\ 2 & 0 \\ 2 & 0 \end{pmatrix} \qquad J_{Q'_2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \end{pmatrix}$$

Donde $\ell_{Q'_1} = 1$ e $\ell_{Q'_2} = 0$. Assim

$$Q' = \langle 3\chi_1, \chi_2 + \chi_1,\ \chi_3 + \chi_1 \rangle.$$

Note que neste caso, $f(y) = y^2 + 2y + 1 \in \mathbb{F}_3^2$, pode ser reescrito como

$$f(y) = (y+1)^2 \in \mathbb{F}_3[y]$$

onde $h(y) = y + 1$, e assim,

$$Q = \langle (1+\xi) \otimes \chi_1,\ 1 \otimes (\chi_2 + \chi_1),\ 1 \otimes (\chi_3 + \chi_1) \rangle.$$

Mais ainda, como $h(y)$ é linear, temos que $Q \in C$ é racional, e pelo Teorema 2.2.(ii),

$$\dim(T_Q C) = \operatorname{edim}_Q(C) = l_{Q'} + 1 = 1 + 1 = 2.$$

Com o objetivo de reduzir o número de geradores de Q, note que

$$\chi_2 + 2\chi_1 = (\chi_3 + \chi_1)^2 - 3\chi_1$$

e disso,

$$Q = \langle (1+\xi) \otimes \chi_1,\ 1 \otimes (\chi_3 + \chi_1) \rangle,$$

o que prova o item (ii) desta Proposição. □

3.2 O Caso do grupo diedral D_4

Seja D_4 o grupo diedral 4. Nesta seção, consideremos $\xi := \xi_8 = e^{2\pi i/8}$ a raiz oitava primitiva da unidade.

Proposição 3.2. *A curva afim*

$$C = \operatorname{Spec}\left(\mathbb{Z}[\xi] \otimes R(D_4)\right)$$

têm apenas um ponto singular:

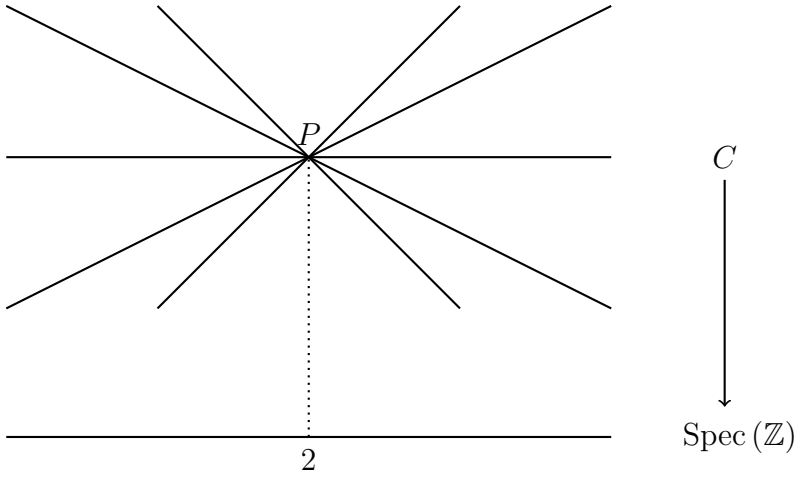
$$P := \langle (1+\xi) \otimes \chi_1, 1 \otimes (\chi_1 + \chi_2), 1 \otimes (\chi_1 + \chi_3), 1 \otimes \chi_5 \rangle$$

com $\dim\left(T_P C\right) = \operatorname{edim}_P\left(C\right) = 4$.

Demonstração. Observe inicialmente que temos do Exemplo (1.2) que

$$c_1(2) = c_2(2) = c_3(2) = c_4(2) = c_5(2) = c_1.$$

e segue disso que a figura neste exemplo é



De modo análogo feito na demonstração da Proposição 3.1 e da tabela de multiplicação dos caráteres de D_4 dada em (1.7) obtemos as seguintes relações dos caráteres irredutíveis de D_4:

$$\begin{array}{lll} \chi_1^2 = \chi_1 & \chi_2^2 = \chi_1 & \chi_3\chi_4 = \chi_2 \\ \chi_1\chi_2 = \chi_2 & \chi_2\chi_3 = \chi_4 & \chi_3\chi_5 = \chi_5 \\ \chi_1\chi_3 = \chi_3 & \chi_2\chi_4 = \chi_3 & \chi_4^2 = \chi_1 \\ \chi_1\chi_4 = \chi_4 & \chi_2\chi_5 = \chi_5 & \chi_4\chi_5 = \chi_5 \\ \chi_1\chi_5 = \chi_5 & \chi_3^2 = \chi_1 & \chi_5^2 = \chi_1 + \chi_2 + \chi_3 + \chi_4 \end{array} \tag{3.9}$$

Note que pela relação $\chi_2\chi_3 = \chi_4$ podemos assumir que χ_4 é um caráter redundante multiplicativamente. Daí, obtemos um sistema em $\mathbb{F}_2^3 = (x_2, x_3, x_5)$ dado por

$$\begin{aligned} x_2^2 &= 1 \\ x_2x_5 &= x_5 \\ x_3^2 &= 1 \\ x_3x_5 &= x_5 \\ x_5^2 &= 1 + x_2 + x_3 + x_2x_3 \end{aligned} \tag{3.10}$$

cuja única solução é $P' = (1, 1, 0)$. A matriz Jacobiana de (3.10) é

$$J = \begin{pmatrix} 0 & 0 & 0 \\ x_5 & 0 & x_2 + 1 \\ 0 & 0 & 0 \\ 0 & x_5 & x_3 + 1 \\ 1 + x_3 & 1 + x_2 & 0 \end{pmatrix}$$

donde

$$J_{P'} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Donde $\ell_P = 3$. Pela figura acima e pelo Teorema 2.1(i), o ponto P' está sobre um ponto singular de C, e como $P' \in C'$ é um ponto racional, segue que

$$P' = \langle 2, \chi_2 + \chi_1, \chi_3 + \chi_1, \chi_5 \rangle.$$

Ainda, note que, $f(y) = y^4 + 1 = (y+1)^4$ em $\mathbb{F}_2[y]$, e como $h(y) = y + 1$ é um fator linear, então por (2.9) e (2.12),

$$P = \langle (1+\xi) \otimes \chi_1, 1 \otimes (\chi_2 + \chi_1), 1 \otimes (\chi_3 + \chi_1), 1 \otimes \chi_5 \rangle \in C.$$

Neste caso, temos que $k_P = \mathbb{F}_2$, o que prova que $P \in C$ é um ponto racional, e pelo Teorema 2.2.(ii)

$$\dim(T_P C) = \operatorname{edim}_P(C) = \ell_{P'} + 1 = 3 + 1 = 4$$

como afirmado. □

3.3 O caso do grupo alternado A_4

Repetindo o processo realizado nas duas seções anteriores, agora estudaremos o caso do grupo alternado A_4. Para simplificar a notação, consideremos nesta seção $\xi := \xi_{12} = e^{2\pi i/12}$ uma raiz 12-ésima primitiva da unidade.

Proposição 3.3. *A curva afim*

$$C = \operatorname{Spec}\left(\mathbb{Z}[\xi] \otimes R(A_4)\right)$$

possui apenas dois pontos singulares:

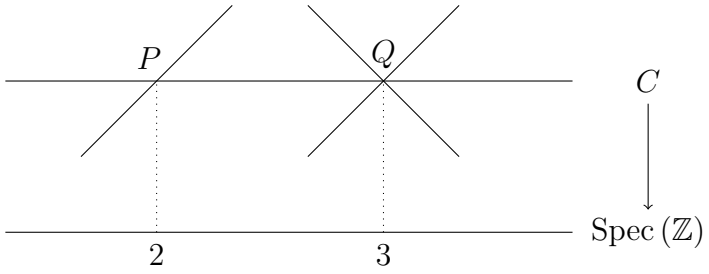
(i) *O ponto* $P = \langle (1 + \xi + \xi^2) \otimes \chi_1, 1 \otimes (\chi_1 + \chi_4) \rangle$ *com* $\operatorname{edim}_P(C) = 2$.

(ii) *O ponto* $Q := \langle (1 + \xi^2) \otimes \chi_1, 1 \otimes (2\chi_1 + \chi_2), 1 \otimes \chi_4 \rangle$ *com* $\operatorname{edim}_Q(C) = 2$.

Demonstração. Com o objetivo de determinar os pontos singulares de C, procederemos de modo semelhante ao utilizado nas duas seções anteriores. Pelo exemplo 1.2 temos que

$$c_1(2) = c_2(2) = c_1, \;\; c_3(2) = c_3, \;\; c_4(2) = c_4; \qquad c_1(3) = c_3(3) = c_4(3) = c_1, \;\; c_2(3) = c_2.$$

E portanto, temos neste caso que a figura é a seguinte



Pela figura acima, temos que P e Q são os únicos pontos singulares de C (Teorema 2.1.(i)). A tabela de multiplicação dos caráteres de A_4 dada em (1.6) obtemos as seguintes relações dos caráteres irredutíveis de A_4:

$$\begin{array}{lll} \chi_1^2 = \chi_1 & \chi_2^2 = \chi_3 & \chi_3^2 = \chi_2 \\ \chi_1\chi_2 = \chi_2 & \chi_2\chi_3 = \chi_1 & \chi_3\chi_4 = \chi_4 \\ \chi_1\chi_3 = \chi_3 & \chi_2\chi_4 = \chi_4 & \chi_4^2 = \chi_1 + \chi_2 + \chi_3 + 2\chi_4 \\ \chi_1\chi_4 = \chi_4 & & \end{array} \tag{3.11}$$

Note que pela relação

$$\chi_2^2 = \chi_3$$

podemos assumir que χ_3 é um caráter redundante multiplicativamente. Assim, para encontrar P, basta analisarmos o sistema em $\mathbb{F}_2^2 = (x_2, x_4)$ dado por

$$\begin{aligned} x_2^3 &= 1 \\ x_2x_4 &= x_4 \\ x_4^2 &= 1 + x_2 + x_2^2 \end{aligned}$$

o qual possui uma única solução $P' := (1, 1)$. A matriz Jacobiana é

$$J = \begin{pmatrix} x_2^2 & 0 \\ x_4 & x_2 + 1 \\ 1 & 0 \end{pmatrix}$$

e disso

$$J_{P'} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

onde $\ell_{P'} = 1$.

Como P' é racional, temos que

$$P' = \langle 2, \chi_2 + \chi_1, \chi_4 + \chi_1 \rangle$$

e mais, neste caso temos que $f(y) = y^4 - y^2 + 1 = (y^2 + y + 1)^2$ em $\mathbb{F}_2[y]$, e como $h(y) = y^2 + y + 1$ é irredutível, então (por (2.9) e (2.12))

$$P = \langle (1 + \xi + \xi^2) \otimes \chi_1, 1 \otimes (\chi_2 + \chi_1), 1 \otimes (\chi_4 + \chi_1) \rangle \in C.$$

Note que neste caso, $P \in C$ não é racional, então segue do Teorema 2.2.(i) que

$$\text{edim}_P(C) \leq l_{P'} + 1 = 1 + 1 = 2. \tag{3.12}$$

e como P é um ponto singular de C, temos que a igualdade acima é válida.Com o objetivo de reduzir o conjunto de geradores de P, note que

$$\chi_2 + \chi_1 = (\chi_3 + \chi_4)(\chi_4 + \chi_1) - ((2 - \xi - \xi^2 + \xi^3) \otimes (\chi_3 - \chi_4))((1 + \xi + \xi^2) \otimes \chi_1),$$

e assim podemos escrever

$$P = \langle (1 + \xi + \xi^2) \otimes \chi_1, 1 \otimes (\chi_1 + \chi_4) \rangle, \tag{3.13}$$

como desejado.

Para encontrar Q, estudaremos o sistema em $\mathbb{F}_3^2 = (x_2, x_4)$ dado por

$$\begin{aligned} x_2^3 &= 1 \\ x_2 x_4 &= x_4 \\ x_4^2 &= 1 + x_2 + x_2^2 + 2x_4 \end{aligned}$$

cujas soluções são $Q_1' := (1, 0)$ e $Q_2' = (1, 2)$. A matriz Jacobiana é

$$J = \begin{pmatrix} 0 & 0 \\ x_4 & x_2 + 2 \\ 2 + x_2 & 2x_4 + 1 \end{pmatrix}$$

donde

$$J_{Q_1'} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad J_{Q_2'} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \\ 0 & 2 \end{pmatrix}$$

assim, obtemos que $\ell_{Q_1'} = 1$ e $\ell_{Q_2'} = 0$. Portanto Q_2' está sobre um ponto regular de C (Teorema 2.2.(i)) e $Q' := Q_1'$ está sobre o ponto singular Q de C.

Como Q_1' é racional que

$$Q' := Q_1' = \langle 3, \chi_2 + 2\chi_1, \chi_4 \rangle$$

e mais, neste caso temos que $f(y) = y^4 + 2y^2 + 1 = (y^2 + 1)^2$ em $\mathbb{F}_3[y]$, e como $h(y) = y^2 + 1$ é irredutível, então por (2.9) e (2.12)

$$Q = \langle (1 + \xi^2) \otimes \chi_1, 1 \otimes (\chi_2 + 2\chi_1), 1 \otimes \chi_4 \rangle \in C.$$

Note que neste caso, $Q \in C$ não é racional, então segue do Teorema 2.2.(i) que

$$\text{edim}_Q(C) \leq l_{Q'} + 1 = 1 + 1 = 2. \tag{3.14}$$

e como Q é um ponto singular de C, temos que a igualdade acima é válida, ou seja,

$$\text{edim}_Q(C) = 2.$$

como queríamos demonstrar. □

4 Algoritmo Geral

Neste capítulo propomos um algoritmo, não implementado, para a determinação de pontos singulares para a curva afim C, como no enunciado do Teorema 2.1. Um fator motivador para a obtenção desse algoritmo é dada na observação abaixo

Observação 4.1. Note que não é verdade que qualquer ponto de C é da forma apresentada no Teorema 2.2. Por exemplo, no caso de $C = \operatorname{Spec}(\mathbb{Z}[\xi_{12}] \otimes R(A_4))$ visto acima, considere o anel

$$A := \frac{R(A_4)}{\langle 2\chi_1 \rangle} = \{a\chi_1 + b\chi_2 + c\chi_3 + d\chi_4 \,|\, a, b, c, d \in \{0, 1\}\}$$

onde a última igualdade é consequência de que a característica de A é 2. Note que

$$(\chi_1 + \chi_2)\chi_4 = 2\chi_4 = 0$$

em A, e, portanto não é um domínio. Em particular, desde que χ_4 não é uma unidade, existe um ideal primo P de $\mathbb{Z}[\xi] \otimes R(A_4)$ (um ponto de C) o qual se projeta sobre $\langle 2 \rangle$ e contém $1 \otimes \chi_4$. Este ideal não pode ser o obtido pelo raciocínio utilizado na demonstração da Proposição 3.3.(i) uma vez que não existe do sistema uma solução com $x_4 = 0$. Com o objetivo de descrever este ideal primo P usaremos um método alternativo. Em primeiro lugar, começaremos com o anel $R(A_4)$. Assim,

$$A' := \frac{R(A_4)}{\langle 2\chi_1,\, \chi_4 \rangle} = \{a\chi_1 + b\chi_2 \,|\, a, b \in \{0, 1\}\} \cong \mathbb{F}_4 \tag{4.1}$$

onde o isomorfismo é válido pois

$$\chi_3 = \chi_4^2 - \chi_1 - \chi_2 - 2\chi_4 = \chi_1 + \chi_2$$

em A'. Assim,

$$P' := \langle 2\chi_1,\, \chi_4 \rangle$$

é um ideal primo de $R(A_4)$. Agora $\langle 2 \rangle$ não é um ideal primo de $\mathbb{Z}[\xi]$. De fato,

$$(1 + \xi^3)(1 - \xi^3) = 1 - \xi^6 = 2.$$

Então considere

$$B := \frac{\mathbb{Z}[\xi] \otimes R(A_4)}{\langle (1 + \xi^3) \otimes \chi_1,\, 1 \otimes \chi_4 \rangle}. \tag{4.2}$$

Note que

$$\xi^3 \otimes \chi_1 = 1 \otimes \chi_1 \tag{4.3}$$

em B, o que implica que

$$\xi^2 \otimes \chi_1 = (1 + \xi^4) \otimes \chi_1 = (1 + \xi) \otimes \chi_1 \tag{4.4}$$

em B. Portanto

$$\begin{aligned}(\xi \otimes \chi_1 + 1 \otimes \chi_2)((1+\xi) \otimes \chi_1 + 1 \otimes \chi_2) &= (\xi + \xi^2) \otimes \chi_1 + 1 \otimes (\chi_2 + \chi_2^2) + 2\xi \otimes \chi_2 \\ &= (1 + 2\xi) \otimes \chi_1 + 1 \otimes (\chi_2 + \chi_3) \\ &= 1 \otimes \chi_1 + 1 \otimes (\chi_1 + 2\chi_2) \\ &= 2 \otimes \chi_1 = 0\end{aligned}$$

em B, e isto prova que B não é um domínio. Agora, afirmamos que

$$B' := \frac{\mathbb{Z}[\xi] \otimes R(A_4)}{\langle (1+\xi^3) \otimes \chi_1,\ \xi \otimes \chi_1 + 1 \otimes \chi_2,\ 1 \otimes \chi_4 \rangle} \cong \mathbb{F}_4. \tag{4.5}$$

De fato, note que um elemento genérico B' é da forma

$$\sum_{i=0}^{3} \sum_{j=1}^{2} (a_{ij} \xi^i \otimes \chi_j)$$

com $a_i, b_j \in \{0, 1\}$. Assim, (4.5) segue de (4.3), (4.4) e do fato de $1 \otimes \chi_2 = \xi \otimes \chi_1$ em B'. Portanto

$$P = \langle (1+\xi^3) \otimes \chi_1,\ \xi \otimes \chi_1 + 1 \otimes \chi_2,\ 1 \otimes \chi_4 \rangle.$$

é o primo procurado. Agora

$$1 \otimes \chi_4 = \Big((\xi^2 + \xi^3) \otimes \chi_4\Big)\Bigg(\Big((1-\xi^3) \otimes \chi_1\Big)\Big((1+\xi^3) \otimes \chi_1\Big) - (\xi \otimes \chi_1 + 1 \otimes \chi_2)\Bigg).$$

Assim

$$P = \langle (1+\xi^3) \otimes \chi_1,\ \xi \otimes \chi_1 + 1 \otimes \chi_2 \rangle.$$

Sabemos que esse ponto P não é singular, uma vez que já encontramos o único ponto singular de C que está sobre o 2 (mas e se nós não o tivéssemos encontrado?). Esta dúvida é um motivador para a obtenção de um algoritmo geral.

4.1 O Algoritmo

O método que utilizamos nas seções anteriores funcionam sob certas condições, ou seja, desde que as equações que definem o anel de Green admitam soluções, e, além disso, pelo menos uma delas tenha a matriz Jacobiana com núcleo não trivial. Nesta seção esboçaremos um algoritmo para um caso geral com o objetivo de tentar contornar situações em que as condições acima não são satisfeitas.

Passo 1: *Definindo as entradas:*

Seja G um grupo finito.

- $n := |G|$;

- $s := |\mathrm{Cl}(G)|$;
- $\xi := e^{2\pi/n}$;
- $f_{ij} \in \mathbb{Z}[x_2, \ldots, x_s]$ como em (2.10) para todo $i, j \in \{2, \ldots, s\}$;
- $f(y) \in \mathbb{Z}[y]$ o n-ésimo polinômio ciclotômico;
- $p :=$ um número inteiro divisor de n.

Passo 2: *Determinando o número de pontos singulares:*

De acordo com a prova do Teorema 2.1.(II).(i), calculamos $c(p)$ para todo $c \in \mathrm{Cl}(G)$, e definimos:

$$s_p := \left| \left\{ c(p) \;\middle|\; c \in \mathrm{Cl}(G) \text{ e } c(p) = d(p) \text{ para algum } d \in \mathrm{Cl}(G) \text{ com } d \neq c \right\} \right|$$

onde os $c(p)$ que pertencem ao conjunto acima definido são tomados todos diferentes uns dos outros.

Ainda, pelo Teorema 2.1.(II).(i), o número de pontos singulares de C é no máximo s_p.

Passo 3: *Encontrando os pontos singulares racionais de C e estimando suas dimensões:*

Encontrar os pontos racionais de C' significa encontrar todas as soluções das equações f_{ij} (vistas como polinômios em $\mathbb{F}_p[x_2, \ldots, x_s]$) em $\mathbb{F}_p^{s-1}$. Se $P' = (c_2, \ldots, c_s) \in \mathbb{F}_p^{s-1}$ é uma tal solução, defina $\ell_{P'} := \dim(\ker(J_{P'}))$.

Se $\ell_{P'} \geq 1$ e $c \in \mathbb{F}_p$ é uma raiz de $\Phi_n(y)$ em $\mathbb{F}_p[y]$, então

$$P := \langle (\xi - c) \otimes \chi_1, 1 \otimes (\chi_2 - c_2\chi_1), \ldots, 1 \otimes (\chi_s - c_s\chi_1) \rangle$$

é um ponto singular de C e

$$\dim(T_P C) = \mathrm{edim}_P(C) = \ell_{P'} + 1$$

pelo Teorema 2.2.(ii).

Passo 4: *Encontrando singularidades sobre pontos racionais de C' e estimando suas dimensões:*

Seguindo o passo anterior, se $\ell_{P'} \geq 1$ e $\Phi_n(y)$ não possui raízes em $\mathbb{F}_p$, então

$$P = \begin{cases} \langle p \otimes \chi_1, 1 \otimes (\chi_2 - c_2\chi_1), \ldots, 1 \otimes (\chi_s - c_s\chi_1) \rangle & \text{se } f \text{ é irredutível em } \mathbb{F}_p[y] \\ \langle h(\xi) \otimes \chi_1, 1 \otimes (\chi_2 - c_2\chi_1), \ldots, 1 \otimes (\chi_s - c_s\chi_1) \rangle & \text{se } h | f \text{ em } \mathbb{F}_p[y] \end{cases}$$

é um ponto singular de C e

$$\dim(T_P C) \leq \mathrm{edim}_P(C) \leq \ell_{P'} + 1$$

pelo Teorema 2.1.(II).(iii) e Teorema 2.2.(ii).

Passo 5: *Encontrando pontos singulares não-racionais de C' e estimando suas dimensões:*

Se a quantidade de pontos singulares que encontramos nas etapas anteriores não foram suficientes para atingir o número s_p, então teremos de encontrar pontos não-racionais de C' sobre p. Para tal, dispomos de dois métodos:

Método 1: *Eliminação de divisores de zero.*

A ideia central deste método é incluir geradores (divisores de zeros) a um dado ideal inicial até obtermos um ideal primo e, em seguida, reduzir os geradores se necessário e verificar se ele é singular ou não. (Note que dependendo da sequência de geradores, podemos obter um ponto racional.)

Como ideal inicial podemos sempre

$$I_0 := \langle p \otimes \chi_1 \rangle.$$

O fato fundamental para esse processo é que

$$A_0 := \frac{\mathbb{Z}[\xi_n] \otimes R(G)}{I_0}$$

é sempre um anel finito com característica prima p.

Para ilustrar como este método funciona, refaremos nosso primeiro caso particular, ou seja, obteremos o ponto singular de $C = \mathrm{Spec}(\mathbb{Z}[\xi_6] \otimes R(S_3))$ que se projeta sobre $\langle 2 \rangle \in \mathrm{Spec}(\mathbb{Z})$. Uma vez que a essência da ideia deste processo não muda, podemos substituir esse trabalho por um mais simples, e lidar com $C' := \mathrm{Spec}(R(S_3))$ ao invés de C. (Com essa simplificação, $I'_0 := \langle p\chi_1 \rangle$).

Note que

$$A'_0 := \frac{R(S_3)}{\langle 2\chi_1 \rangle} = \{a\chi_1 + b\chi_2 + c\chi_3 \mid a, b, c \in \{0, 1\}\}.$$

Com o objetivo de simplificar a notação, estabeleça

$$(a, b, c) := a\chi_1 + b\chi_2 + c\chi_3, \quad 0 := (0, 0, 0) \quad \text{e} \quad a := (a, 0, 0),$$

com a, b, c constantes em um conjunto adequado. Portanto,

$$A'_0 = \{0, 1, (0, 1, 0), (1, 1, 0), (0, 0, 1), (1, 0, 1), (0, 1, 1), (1, 1, 1)\}.$$

Sabemos que $I'_0 = \langle 2 \rangle$ é um ideal primo se, e somente se A'_0 for um corpo, ou equivalentemente, para anéis comutativos finitos, se A'_0 não tem divisores de zero. Assim, a ideia do programa é basicamente para eliminar os divisores de zero estendendo o ideal original.

Então, vamos começar por tomar todos os produtos entre os elementos de A'_0, depois de desconsiderar as suas identidades e o seu zero (os quais são irrelevantes para os nossos propósitos). De acordo com a regra que define $R(S_3)$, temos

$$(a, b, c)(d, e, f) = (ad + be + cf, ae + bd + cf, af + bf + cd + ce + cf).$$

O próximo passo é determinar os divisores de zero. Para isso, fixe $(0,1,0)$ e

$$\begin{aligned}(0,1,0)(0,1,0) &= (1,0,0)\\ (0,1,0)(1,1,0) &= (1,1,0)\\ (0,1,0)(0,0,1) &= (0,0,1)\\ (0,1,0)(1,0,1) &= (0,1,1)\\ (0,1,0)(0,1,1) &= (1,0,1)\\ (0,1,0)(1,1,1) &= (1,1,1)\end{aligned}$$

Com as operações realizadas acima verificamos que $(0,1,0)$ não é um divisor de zero uma vez que nenhum dos produtos acima se anula, e daí o programa continua. Continuando o processo com o próximo elemento de A_0', fixamos agora $(1,1,0)$ e obtemos

$$\begin{aligned}(1,1,0)(0,1,0) &= (1,1,0)\\ (1,1,0)(1,1,0) &= (0,0,0)\\ (1,1,0)(0,0,1) &= (0,0,0)\\ (1,1,0)(1,0,1) &= (1,1,0)\\ (1,1,0)(0,1,1) &= (1,1,0)\\ (1,1,0)(1,1,1) &= (0,0,0)\end{aligned}$$

donde vemos que $(1,1,0)$ é um divisor de zero e o programa para. Assim, escrevemos

$$I_1' := \langle 2, (1,1,0)\rangle$$

e daí

$$A_1' = \frac{R(S_3)}{I_1} = \{0, 1, (0,1,0), (0,0,1), (1,0,1), (0,1,1), (1,1,1)\}.$$

Note agora que A_1' escrito acima pode ter elementos iguais módulo I_1', como por exemplo

$$1 = 1 + 0 = 1 + (1,1,0) = (0,1,0).$$

Eliminando as redundâncias mod I_1', obtemos que

$$A_1' := \frac{R(S_3)}{I_1} = \{0, 1, (0,0,1), (1,0,1)\}.$$

Reiniciando o processo, fixamos agora $(0,0,1)$,

$$\begin{aligned}(0,0,1)(0,0,1) &= (1,1,1);\\ (0,0,1)(1,0,1) &= (1,1,0) = 0;\end{aligned}$$

onde temos que existem produtos se anulando módulo I_1', e portanto $(0,0,1)$ é um divisor de zero em A_1' e daí escreva

$$I_2' := \langle 2, (1,1,0), (0,0,1) \rangle$$

donde vemos que (já eliminando as redundâncias mod I_2')

$$A_2' := \frac{R(S_3)}{I_2'} = \{0,1\}.$$

E portanto, concluímos que $A_2' \cong \mathbb{F}_2$, e I_2' é um ideal primo (neste caso, é também um ideal maximal). Escreva então

$$P' := I_2' = \langle 2, (1,1,0), (0,0,1) \rangle.$$

Agora tentaremos reduzir o número de geradores de I_2', e para isso, escreva

$$(1,1,0) = (a,b,c)(0,0,1)$$

o qual fornece o sistema em $\mathbb{F}_2$:

$$\begin{aligned} 1 &= c \\ 1 &= c \\ 0 &= a+b+c \end{aligned}$$

dos quais buscamos soluções não triviais. E ele tem duas:

$$(1,1,0) = (1,0,1)(0,0,1) = (0,1,1)(0,0,1)$$

e disso, podemos escrever

$$P' = \langle 2, (0,0,1) \rangle$$

e com isso, podemos escrever que

$$P' := I_2' = \langle 2\chi_1, \chi_3 \rangle$$

é um ideal primo $R(G)$ (ponto de C_1') que projeta sobre $\langle 2 \rangle \in \mathrm{Spec}(\mathbb{Z})$. E pelo Teorema 2.1.(II).(vi)

$$\mathrm{edim}_{P'}(C') \leq 2.$$

Note que neste caso obtivemos precisamente o ponto racional determinado na demonstração da Proposição 3.1.

Método 2: *Estudo do grafo orientado associado a $R(G)/\langle p \rangle$.*

Podemos saber previamente da teoria quantos pontos singulares a curva C pode ter e, aqui, tivemos sorte que encontramos o caminho certo. Mas note, por exemplo, que $\langle 2\chi_1, \chi_1 + \chi_3 \rangle$ é outro ponto de C que projeta sobre $\langle 2 \rangle \in \mathrm{Spec}(\mathbb{Z})$. Em geral, esse

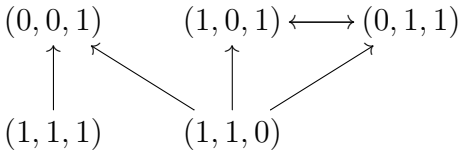
procedimento tem de ser repetido algumas vezes, com diferentes ordenamentos de A_0'. E isso é o que motiva o método 2.

Primeiro note que não precisamos de olhar para todas as ordenações possíveis para os elementos de A_0', basta considerar as diferentes ordenações para os divisores de zero de A_0', algo que poderíamos calcular a priori através da sua tabela de multiplicação, que no caso exemplificado neste passo é:

$\times$	$(0,1,0)$	$(1,1,0)$	$(0,0,1)$	$(1,0,1)$	$(0,1,1)$	$(1,1,1)$
$(0,1,0)$	1	$(1,1,0)$	$(0,0,1)$	$(0,1,1)$	$(0,1,1)$	$(1,1,1)$
$(1,1,0)$	$(1,1,0)$	0	0	$(1,1,0)$	$(1,1,0)$	0
$(0,0,1)$	$(0,0,1)$	0	$(1,1,1)$	$(1,1,0)$	$(1,1,0)$	$(1,1,1)$
$(1,0,1)$	$(0,1,1)$	$(1,1,0)$	$(1,1,0)$	$(0,1,1)$	$(1,0,1)$	0
$(0,1,1)$	$(0,1,1)$	$(1,1,0)$	$(1,1,0)$	$(1,0,1)$	$(0,1,1)$	0
$(1,1,1)$	$(1,1,1)$	0	$(1,1,1)$	0	0	$(1,1,1)$

E daí vemos que $(1,1,0)$, $(0,0,1)$, $(1,0,1)$, $(0,1,1)$ e $(1,1,1)$ são os divisores de zero de A_0. Note também que não podemos incluir todos os divisores de zero ao mesmo tempo. Por exemplo, $(0,0,1)$ e $(1,0,1)$ são divisores de zero, mas reunindo-os em um ideal produziremos todo o anel.

Uma vez conhecidos os divisores de zero de A_0', podemos construir o seguinte grafo orientado (note que o mesmo pode, eventualmente, ser decompostos em grafos orientados disjuntos):



onde "$a \longrightarrow b$" significa *"a pertence ao ideal gerado por b"* e para construir o grafo tomamos os divisores de zero distintos de A como *vértices*.

Em seguida, tomar como *sorvedouro* (= um vértice do grafo que tem grau de saída nulo, ou seja, o número de "setas" que saem do vértice é zero) os elementos $(0,0,1)$ e $(1,0,1)$ (ou o "equivalente" vértice $(0,1,1)$) e verifique se reunindo-os em um ideal obtemos um elemento inversível. Isso pode ser feito tomando somas de elementos nas linhas 3 e 4 da tabela de multiplicação. E, na verdade, a primeira soma já produz um inversível: $(0,0,1)+(0,1,1)=(0,1,0)$. Assim, podemos concluir imediatamente a partir do grafo orientado que

$$P_1 := \langle 2\chi_1, \chi_3 \rangle \qquad \text{e} \qquad P_2 := \langle 2\chi_1, \chi_1+\chi_3 \rangle = \langle 2\chi_1, \chi_2+\chi_3 \rangle$$

são pontos de C' sobre 2, e que

$$\operatorname{edim}_{P_1}(C') \leq 2 \quad \text{e} \quad \operatorname{edim}_{P_2}(C') \leq 2$$

pelo Teorema 2.1.(II).(v).

Passo 6: *Determinando as dimensões de mergulho:*

Com o objetivo de determinar $\mathrm{edim}_{P'}(C')$, devemos encontrar o corpo residual $k_{P'}$.

No caso em que estamos desenvolvendo, obtivemos no passo anterior que $k_{P'} = \mathbb{F}_2$. O próximo passo é determinar se o conjunto de geradores para P' é linearmente independente no $k_{P'}$-espaço vetorial P'/P'^2. Calculando

$$P'^2 = \langle 4, (0,0,2), (1,1,1) \rangle.$$

Escreva

$$a(2,0,0) + b(0,0,1) \in P'^2$$

com $a, b \in k_{P'} = \mathbb{F}_2 = \{0,1\}$, o que fornece o seguinte sistema:

$$\begin{aligned} 2a &= 4c + 2h + i + j + k \\ 0 &= 4d + 2h + i + j + k \\ b &= 4e + 2f + 2g + 2h + i + j + k \end{aligned}$$

com c, d, e, f, g, h, i, j, $k \in \mathbb{Z}$. Assim, o lado direito do sistema pode ser reduzido a $\mathbb{F}_2$ e obtemos

$$\begin{aligned} 2a &= i + j + k \\ 0 &= i + j + k \\ b &= i + j + k \end{aligned}$$

o que implica que $a = b = 0$ e assim, $\mathrm{edim}_{P'}(C') = 2$.

Passo 7: *Reinicie o algoritmo com o próximo primo.*

Referências

[A] M. F. Atiyah, *Characters and cohomology of finite group*, Publ. Math. de l'IHÉS, **9** (1961) 23-64.

[B] A. G. Bueno, *Os Esquemas Associados aos Anéis de Grupos Abelianos*, Ph. D. Thesis (2006).

[BC] J. M. F. Bassalo, M. S. D. Cattani *Teoria de Grupos*, Livraria da Física, São Paulo (2008).

[BD] A. G. Bueno, M. Dokuchaev, *On spectra of abelian group rings*, Publicationes Mathematicae (Debrecen), **76** (2008) 269-284.

[BJN] P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul *Basic Abstract Algebra*, 2ªed., Cambridge University Press (1994).

[CS] G. Cornell, J. Silverman, *Arithmetic Geometry*, Springer, New York, (1986).

[D] M. Demazure, *Lectures on p-divisible groups*, Lecture Notes in Math. 302, Springer, Heidelberg, (1972).

[H] R. Hartshorne, *Algebraic Geometry*, Springer (1977).

[Mr] P. A. Martin, *Grupos, Corpos e Teoria de Galois*, Textos Universitários do IME-USP 02, Livraria da Física (2010).

[Mt] H. Matsumura, Commutative Ring Theory, Cambridge University Press (1986)

[Ml] J. S. Milne, *Étale Cohomology*, Princeton University Press (1980).

[Sg] G. Segal, *The representation-ring of a compact Lie group*, Publ. Math. de l'IHÉS, **34** (1968) 113-128.

[Sr] J. P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, Springer 42 (1977).

[Wa] W. Waterhouse, *Introduction to Affine Group Schemes*, Graduate Texts in Mathematics, Springer-Verlag, New York, **66** (1979).

[We] P. Webb, *A Course in Finite Group Representation Theory*, Cambridge Studies in Advanced Mathematics, Cambridge, University of Minnesota (2016).