Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

ALGUMAS GENERALIZAÇÕES PARA O ÚLTIMO TEOREMA DE FERMAT

por

BÁRBARA SEELIG POGORELSKY

Porto Alegre, agosto de 2005

Dissertação submetida por BÁRBARA SEELIG POGORELSKY* como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professora Orientadora:

Dra. Luisa Rodriguez Doering

Banca Examinadora:

Dra. Ada Maria de Souza Doering
Dr. Antonio Paques
Dra. Luisa Rodriguez Doering
Dr. Yves Albert Emile Lequain (IMPA)

Data de Defesa: 25 de agosto de 2005.

---

* Bolsista do Conselho Nacional de Desenvolvimento Científico e Técnológico - CNPq

Agradecimentos

Aos meus pais, por todo apoio e incentivo que sempre recebi. Ao Alexandre, por estar sempre presente. A toda minha família, pelo amor e pelo carinho.

À UFRGS, pelo excelente ensino. Ao CNPq, pelo auxílio financeiro. Aos meus professores, por todo conhecimento transmitido, em especial à minha orientadora, Luisa Rodriguez Doering.

Agradeço também aos meus amigos, colegas e companheiros de escalada, em especial Leandro, Edson, Cíntia, Rodrigo, Joyce, Ricardo, Régis e Almeida.

Resumo

Neste trabalho estudamos três generalizações para o Último Teorema de Fermat.

A primeira generalização trata de expoentes negativos e de expoentes racionais. Além de mostrar em que casos estas equações possuem soluções, damos uma caracterização completa para todas as soluções inteiras não-nulas existentes.

A segunda generalização também trata de expoentes racionais, porém num contexto mais amplo. Aqui permitimos que as raízes n-ésimas sejam complexas, não necessariamente reais.

Na terceira generalização vemos que o Último Teorema de Fermat também vale para expoentes inteiros gaussianos.

Abstract

In this work we study three extensions of Fermat's Last Theorem.

The first extension deals with negative and rational exponents. Here we show when these equations have nonzero integral solutions and we characterize these solutions when they exist.

The second extension also deals with rational exponents, but in a wider context. Here we allow the use of complex roots, not necessarily the real ones.

In the third extension we show that Fermat's Last Theorem also holds for Gaussian integer exponents.

Conteúdo

Introdução

Por volta de 1637, o seguinte resultado foi enunciado pelo matemático francês Pierre de Fermat.

Teorema 0.1. *Se m é um número inteiro maior que 2, então a equação $x^m + y^m = z^m$ não tem solução inteira com $xyz \neq 0$.*

Fermat, que afirmava ter a demonstração para este resultado, acabou morrendo sem divulgar sua solução. Este problema ficou então conhecido como Último Teorema de Fermat, e ficou em aberto por mais de 350 anos. Ao longo destes anos, muitos matemáticos dedicaram suas carreiras à tentativa de provar este teorema. Finalmente em 1995, o matemático Andrew Wiles conseguiu provar o Último Teorema de Fermat. Sua demonstração, que utiliza teorias avançadas, não será estudada nesta dissertação, podendo ser encontrada em [6] e [9], mas utilizaremos, em vários momentos, o resultado.

A partir do resultado proposto por Fermat, já foram estudadas várias generalizações, algumas antes mesmo da prova do teorema. Nesta dissertação vamos estudar as generalizações feitas em [2], [7] e [10].

No Capítulo 2 mostraremos o trabalho de Tomescu e Vulpescu-Jalea apresentado em [7]. Veremos aqui generalizações para expoentes negativos e para expoentes racionais m/n. No caso dos expoentes racionais, trabalharemos apenas com raízes n-ésimas reais, porém sem restrições para os valores de m. Além disso, caracterizaremos todas as soluções destas equações, quando existirem. Neste caítulo provaremos os seguintes resultados:

Teorema: Seja $m \in \mathbb{N}^*$, $m > 2$. Então $x^{-m} + y^{-m} = z^{-m}$ não tem solução inteira.

Teorema: Sejam $m, n \in \mathbb{Z}^*$ com $n \geq 2$ tais que $mdc(m, n) = 1$. Então $x^{m/n} + y^{m/n} = z^{m/n}$ não tem solução inteira com $xyz \neq 0$ se $m \neq \pm 1, \pm 2$.

No Capítulo 3 veremos a generalização para expoentes racionais feita em [2] por Bennett, Glass e Székely. No teorema mostrado por eles trabalharemos com raízes n-ésimas complexas da unidade, porém exigiremos $m > 2$. Mostraremos o teorema a seguir:

Teorema: Sejam m e n números inteiros positivos primos entre si com $m > 2$. Então a equação $x^m + y^m = z^m$ possui uma solução complexa (a, b, c) com $a^n, b^n, c^n \in \mathbb{Z}$ se e somente se n é divisível por 6. Neste caso, $a^n = b^n = c^n$.

Finalmente no Capítulo 4 veremos a generalização de Zuehlke para expoentes inteiros gaussianos mostrada em [10]. Esta generalização é dada pelo seguinte teorema:

Teorema: Sejam $m, n \in \mathbb{Z}$ com $m \neq 0$. Então a equação

$$x^{n+im} + y^{n+im} = z^{n+im}$$

não possui soluções inteiras não-nulas.

Antes de provar estas generalizações, vamos analisar alguns resultados da Teoria de Galois, ferramenta que será usada no Capítulo 2.

Capítulo 1

Preliminares

Neste capítulo serão provados alguns resultados da Teoria de Galois que serão necessários nos próximos capítulos.

1.1 Extensões de Corpos

Sejam K e L corpos de característica zero.

Definição 1.1. Dizemos que L é uma extensão de K se existe um monomorfismo $i : K \hookrightarrow L$.

Observação 1.2. Note que, associando K com $i(K)$, podemos pensar que $K \subseteq L$.

Definição 1.3. Sejam L uma extensão de K e L^* uma extensão de K^*. Dizemos que estas extensões são isomorfas se existem isomorfismos $\lambda : K \to K^*, \mu : L \to L^*$ tais que $\mu|_K = \lambda$.

Definição 1.4. Seja $\alpha \in L$. Dizemos que α é algébrico sobre K se existe um polinômio não-nulo $p(x) \in K[x]$ tal que $p(\alpha) = 0$.

Definição 1.5. Se $\alpha \in L$ não é algébrico sobre K, então dizemos que α é transcendente sobre K.

Definição 1.6. Dizemos que L é uma extensão algébrica de K se todo elemento de L é algébrico sobre K. Caso contrário, dizemos que L é uma extensão transcendente de K.

Definição 1.7. Seja $\alpha \in L$. $K(\alpha)$ é o menor corpo contendo K e α. Indutivamente definimos $K(\alpha_1, ..., \alpha_n) = K(\alpha_1, ..., \alpha_{n-1})(\alpha_n)$.

Definição 1.8. Dizemos que L é uma extensão simples de K se existe $\alpha \in L$ tal que $L = K(\alpha)$.

Definição 1.9. Seja $\alpha \in L$ algébrico sobre K. O polinômio mínimo de α sobre K é um polinômio mônico $p_\alpha(x) \in K[x]$ de grau mínimo tal que $p_\alpha(\alpha) = 0$.

Observação 1.10. Decorre diretamente da definição que o polinômio mínimo é sempre irredutível.

Proposição 1.11. *Seja $\alpha \in L$ algébrico sobre K e seja $q(x) \in K[x]$ tal que $q(\alpha) = 0$. Então $p_\alpha(x)$ divide $q(x)$ em K.*

Demonstração: Como $q(\alpha) = 0$, temos que o grau de $q(x)$ é maior ou igual ao grau de $p_\alpha(x)$. Logo, existem polinômios $r(x), s(x) \in K[x]$ tais que

$$q(x) = p_\alpha(x) \cdot s(x) + r(x)$$

com o grau de $r(x)$ menor que o grau de $p_\alpha(x)$. Logo,

$$0 = q(\alpha) = p_\alpha(\alpha) \cdot s(\alpha) + r(\alpha) = r(\alpha).$$

Se $r \neq 0$ temos um absurdo, pois pela definição de polinômio mínimo o grau de $p_\alpha(x)$ é mínimo. Então $r(x) = 0$ e $p_\alpha(x)$ divide $q(x)$. □

Observação 1.12. Obtemos da proposição anterior que o polinômio mínimo é único. De fato, suponhamos que existam dois polinômios mônicos de grau mínimo r $p_\alpha(x), p'_\alpha(x)$ tais que $p_\alpha(\alpha) = p'_\alpha(\alpha) = 0$. Da proposição anterior, temos $p_\alpha(x)|p'_\alpha(x)$ e também $p'_\alpha(x)|p_\alpha(x)$. Logo, estes polinômios diferem por uma constante multiplicada. Mas $p_\alpha(x), p'_\alpha(x)$ são mônicos, então esta constante é igual a um e portanto $p_\alpha(x) = p'_\alpha(x)$.

Lema 1.13. *Se $\phi : K \to R$ é um homomorfismo de anéis, K é um corpo e $\phi \neq 0$, então ϕ é um monomorfismo.*

Demonstração: Seja $I = Ker\phi$. Sabemos que I é um ideal de K. Como K é um corpo, seus únicos ideais são 0 e K. Mas $I = K$ nos dá $\phi \equiv 0$. Logo, $I = 0$ e ϕ é um monomorfismo. □

Lema 1.14. *Se $m \in K[x]$ é um polinômio irredutível e $I = (m)$ é o ideal de $K[x]$ gerado por m, então $K[x]/I$ é um corpo.*

Demonstração: Seja $f + I$ um elemento não-nulo de $K[x]/I$. Como $f \notin I$ e m é irredutível, temos $mdc(m, f) = 1$. Então existem $a, b \in K[x]$ tais que:

$$af + bm = 1.$$

Passando ao anel quociente obtemos:

$$(a + I)(f + I) + (b + I)(m + I) = (a + I)(f + I) = 1 + I$$

pois $m + I = I = 0$. Daí temos que $a + I$ é o inverso de $f + I$ e portanto $K[x]/I$ é um corpo. □

Proposição 1.15. *Se $m \in K[x]$ é um polinômio mônico e irredutível sobre K, então existe uma extensão $K(\alpha)$ de K tal que m é o polinômio mínimo de α sobre K.*

Demonstração: Sejam $i : K \hookrightarrow K[x]$ o monomorfismo identidade, $I = (m)$ o ideal de $K[x]$ gerado por m e $\nu : K[x] \to K[x]/I$ o homomorfismo projeção. Por 1.14, $K[x]/I$ é um corpo. Logo, por 1.13, $\nu i : K \to K[x]/I$ é um monomorfismo e podemos identificar K com $K' = \nu(i(K)) \subseteq K[x]/I$. Vejamos agora que $K[x]/I = K'(x + I)$.

Seja $f + I \in K[x]/I$, onde $f(x) = a_0 + a_1x + ... + a_nx^n$. Então:

$$f + I = (a_0 + I) + (a_1 + I)(x + I) + ... + (a_n + I)(x + I)^n$$

Logo, $f + I \in K'(x + I)$. Reciprocamente, seja $\dfrac{\overline{f}}{\overline{g}} \in K'(x + I)$. Temos claramente que $\overline{f}, \overline{g} \in K[x]/I$. Como, por 1.14, $K[x]/I$ é corpo, então $\dfrac{\overline{f}}{\overline{g}} \in K[x]/I$.

Notemos agora que m é o polinômio mínimo de $x + I$ em $K[x]$ pois:

$$m(x + I) = m(x) + I = I = 0$$

e ainda m é um polinômio mônico e irredutível. □

Lema 1.16. *Sejam $K(\alpha)$ uma extensão algébrica simples de K e $p_\alpha(x) \in K[x]$ o polinômio mínimo de α sobre K. Então todo elemento de $K(\alpha)$ pode ser unicamente expressado na forma $q(\alpha)$, onde $q(x) \in K[x]$ e o grau de $q(x)$ é menor que o grau de $p_\alpha(x)$.*

Demonstração: Seja $k \in K(\alpha)$. Então $k = \dfrac{f(\alpha)}{g(\alpha)}$ com $f, g \in K[x],\ g(\alpha) \neq 0$. Portanto, $p_\alpha(x)$ não divide $g(x)$. Como $p_\alpha(x)$ é irredutível sobre K, então $mdc(p_\alpha, g) = 1$, o que implica que existem $a, b \in K[x]$ tais que $ag + bp_\alpha = 1$. Logo:

$$1 = a(\alpha)g(\alpha) + b(\alpha)p_\alpha(\alpha) = a(\alpha)g(\alpha).$$

Obtemos então:

$$k = \frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha) = h(\alpha),\ \text{com } h(x) \in K[x].$$

Seja $r(x)$ o resto da divisão de $h(x)$ por $p_\alpha(x)$. Então $\partial r < \partial p_\alpha$ e ainda:

$$h(\alpha) = p_\alpha(\alpha)s(\alpha) + r(\alpha) = r(\alpha).$$

Daí temos $k = r(\alpha)$, com $r(x) \in K[x]$ e $\partial r < \partial p_\alpha$.

Suponhamos agora que $k = r(\alpha) = q(\alpha)$ com $r(x), q(x) \in K[x]$ e $\partial r, \partial q < \partial p_\alpha$. Seja $u = r - q$. Temos que $\partial u < \partial p_\alpha$ e:

$$u(\alpha) = r(\alpha) - q(\alpha) = k - k = 0.$$

Logo, pela definição de polinômio mínimo, temos que $u \equiv 0$ e portanto $r(x) = q(x)$. □

Proposição 1.17. *Sejam $K(\alpha), K(\beta)$ extensões algébricas simples de K tais que α e β possuem o mesmo polinômio mínimo $p(x)$ sobre K. Então as extensões $K(\alpha)$ e $K(\beta)$ são isomorfas e este isomorfismo pode ser tal que α é levado em β.*

Demonstração: Sejam $x, y \in K(\alpha)$. Então, por 1.16:

$$x = f(\alpha) = x_0 + x_1\alpha + ... + x_n\alpha^n,\ \text{com } f(x) \in K[x]$$

$$y = g(\alpha) = y_0 + y_1\alpha + ... + y_n\alpha^n,\ \text{com } g(x) \in K[x]$$

onde $n = \partial p_\alpha - 1$. Definimos:

$$\begin{aligned} \phi : K(\alpha) &\to K(\beta) \\ q(\alpha) &\mapsto q(\beta) \end{aligned}$$

onde $q(x) \in K[x]$ e $\partial q \leq n = \partial p_\alpha - 1$. Por 1.16, ϕ é claramente sobrejetora. Além disso, $\phi(1) = 1$ nos dá ϕ injetora. Vejamos agora que é um homomorfismo:

$$\begin{aligned} \phi(x+y) = \phi((f+g)(\alpha)) = (f+g)(\beta) = f(\beta) + g(\beta) \\ = \phi(f(\alpha)) + \phi(g(\alpha)) = \phi(x) + \phi(y). \end{aligned}$$

Seja $h(\alpha) = xy$. Temos que:

$$\phi(x) \cdot \phi(y) = f(\beta) \cdot g(\beta) \text{ e } \phi(xy) = h(\beta).$$

Mas:

$$f(\alpha) \cdot g(\alpha) - h(\alpha) = xy - xy = 0.$$

Logo, $p_\alpha | (fg - h)$, ou seja, existe $q(x) \in K[x]$ tal que $fg = p_\alpha q + h$. Então $f(\beta)g(\beta) = p_\alpha(\beta)q(\beta) + h(\beta) = h(\beta)$, pois $p_\alpha(x) = p_\beta(x)$. Portanto:

$$\phi(xy) = h(\beta) = f(\beta) \cdot g(\beta) = \phi(x) \cdot \phi(y)$$

e segue que ϕ é um isomorfismo tal que $\phi|_K = id$ e $\phi(\alpha) = \beta$. □

Definição 1.18. Seja $i : K \to L$ um monomorfismo de corpos. Podemos definir naturalmente um monomorfismo $\bar{i} : K[x] \to L[x]$ por:

$$\bar{i}(k_0 + k_1 x + ... + k_n x^n) = i(k_0) + i(k_1)x + ... + i(k_n)x^n.$$

Observação 1.19. Se i é um isomorfismo, então $\bar{i}$ também é um isomorfismo.

Proposição 1.20. *Sejam K, L corpos e $i : K \to L$ um isomorfismo. Sejam $K(\alpha), L(\beta)$ extensões algébricas simples. Se $i(m_\alpha(x)) = m_\beta(x)$, então existe um isomorfismo $j : K(\alpha) \to L(\beta)$ tal que $j|_K = i$ e $j(\alpha) = \beta$.*

Demonstração: Seja $n = \partial m_\alpha - 1$. Todo elemento de $K(\alpha)$ pode ser escrito da forma $p(\alpha) = k_0 + k_1\alpha + ... + k_n\alpha^n$. Definimos então $j : K(\alpha) \to L(\beta)$ da

forma $j(p(\alpha)) = \overline{i}(p)(\beta)$. Temos que j é claramente bijetor, vejamos então que é homomorfismo:

$$\begin{aligned} j(p(\alpha) + q(\alpha)) &= j((p+q)(\alpha)) = \overline{i}(p+q)(\beta) = (\overline{i}(p) + \overline{i}(q))(\beta) \\ &= \overline{i}(p)(\beta) + \overline{i}(q)(\beta) = j(p(\alpha)) + j(q(\alpha)). \end{aligned}$$

$$\begin{aligned} j(p(\alpha) \cdot q(\alpha)) &= j((pq)(\alpha)) = \overline{i}(pq)(\beta) = \overline{i}(p)(\beta) \cdot \overline{i}(q)(\beta) \\ &= j(p(\alpha)) \cdot j(q(\alpha)). \end{aligned}$$

Logo, j é um isomorfismo de corpos. Além disso, $j|_K = i$ e $j(\alpha) = \beta$ e portanto as extensões são isomorfas. □

1.2 O Grau de uma Extensão

Definição 1.21. O grau de uma extensão L de K, notado $[L : K]$, é a dimensão de L considerado como K-espaço vetorial.

Proposição 1.22. *Sejam $K \subseteq M \subseteq L$ corpos. Então*

$$[L : K] = [L : M] \cdot [M : K].$$

Demonstração: Sejam $(x_i)_{i \in I}$ base de M como K-espaço vetorial e $(y_j)_{j \in J}$ base de L como M-espaço vetorial. Vejamos que $(x_i y_j)_{i \in I, j \in J}$ é base de L como K-espaço vetorial.

Primeiramente vejamos que $(x_i y_j)_{i \in I, j \in J}$ é um conjunto linearmente independente sobre K. Suponhamos que existe uma combinação linear nula

$$0 = \sum_{i,j} k_{ij} x_i y_j = \sum_j \left(\sum_i k_{ij} x_i \right) y_j$$

com $k_{ij} \in K$. Como $\sum_i k_{ij} x_i \in M$ e $(y_j)_{j \in J}$ é um conjunto linearmente independente sobre M, temos que $\sum_i k_{ij} x_i = 0$ para todo $j \in J$. Mas $k_{ij} \in K$ e $(x_i)_{i \in I}$ é um conjunto linearmente independente sobre K, então $k_{ij} = 0$ para todos $i \in I, j \in J$.

Vejamos agora que $(x_i y_j)_{i\in I, j\in J}$ gera L sobre K. Seja $l \in L$. Então existem $y_j \in L$ e $m_j \in M$ tais que $l = \sum_j m_j y_j$. Mas sabemos também que para todo j temos $m_j = \sum_i k_{ij} x_i$, com $k_{ij} \in K$. Temos então

$$l = \sum_j \left(\sum_i k_{ij} x_i \right) y_j = \sum_{i,j} k_{ij} x_i y_j.$$

□

Proposição 1.23. *Seja $K(\alpha)$ uma extensão simples. Se $K(\alpha)$ é transcendente, então $[K(\alpha) : K] = \infty$. Se $K(\alpha)$ é algébrica, então $[K(\alpha) : K] = \partial p_\alpha(x)$.*

Demonstração: Se α é transcendente, basta notar que $1, \alpha, \alpha^2, ...$ são linearmente independentes sobre K. Logo, $[K(\alpha) : K] = \infty$. Para o caso algébrico, seja $n = \partial p_\alpha$. Decorre de 1.16 que $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ é uma base de $K(\alpha)$ como K-espaço vetorial. Portanto, $[K(\alpha) : K] = n = \partial p_\alpha(x)$. □

Lema 1.24. *L é uma extensão finita de K se e somente se L é algébrica sobre K e existem $\alpha_1, ..., \alpha_s \in L$ tais que $L = K(\alpha_1, ..., \alpha_s)$.*

Demonstração: Seja L uma extensão finita de K. Então existe uma base $\alpha_1, ..., \alpha_s$ de L como K-espaço vetorial, o que nos dá $L = K(\alpha_1, ..., \alpha_n)$. Vejamos que a extensão é algébrica. Sejam $n = [L : K]$ e $l \in L$. Então $1, l, ..., l^n$ é linearmente dependente e portanto existem $k_0, ..., k_n \in K$ tais que $k_0 + k_1 l + ... + k_n l^n = 0$, ou seja, l é algébrico sobre K. Concluímos que a extensão é algébrica.

Reciprocamente, seja $K(\alpha_1, ..., \alpha_s)$ uma extensão algébrica. Vejamos por indução que esta extensão é finita. Se $s = 1$, temos de 1.23 que a extensão é finita. Suponhamos agora que $K(\alpha_1, ..., \alpha_{s-1})$ é finita. Temos que $K(\alpha_1, ..., \alpha_s) = K(\alpha_1, ..., \alpha_{s-1})(\alpha_s)$ e ainda, por 1.22:

$$\begin{aligned}[K(\alpha_1, ..., \alpha_s) : K] = [K(\alpha_1, ..., \alpha_{s-1})(\alpha_s) : K(\alpha_1, ..., \alpha_{s-1})] \\ \cdot [K(\alpha_1, ..., \alpha_{s-1}) : K] = n.m\end{aligned}$$

onde $n = \partial m_{\alpha_s}$ sobre $K(\alpha_1, ..., \alpha_{s-1})$ e $m = [K(\alpha_1, ..., \alpha_{s-1}) : K]$. Logo, $K(\alpha_1, ..., \alpha_s)$ é uma extensão finita de K. □

1.3 Extensões Normais e Separáveis

Definição 1.25. Seja $f \in K[x]$. Dizemos que f se decompõe sobre K se f pode ser expresso como um produto de fatores lineares da forma:

$$f(x) = k(x - \alpha_1)...(x - \alpha_n)$$

onde $k, \alpha_1, ..., \alpha_n \in K$.

Definição 1.26. O corpo Σ é dito um corpo de decomposição para o polinômio $f \in K[x]$ se $K \subseteq \Sigma$ e:

i) f se decompõe sobre K.

ii) Se $K \subseteq \Sigma' \subseteq \Sigma$ e f se decompõe sobre Σ' então $\Sigma' = \Sigma$.

Observação 1.27. A condição ii) da definição de corpo de decomposição é claramente equivalente a dizer que $\Sigma = K(\sigma_1, ..., \sigma_n)$, onde $\sigma_1, ..., \sigma_n$ são as raízes de f em Σ.

Proposição 1.28. *Seja $f \in K[x]$. Então existe um corpo de decomposição para f.*

Demonstração: Provaremos por indução em $n = \partial f$. Se $\partial f = 1$ então f se decompõe sobre K. Suponhamos agora que f não se decompõe sobre K. Seja f_1 um fator irredutível de f de grau maior que um. Então, por 1.15, existe $K(\sigma_1)$ tal que $f_1(\sigma_1) = 0$. Logo, em $K(\sigma_1)[x]$ temos $f = (x - \sigma_1)g$ onde $\partial g = \partial f - 1$. Pela hipótese de indução existe Σ corpo de decomposição de g sobre $K(\sigma_1)$ e portanto Σ também é corpo de decomposição de f sobre K. □

Proposição 1.29. *Sejam $i : K \to K'$ um isomorfismo de corpos, $f \in K[x]$ e Σ um corpo de decomposição de f sobre K. Seja L uma extensão de K' tal que $i(f)$ se decompõe sobre L. Então existe um monomorfismo $j : \Sigma \to L$ tal que $j|_K = i$.*

Demonstração: Provaremos o resultado por indução em ∂f. Se $\partial f = 1$, então $\Sigma = K$ e o resultado é trivial. Se $\partial f = n$, em $\Sigma[x]$ temos:

$$f(x) = k(x - \sigma_1)...(x - \sigma_n).$$

Temos que $m_{\sigma_1} \in K[x]$ é um fator irredutível de f e que $i(m_{\sigma_1})$ divide $i(f)$, que se decompõe sobre L. Logo, em $L[x]$ temos:

$$i(m_{\sigma_1}) = (x - \alpha_1)...(x - \alpha_r).$$

Como $i(m_{\sigma_1})$ é mônico e irredutível sobre K', então $i(m_{\sigma_1}) = m_{\alpha_1}$ sobre K'. Por 1.20 obtemos que existe um isomorfismo $j_1 : K(\sigma_1) \to K'(\alpha_1)$ tal que $j_1|_K = i$ e $j_1(\sigma_1) = \alpha_1$. Agora Σ é um corpo de decomposição de $g = f/(x - \sigma_1)$ sobre $K(\sigma_1)$ e pela hipótese de indução existe um monomorfismo $j : \Sigma \to L$ tal que $j|_{K(\sigma_1)} = j_1$. Então $j|_K = i$, de onde segue o resultado. □

Proposição 1.30. *Sejam $i : K \to K'$ um isomorfismo de corpos, T um corpo de decomposição de f sobre K e T' um corpo de decomposição de $i(f)$ sobre K'. Então existe um isomorfismo $j : T \to T'$ tal que $j|_K = i$, ou seja, T e T' são extensões isomorfas.*

Demonstração: Por 1.29 sabemos que existe um monomorfismo $j : T \to T'$ tal que $j|_K = i$. Mas $i(f)$ se decompõe sobre $j(T) \subseteq T'$ e T' é um corpo de decomposição de $i(f)$, então $j(T) = T'$ e j é um isomorfismo. □

Definição 1.31. Uma extensão L de um corpo K é dita normal se todo polinômio irredutível sobre K que possui uma raiz em L se decompõe em L.

Proposição 1.32. *Uma extensão L de um corpo K é normal e finita se e somente se L é o corpo de decomposição para algum polinômio $f \in K[x]$.*

Demonstração: Suponhamos que L é uma extensão normal e finita de K. Por 1.24, temos que $L = K(\alpha_1, ..., \alpha_s)$, com α_i algébrico sobre K para $i = 1, ..., s$. Seja $f = m_{\alpha_1} \cdot ... \cdot m_{\alpha_s}$. Temos que cada m_{α_i} é irredutível sobre K e possui uma raiz α_i em L. Logo, como L é normal, m_{α_i} se decompõe sobre L. Além disso, como L é gerado por K e por raízes de f, então L é o corpo de decomposição de f sobre K.

Reciprocamente, suponhamos que L é o corpo de decomposição de um polinômio $g \in K[x]$. Por 1.24, sabemos que L é uma extensão finita de K. Vejamos que é normal. Seja $f \in K[x]$ um polinômio irredutível com uma raiz $\theta_1 \in L$. Sejam $M \supseteq L$ o corpo de decomposição de fg sobre K e $\theta_2 \in M$ uma raiz de f. Temos:

$$[L(\theta_1) : L][L : K] = [L(\theta_1) : K] = [L(\theta_1) : K(\theta_1)][K(\theta_1) : K].$$

$$[L(\theta_2) : L][L : K] = [L(\theta_2) : K] = [L(\theta_2) : K(\theta_2)][K(\theta_2) : K].$$

Por 1.23, $[K(\theta_1) : K] = [K(\theta_2) : K]$. Além disso, $L(\theta_j)$ é um corpo de decomposição de g sobre $K(\theta_j)$, logo, por 1.17, as extensões $L(\theta_1), L(\theta_2)$ são isomorfas e portanto $[L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)]$. Concluímos então que $[L(\theta_1) : L] = [L(\theta_2) : L)] = n$. Mas $\theta_1 \in L$ nos dá $n = 1$ e conseqüentemente $\theta_2 \in L$, de onde segue que f se decompõe sobre L, ou seja, L é uma extensão normal de K. □

Definição 1.33. Um polinômio irredutível $f \in K[x]$ é separável sobre K se não possui raízes múltiplas em um corpo de decomposição. Dizemos que um polinômio qualquer é separável sobre K se seus fatores irredutíveis são separáveis sobre K.

Definição 1.34. Seja L uma extensão algébrica de K. Dizemos que $\alpha \in L$ é separável sobre K se m_α é separável sobre K. A extensão L é separável se todo $\alpha \in L$ é separável sobre K.

Lema 1.35. *Seja L uma extensão algébrica e separável de K e seja M um corpo intermediário. Então M é uma extensão separável de K e L é uma extensão separável de M.*

Demonstração: M é claramente separável sobre K pois $\alpha \in M \subseteq L$ e $m_\alpha \in K[x]$ é separável sobre K. Sejam $\alpha \in L$ e m_K, m_M seus polinômios mínimos sobre K e sobre M. Temos que α é separável sobre K, então m_K não possui raízes múltiplas. Mas $m_M | m_K$ em $M[x]$, logo, m_M não possui raízes múltiplas e portanto é separável sobre M. Segue daí que L é uma extensão separável de M. □

1.4 K-Automorfismos e K-Monomorfismos

Definição 1.36. Sejam $K \subseteq L$ corpos. Um automorfismo α de L é dito um K-automorfismo se $\alpha(k) = k$ para todo $k \in K$.

Definição 1.37. O grupo de Galois $\Gamma(L : K)$ de uma extensão é o grupo formado pelos K-automorfismos de L com a operação de composição de funções.

Definição 1.38. Seja H um subgrupo de $\Gamma(L : K)$. O corpo fixo de H, notado $H^{\dagger}$, é formado pelos elementos de L que são fixados por todos os K-automorfismos de H.

Definição 1.39. Sejam L uma extensão de K e M um corpo intermediário. $M^* = \Gamma(L : M)$ é o grupo formado pelos M-automorfismos de L.

Lema 1.40. *Se K, L são corpos, então todo conjunto de monomorfismos distintos $i : K \to L$ é linearmente independente sobre L.*

Demonstração: Sejam $\lambda_1, ..., \lambda_n$ monomorfismos distintos com $n > 1$. Suponhamos por absurdo que

$$a_1\lambda_1(x) + a_2\lambda_2(x) + ... + a_n\lambda_n(x) = 0$$

para todo $x \in K$ com $a_i's \in L$ não todos nulos. Sem perda de generalidade suponhamos que n é o número mínimo de $a_i's$ não nulos tais que a igualdade ocorre. Como $\lambda_1 \neq \lambda_n$, existe $y \in K$ tal que $\lambda_1(y) \neq \lambda_n(y)$, o que garante $y \neq 0$. Temos:

$$0 = a_1\lambda_1(xy) + ... + a_n\lambda_n(xy) = a_1\lambda_1(x)\lambda_1(y) + ... + a_n\lambda_n(x)\lambda_n(y)$$

para todo $x \in K$. Multiplicando a primeira equação por $\lambda_1(y)$ obtemos:

$$a_1\lambda_1(x)\lambda_1(y) + ... + a_n\lambda_n(x)\lambda_1(y) = 0.$$

Logo, subtraindo desta equação a anterior:

$$a_2\lambda_2(x)(\lambda_1(y) - \lambda_2(y)) + ... + a_n\lambda_n(x)(\lambda_1(y) - \lambda_n(y)) = 0$$

onde $a_n\lambda_n(x)(\lambda_1(y)-\lambda_n(y)) \neq 0$, ou seja, construímos uma combinação linear nula com $n-1$ termos não todos nulos. Absurdo. □

Lema 1.41. *Se $G = \{g_1, ..., g_n\}$ é um grupo e $g \in G$, então $\phi : G \to G$ tal que $\phi(g_i) = gg_i$ é um isomorfismo.*

Demonstração: Como $|G|$ é finita, basta mostrar que ϕ é injetor. Suponhamos que $gg_i = gg_j$. Como G é um grupo, existe $g^{-1} \in G$. Logo, $g^{-1}gg_i = g^{-1}gg_j$, ou seja, $g_i = g_j$ e portanto ϕ é um isomorfismo. □

Proposição 1.42. *Seja G um subgrupo finito do grupo de automorfismos de um corpo K e seja K_0 o corpo fixo de G. Então $[K : K_0] = |G|$.*

Demonstração: Suponhamos que $G = \{id = g_1, ..., g_n\}$. Então $|G| = n$. Suponhamos por absurdo que $[K : K_0] = m < n$ e seja $x_1, ..., x_m$ base de K como K_0-espaço vetorial. Temos o seguinte sistema de m equações e n incógnitas:

$$\begin{aligned} g_1(x_1)y_1 + ... + g_n(x_1)y_n &= 0 \\ g_1(x_2)y_1 + ... + g_n(x_2)y_n &= 0 \\ &\vdots \\ g_1(x_m)y_1 + ... + g_n(x_m)y_n &= 0 \end{aligned}$$

Como $m < n$, existem $y_1, ..., y_n \in K$ não todos nulos que verificam o sistema. Seja $a \in K$. Então $a = \sum_{i=1}^{m} \alpha_i x_i,\ \alpha_i \in K_0$ e portanto:

$$\begin{aligned} g_1(a)y_1 + ... + g_n(a)y_n &= g_1(\sum_{i=1}^{m} \alpha_i x_i)y_1 + ... + g_n(\sum_{i=1}^{m} \alpha_i x_i)y_n \\ &= \sum_{i=1}^{m} \alpha_i (g_1(x_i)y_1 + ... + g_n(x_i)y_n) \\ &= \sum_{i=1}^{m} \alpha_i \cdot 0 = 0 \end{aligned}$$

para todo $a \in K$, de onde $g_1, ..., g_n$ são linearmente dependentes. Absurdo, por 1.40.

Suponhamos agora que $[K : K_0] = m > n$. Seja $\{x_1, ..., x_{n+1}\}$ um conjunto linearmente independente. Então temos o seguinte sistema de n equações e $n + 1$ incógnitas:

$$\begin{aligned} g_1(x_1)y_1 + ... + g_1(x_{n+1})y_{n+1} &= 0 \\ g_2(x_1)y_1 + ... + g_2(x_{n+1})y_{n+1} &= 0 \\ &\vdots \\ g_n(x_1)y_1 + ... + g_n(x_{n+1})y_{n+1} &= 0 \end{aligned}$$

Como $n + 1 > n$, existem $y_1, ..., y_{n+1} \in K$ não todos nulos que satisfazem o sistema. Pego então uma solução com o número mínimo r de $y_i's \neq 0$. Seja

$g \in G$. Temos $g(g_j(x_1)y_1 + ... + g_j(x_r)y_r) = g(0) = 0$ para $j = 1, ..., n$. Mas, por 1.41, o sistema dado por

$$gg_j(x_1)g(y_1) + ... + gg_j(x_r)g(y_r) = 0$$

é equivalente ao sistema dado por

$$g_j(x_1)g(y_1) + ... + g_j(x_r)g(y_r) = 0$$

para $j = 1, ..., n$ pois uma equação é levada em outra. Logo,

$$g(y_1)(g_j(x_1)y_1 + ... + g_j(x_r)y_r) = g_j(x_1)y_1g(y_1) + ... + g_j(x_r)y_rg(y_1) = 0.$$

$$y_1(g_j(x_1)g(y_1) + ... + g_j(x_r)g(y_r)) = g_j(x_1)g(y_1)y_1 + ... + g_j(x_r)g(y_r)y_1 = 0.$$

Subtraindo a segunda equação da primeira obtemos:

$$g_j(x_2)(y_2g(y_1) - g(y_2)y_1) + ... + g_j(x_r)(y_rg(y_1) - g(y_r)y_1) = 0$$

para $j = 1, ..., n$. Pela minimalidade de r, $y_ig(y_1) - g(y_i)y_1 = 0$, ou seja, $y_ig(y_1) = g(y_i)y_1$ para $i = 2, ..., r$. Daí obtemos $g(y_1{y_i}^{-1}) = y_1{y_i}^{-1}$ para todo $g \in G$ e portanto $y_1{y_i}^{-1} = z_i' \in K_0$, ou seja, $y_i = y_1z_i$ com $z_i \in K_0, y_i \in K$ para $i = 2, ..., r$. Temos então:

$$\begin{aligned} g_j(x_1)y_1 + ... + g_j(x_r)y_r &= g_j(x_1)y_1 + g_j(x_2)y_1z_2... + g_j(x_r)y_1z_r \\ &= y_1(g_j(x_1) + g_j(x_2)z_2... + g_j(x_r)z_r) = 0 \end{aligned}$$

para $j = 1, ..., n$. Logo, pegando $j = 1$:

$$g_1(x_1) + g_1(x_2)z_2... + g_1(x_r)z_r = x_1 + x_2z_2 + ... + x_rz_r = 0$$

pois $g_1 = id$. Concluímos que $x_1, ..., x_r$ é linearmente dependente, o que é absurdo. Isto nos garante que $[K : K_0] = n = |G|$. □

Definição 1.43. Sejam $K \subseteq M \subseteq L$ corpos. Um K-monomorfismo $\phi : M \to L$ é um monomorfismo tal que $\phi(k) = k$ para todo $k \in K$.

Proposição 1.44. *Suponhamos que L é uma extensão normal e finita de K e M é um corpo intermediário. Seja $\tau : M \to L$ um K-monomorfismo. Então existe um K-automorfismo σ de L tal que $\sigma|_M = \tau$.*

Demonstração: Como L é uma extensão normal de K, então por 1.32 L é o corpo de decomposição de um polinômio $f \in K[x]$. Além disso, L também é o corpo de decomposição de f sobre M e de $\tau(f) = f$ sobre $\tau(M)$. Obtemos então o diagrama

$$\begin{array}{ccc} M & \to & \tau(M) \\ \downarrow & & \downarrow \\ L & \to & L \end{array}$$

e usando 1.30 concluímos que existe um isomorfismo $\sigma : L \to L$ tal que $\sigma|_M = \tau$. Portanto, σ é um K-automorfismo de L. □

Proposição 1.45. *Suponhamos que L é uma extensão normal e finita de K e que α, β são raízes em L de um polinômio irredutível $p \in K[x]$. Então existe um K-automorfismo $\sigma : L \to L$ tal que $\sigma(\alpha) = \beta$.*

Demonstração: Por 1.17 sabemos que existe um isomorfismo $\tau : K(\alpha) \to K(\beta)$ tal que $\tau|_K = id$ e $\tau(\alpha) = \beta$. Então, usando 1.44, basta extender τ para um automorfismo $\sigma : L \to L$. □

Definição 1.46. Seja L uma extensão algébrica de K. O fecho normal de L sobre K é uma extensão N de L tal que:

i) N é extensão normal de K.

ii) Se $L \subseteq M \subseteq N$ e M é extensão normal de K, então $M = N$.

Proposição 1.47. *Seja L uma extensão finita de K. Então existe um fecho normal N de L tal que N é uma extensão finita de K. Além disso, se M é outro fecho normal, então as extensões de K dadas por M e N são isomorfas.*

Demonstração: Sejam $x_1, ..., x_r$ base de L sobre K e p_{x_i} o polinômio mínimo de x_i sobre K para $i = 1, ..., r$. Seja N um corpo de decomposição para $f = p_{x_1}...p_{x_r}$ sobre L. Temos que N também é um corpo de decomposição para f sobre K e, por 1.32, N é uma extensão normal e finita de K. Seja P uma extensão normal de K tal que $L \subseteq P \subseteq N$. Então $x_i \in P$ e portanto p_{x_i} possui uma raiz em P para todo $i = 1, ..., r$. Como P é normal, concluímos

que f se decompõe sobre P e portanto $P = N$, de onde N é um fecho normal. Suponhamos agora que M e N são fechos normais. Então f se decompõe sobre M e sobre N. Logo, M e N contêm um corpo de decomposição de f sobre K e estes corpos M' e N' contêm L e são normais sobre K. Então $M = M'$ e $N = N'$ e pela unicidade dos corpos de decomposição dada em 1.30 temos que M e N são extensões isomorfas de K. □

Lema 1.48. *Suponhamos que $K \subseteq L \subseteq N \subseteq M$ onde L é uma extensão finita de K e N é o fecho normal. Seja τ um K-monomorfismo $\tau : L \to M$. Então $\tau(L) \subseteq N$.*

Demonstração: Sejam $\alpha \in L$ e p_α o polinômio mínimo de α sobre K. Então $0 = p_\alpha(\alpha) = \tau(p_\alpha(\alpha)) = p_\alpha(\tau(\alpha))$ e portanto $\tau(\alpha)$ é raiz de p_α. Como N é extensão normal de K temos que $\tau(\alpha) \in N$ e então $\tau(L) \subseteq N$. □

Proposição 1.49. *Seja L uma extensão finita de K. São equivalentes:*

i) L é uma extensão normal de K.

ii) Para toda extensão normal M de K contendo L todo K-monomorfismo $\tau : L \to M$ é um K-automorfismo de L.

iii) Existe uma extensão normal N de K contendo L tal que todo K-monomorfismo $\tau : L \to N$ é um K-automorfismo de L.

Demonstração: Suponhamos que L é uma extensão normal de K. Então L é o fecho normal desta extensão e por 1.48 $\tau(L) \subseteq L$. Mas L é um K-espaço vetorial e τ é uma aplicação K-linear, logo, como $[L : K]$ é finito e τ injetiva, $\tau(L) = L$. Daí segue que τ é um K-automorfismo de L.

Suponhamos agora que vale ii). Por 1.47 temos que existe o fecho normal N da extensão L de K. Então basta pegar a extensão de K dada por N o fecho normal e iii) segue trivialmente.

Para ver que iii) implica i), seja $f \in K[x]$ irredutível com uma raiz $\alpha \in L$. Então f se decompõe sobre N. Seja $\beta \in N$ uma raiz de f. Por 1.45, existe um K-automorfismo σ de N tal que $\sigma(\alpha) = \beta$. Mas, por hipótese, σ é um K-automorfismo de L e portanto $\beta \in L$. Logo, f se decompõe sobre L e L é uma extensão normal de K. □

Proposição 1.50. *Seja L uma extensão separável e de grau n de K. Então existem exatamente n K-monomorfismos distintos de L em um fecho normal N (e portanto em qualquer extensão normal M de K contendo L).*

Demonstração: Provaremos por indução em $n = [L : K]$. Se $n = 1$ o resultado segue trivialmente. Suponhamos que o resultado vale para extensões de grau menor ou igual a $n-1$ e sejam L uma extensão de K de grau n e $\alpha \in L \backslash K$ com polinômio mínimo $p_\alpha \in K[x]$. Temos que $\partial p_\alpha = [K(\alpha) : K] = r > 1$ e que p_α é um polinômio irredutível separável com uma raiz $\alpha \in N$. Então p_α se decompõe sobre N e suas raízes $\alpha = \alpha_1, ..., \alpha_r$ são todas distintas. Logo, como $[L : K(\alpha)] = s = \frac{n}{r} < n$, pela hipótese de indução existem exatamente s $K(\alpha)$-homomorfismos distintos $\rho_1, ..., \rho_s : L \to N$. Mas por 1.45 existem r K-automorfismos distintos de N $\tau_1, ..., \tau_r$ tais que $\tau_i(\alpha) = \alpha_i$ para $i = 1, ..., r$. Então $\phi_{ij} = \tau_i \rho_j : L \to N$ fornecem $n = r \cdot s$ K-monomorfismos distintos. Vejamos que estes são os únicos. Seja $\tau : L \to N$ um K-monomorfismo. Então $\tau(\alpha)$ é raiz de p_α em N e $\tau(\alpha) = \alpha_i$ para algum $i = 1, ..., r$. Portanto, $\phi = {\tau_i}^{-1}\tau : L \to N$ é um $K(\alpha)$-monomorfismo, ou seja, $\phi = {\tau_i}^{-1}\tau = \rho_j$ para algum $j = 1, ..., s$ e concluímos que $\tau = \tau_i \rho_j = \phi_{ij}$. □

Corolário 1.51. *Seja L é uma extensão normal, separável e de grau n de K. Então existem exatamente n K-automorfismos distintos de L, ou seja, $|\Gamma(L : K)| = n$.*

Proposição 1.52. *Sejam L uma extensão finita de K e G o seu grupo de Galois. Se L é normal e separável, então K é o corpo fixo de G.*

Demonstração: Seja K_0 o corpo fixo de G e seja $n = [L : K]$. Por 1.51 temos $|G| = n$ e por 1.42 $[L : K_0] = n$. Como $K \subseteq K_0$, temos $K = K_0$. □

1.5 O Teorema Fundamental

Lema 1.53. *Sejam L uma extensão finita, normal e separável de K, M um corpo intermediário e $\tau : L \to L$ um K-automorfismo. Então $(\tau(M))^* = \tau M^* \tau^{-1}$.*

Demonstração: Seja $M' = \tau(M)$ e sejam $\gamma \in M^*$, $x_1 \in M'$. Então $x_1 = \tau(x)$ para algum $x \in M$. Temos:

$$(\tau\gamma\tau^{-1})(x_1) = \tau\gamma(x) = \tau(x) = x_1.$$

Logo, $\tau M^*\tau^{-1} \subseteq M'^*$, pois $\tau\gamma\tau^{-1}$ fixa todo $x \in M'$ para toda $\gamma \in M^*$. Reciprocamente, seja $x_1 \in M$. Então $\tau(x_1) = x \in M'$ e se $\gamma \in M'^*$:

$$\tau^{-1}\gamma\tau(x_1) = \tau^{-1}\gamma(x) = \tau^{-1}(x) = x_1.$$

Portanto, $M'^* \subseteq \tau M^*\tau^{-1}$ de onde segue a igualdade. □

Teorema 1.54. (Teorema Fundamental da Teoria de Galois) *Sejam L uma extensão normal e separável de grau n de K, $G = \Gamma(L : K)$, $\mathcal{F}$ o conjunto dos corpos intermediários, $\mathcal{G}$ o conjunto dos subgrupos de G, $* : \mathcal{F} \to \mathcal{G}$ e $\dagger : \mathcal{G} \to \mathcal{F}$. Temos:*

i) As aplicações $*$ e $\dagger$ são inversas mútuas e determinam uma correspondência entre $\mathcal{G}$ e $\mathcal{F}$.

ii) Um corpo intermediário M é uma extensão normal de K se e somente se M^* é um subgrupo normal de G.

Demonstração:

i) Seja $M \in \mathcal{F}$. Então, por 1.35, L é uma extensão separável de M. Além disso, L é extensão normal de K, então, por 1.32, L é uma extensão normal de M. Logo, por 1.52, M é o corpo fixo de M^*, ou seja, $M^{*\dagger} = M$.

Reciprocamente, seja $H \in \mathcal{G}$. Sabemos que $H \subseteq H^{\dagger *}$, mas $H^{\dagger *\dagger} = (H^\dagger)^{*\dagger} = H^\dagger$, conforme provado acima. Logo, por 1.42, temos:

$$|H| = [L : H^\dagger] = [L : H^{\dagger *\dagger}] = |H^{\dagger *}|$$

e portanto $|H| = |H^{\dagger *}|$. Mas $|H|$ é finito e $H \subseteq H^{\dagger *}$, então $H = H^{\dagger *}$.

ii) Suponhamos que M é uma extensão normal de K e seja $\tau \in \Gamma(L : K)$. Então $\tau|_M : M \to L$ é um K-monomorfismo e por 1.49 concluímos que τ é um K-automorfismo de M, ou seja, $\tau(M) = M$. Usando 1.53 obtemos $\tau M^*\tau^{-1} = M^*$ e portanto $M^* \lhd G$.

Reciprocamente, suponhamos que $M^* \lhd G$ e seja $\sigma : M \to L$ um K-monomorfismo. Por 1.44, existe $\tau : L \to L$ um K-automorfismo tal que $\tau|_M = \sigma$, e então $\tau M^* \tau^{-1} = M^*$, pois $M^* \lhd G$. Usando 1.53 temos $M^* = (\tau(M))^*$ e por i) $\tau(M) = M$. Então $\sigma(M) = M$, e portanto σ é um K-automorfismo de M. Logo, por 1.49, M é uma extensão normal de K.

□

Proposição 1.55. *Seja m um inteiro positivo e seja $K = \mathbb{Q}(e^{2\pi i/m})$. Então $\Gamma(K : \mathbb{Q})$ é abeliano.*

Demonstração: Para isto veremos que K é isomorfo a um subgrupo de $\mathbb{Z}_m$. Temos que $e^{2\pi i/m}$ é uma raiz primitiva m-ésima da unidade. Logo, K é o corpo de decomposição de $p(x) = x^m - 1$ e portanto K é uma extensão normal e separável de $\mathbb{Q}$. Seja $\sigma \in \Gamma(K : \mathbb{Q})$. Como σ leva raízes de p em raízes de p, temos $\sigma(e^{2\pi i/m}) = (e^{2\pi i/m})^k$, onde $1 \leq k \leq m$. Definimos então o seguinte homomorfismo:

$$\begin{aligned} \varphi : &\Gamma(K : \mathbb{Q}) \to \mathbb{Z}_m \\ &\sigma \mapsto k \end{aligned}$$

Podemos ver que $ker\varphi = \{id\}$, logo, $\Gamma(K : \mathbb{Q}) \simeq Im\varphi$, que é um subgrupo de $\mathbb{Z}_m$. Daí concluímos que $\Gamma(K : \mathbb{Q})$ é abeliano. □

Capítulo 2

O Caso Real

O objetivo deste capítulo é caracterizar todas as soluções das equações

$$x^{-m} + y^{-m} = z^{-m} \tag{2.1}$$

onde $m \in \mathbb{N}^*,\ x, y, z \in \mathbb{Z}^*$ e

$$x^{m/n} + y^{m/n} = z^{m/n} \tag{2.2}$$

onde $m, n \in \mathbb{Z}^*,\ n \geq 2,\ mdc(m,n) = 1,\ x, y, z \in \mathbb{N}^*$. Neste caso dos expoentes racionais, $x^{\frac{1}{n}} = \sqrt[n]{x}$ denota exclusivamente a raiz n-ésima real positiva do número real x. Na generalização do Capítulo 3 consideraremos todas raízes n-ésimas complexas. No entanto, aqui analisaremos também os casos em que $m = 1$ e $m = 2$.

No lema a seguir caracterizaremos as soluções da equação $x^2 + y^2 = z^2$. Este resultado já é bastante conhecido, mas será usado em diversos momentos neste capítulo.

Lema 2.1. *As soluções inteiras da equação $x^2 + y^2 = z^2$ são $x = r(p^2 - q^2),\ y = 2rpq,\ z = r(p^2 + q^2)$ ou $x = 2rpq,\ y = r(p^2 - q^2),\ z = r(p^2 + q^2)$, onde $p, q, r \in \mathbb{Z},\ mdc(p,q) = 1$ e ainda p e q possuem paridade oposta.*

Demonstração: Vejamos inicialmente que $(r(p^2 - q^2), 2rpq, r(p^2 + q^2))$ é solução de $x^2 + y^2 = z^2$ para todos $p, q, r \in \mathbb{Z}$:

$$\begin{aligned}(r(p^2 - q^2))^2 + (2rpq)^2 &= r^2p^4 - 2r^2p^2q^2 + r^2q^4 + 4r^2p^2q^2 \\ &= r^2p^4 + 2r^2p^2q^2 + r^2q^4 = (r(p^2 + q^2))^2.\end{aligned}$$

Analogamente, $(2rpq, r(p^2-q^2), r(p^2+q^2))$ também é solução de $x^2+y^2=z^2$.

Reciprocamente, sejam (a', b', c') solução de $x^2+y^2=z^2$ e $r = mdc(a', b', c')$. Então, $a' = ra,\ b' = rb,\ c' = rc$. Notemos que $mdc(a, b, c) = 1$ e que (a, b, c) também é solução de $x^2 + y^2 = z^2$, pois:

$$r^2c^2 = (c')^2 = (a')^2 + (b')^2 = r^2a^2 + r^2b^2 = r^2(a^2 + b^2).$$

Podemos observar também que a, b, c são dois a dois primos entre si, pois se um número divide dois deles teria que dividir também o terceiro, que é uma soma ou diferença dos anteriores. Temos agora três possibilidades para a e b:

i) a e b são pares. Neste caso, $mdc(a, b) = 2k$, contradizendo o que já foi feito.

ii) a e b são ímpares. Temos $a = 2i + 1$ e $b = 2j + 1$ para certos $i, j \in \mathbb{Z}$. Então:

$$c^2 = a^2 + b^2 = (2i + 1)^2 + (2j + 1)^2 = 4(i^2 + i + j^2 + j) + 2.$$

Logo, $2|c^2$ e portanto $2|c$. Daí concluímos que $4|c^2$, mas $c^2 - 4(i^2 + i + j^2 + j) = 2$ nos dá $4|2$. Absurdo.

iii) a é ímpar e b é par ou a é par e b é ímpar. Em ambos os casos temos c^2 ímpar e portanto c é ímpar.

Suponhamos, sem perda de generalidade, que a é ímpar e b é par. Assim:

$$b^2 = c^2 - a^2 = (c - a)(c + a)$$

onde $b, c + a, c - a$ são todos pares. Logo, $b = 2u$, $c - a = 2v$ e $c + a = 2w$ para certos $u, v, w \in \mathbb{Z}$, de onde temos $c = v + w$, $a = w - v$ e $4u^2 = (2u)^2 = (2v)(2w) = 4vw$, ou seja, $u^2 = vw$. Como $mdc(a, c) = 1$ e ainda $mdc(v, w)|(v + w) = c$, $mdc(v, w)|(w - v) = a$, temos que $mdc(v, w) = 1$. Então, como $vw = u^2$, concluímos que $w = p^2$ e $v = q^2$ com $mdc(p, q) = 1$. Temos agora $a = p^2 - q^2$, $c = p^2 + q^2$ e $b^2 = 4u^2 = 4vw = 4p^2q^2$, de onde $b = 2pq$. Portanto:

$$(a', b', c') = (r(p^2 - q^2), 2rpq, r(p^2 + q^2)).$$

Falta apenas ver que p e q têm paridade oposta. Suponhamos que p e q são ambos pares, então $mdc(p, q) = 2k$, o que não ocorre, pois $mdc(p, q) = 1$.

Por outro lado, se p e q são ambos ímpares obtemos $a = p^2 - q^2$ e $c = p^2 + q^2$ ambos pares, o que também não ocorre. Logo, nos resta que p e q são um par e o outro ímpar.

Analogamente, se a é par e b é ímpar temos:

$$(a', b', c') = (2rpq, r(p^2 - q^2), r(p^2 + q^2))$$

onde $mdc(p, q) = 1$ e p, q possuem paridade oposta. □

Usando o Lema 2.1 poderemos caracterizar as soluções da Equação 2.1 para $m = 1$ e $m = 2$, conforme as proposições abaixo.

Proposição 2.2. *As soluções inteiras de* $x^{-1} + y^{-1} = z^{-1}$ *são da forma* $x = rp(p+q),\ y = rq(p+q),\ z = rpq$, *onde* $p, q, r \in \mathbb{Z}^*,\ mdc(p, q) = 1,\ p+q \neq 0$.

Demonstração: Vejamos inicialmente que, para $xyz \neq 0$, as equações $x^{-1} + y^{-1} = z^{-1}$ e $(x-y)^2 + (2z)^2 = (x+y-2z)^2$ são equivalentes. De fato, temos:

$$(x - y)^2 + (2z)^2 = x^2 - 2xy + y^2 + 4z^2 \text{ e}$$

$$(x + y - 2z)^2 = x^2 + 2xy - 4xz + y^2 - 4yz + 4z^2.$$

Logo, $x^2 - 2xy + y^2 + 4z^2 = x^2 + 2xy - 4xz + y^2 - 4yz + 4z^2$. Isto implica diretamente que $xy = xz + yz$. Como $xyz \neq 0$, dividindo a equação por xyz obtemos $x^{-1} + y^{-1} = z^{-1}$. A recíproca é análoga.

Temos então $(x-y)^2 + (2z)^2 = (x+y-2z)^2$. Pelo Lema 2.1, temos duas possibilidades. No primeiro caso:

$$x - y = r(p^2 - q^2),\ 2z = 2rpq,\ x + y - 2z = r(p^2 + q^2)$$

de onde obtemos $z = rpq,\ x + y = r(p^2 + q^2) + 2rpq$. Logo, $2x = 2rp(p + q)$, ou seja:

$$x = rp(p + q) \text{ e } y = x - r(p^2 - q^2) = rq(p + q).$$

No segundo caso:

$$x - y = 2rpq,\ 2z = r(p^2 - q^2),\ x + y - 2z = r(p^2 + q^2)$$

de onde $x - y = 2rpq,\ 2z = r(p^2 - q^2),\ x + y - 2z = r(p^2 + q^2)$. Temos então $x + y = 2rp^2$, o que implica:

$$x = rp(p + q),\ y = rp(p - q),\ z = r(p^2 - q^2)/2.$$

Basta então fazermos $p_1 = p + q$, $q_1 = p - q$ e $r_1 = r/2$ para obtermos

$$x = r_1 p_1 (p_1 + q_1),\ y = r_1 q_1 (p_1 + q_1),\ z = r_1 p_1 q_1.$$

□

Proposição 2.3. *As soluções inteiras de* $x^{-2} + y^{-2} = z^{-2}$ *são da forma* $x = \pm r(p^4 - q^4),\ y = \pm 2rpq(p^2 + q^2),\ z = \pm 2rpq(p^2 - q^2)$ *ou* $x = \pm 2rpq(p^2 + q^2),\ y = \pm r(p^4 - q^4),\ z = \pm 2rpq(p^2 - q^2)$ *onde* $p, q, r \in \mathbb{Z}^*,\ |p| \neq |q|,\ mdc(p, q) = 1$ *e* p *e* q *possuem paridade oposta.*

Demonstração: Sejam $x, y, z \in \mathbb{Z}^*$ uma solução de $x^{-2} + y^{-2} = z^{-2}$ e seja $d = mdc(x, y, z)$. Temos então $x = dx_1, y = dy_1, z = dz_1$, com $x_1, y_1, z_1 \in \mathbb{Z}^*$. Podemos ver que ${x_1}^2, {y_1}^2, {z_1}^2$ é solução de $x^{-1} + y^{-1} = z^{-1}$. Logo, pela Proposição 2.2, obtemos que existem $k, l \in \mathbb{Z}$ tais que:

${x_1}^2 = k(k+l),\ {y_1}^2 = l(k+l),\ {z_1}^2 = kl$, onde $k, l \in \mathbb{Z}^*,\ k+l \neq 0$ e $mdc(k, l) = 1$

Mas ${z_1}^2 = kl$ nos dá $k = a^2,\ l = b^2$ com $mdc(a, b) = 1$ e portanto ${x_1}^2 = a^2(a^2 + b^2)$ com $mdc(a^2, a^2 + b^2) = 1$. Disso concluímos que existe $c \in \mathbb{Z}$ tal que $a^2 + b^2 = c^2$. Então, pelo Lema 2.1:

$$a = \pm(p^2 - q^2),\ b = \pm 2pq,\ c = \pm(p^2 + q^2) \text{ ou}$$

$$a = \pm 2pq,\ b = \pm(p^2 - q^2),\ c = \pm(p^2 + q^2)$$

onde $p, q \in \mathbb{Z}^*,\ mdc(p, q) = 1$ e $p + q \neq 0$. Como ${x_1}^2 = k(k + l) = a^2c^2$, ${y_1}^2 = l(k + l) = b^2c^2$ e ${z_1}^2 = lk = a^2b^2$, obtemos finalmente:

$$x = \pm r(p^4 - q^4),\ y = \pm 2rpq(p^2 + q^2),\ z = \pm 2rpq(p^2 - q^2) \text{ ou}$$

$$x = \pm 2rpq(p^2 + q^2),\ y = \pm r(p^4 - q^4),\ z = \pm 2rpq(p^2 - q^2)$$

onde $p, q, r \in \mathbb{Z}^*,\ mdc(p, q) = 1,\ |p| \neq |q|$. □

Provaremos agora um resultado que relaciona as soluções da Equação 2.1 com as soluções de $x^m + y^m = z^m$.

Proposição 2.4. *Seja* $m \in \mathbb{N}^*$. *Então* $x^{-m} + y^{-m} = z^{-m}$ *e* $x^m + y^m = z^m$ *possuem soluções inteiras com* $xyz \neq 0$ *simultaneamente.*

Demonstração: Seja (x_0, y_0, z_0) solução de $x^{-m} + y^{-m} = z^{-m}$ tal que $x_0 y_0 z_0 \neq 0$. Então:

$$\frac{1}{{x_0}^m} + \frac{1}{{y_0}^m} = \frac{1}{{z_0}^m}, \text{ logo, } \frac{{y_0}^m {z_0}^m + {x_0}^m {z_0}^m}{{x_0}^m {y_0}^m {z_0}^m} = \frac{{x_0}^m {y_0}^m}{{x_0}^m {y_0}^m {z_0}^m}.$$

Multiplicando os dois lados da igualdade por ${x_0}^m {y_0}^m {z_0}^m$ obtemos ${y_0}^m {z_0}^m + {x_0}^m {z_0}^m = {x_0}^m {y_0}^m$, ou seja, $(x_1 = y_0 z_0,\ y_1 = x_0 z_0,\ z_1 = x_0 y_0)$ é solução de $x^m + y^m = z^m$. A recíproca é análoga. □

O seguinte teorema decorre diretamente desta proposição e do Teorema 0.1:

Teorema 2.5. *Seja $m \in \mathbb{N}^*$, $m > 2$. Então $x^{-m} + y^{-m} = z^{-m}$ não tem solução inteira.*

Passaremos agora à caracterização das soluções da Equação 2.2. Para isto, precisaremos do seguinte resultado:

Lema 2.6. (Critério de Cappeli) *Seja $a \in \mathbb{Q},\ a > 0$. Então vale exatamente uma das afirmações:*

i) $x^n - a$ é irredutível em $\mathbb{Q}[x]$.

ii) Existem $b \in \mathbb{Q},\ b > 0$ e $k \in \mathbb{N},\ k > 1$ tais que $k|n$ e $a = b^k$.

Demonstração: Suponhamos que $x^n - a$ é redutível sobre $\mathbb{Q}[x]$. Temos em $\mathbb{C}[x]$:

$$p(x) = (x^n - a) = \prod_{i=0}^{n-1} (x - \omega^i \alpha)$$

onde ω é uma raiz n-ésima primitiva da unidade e $\alpha = \sqrt[n]{a}$. Seja $q(x) \in \mathbb{Q}[x]$ um fator de $p(x)$ tal que $1 \leq \partial q \leq n - 1$. Como q divide p, sabemos que:

$$q(x) = \prod_{j=1}^{m} (x - \omega^{i_j} \alpha) = x^m + ... + (-1)^m \omega^l \alpha^m$$

onde todos coeficientes de q estão em $\mathbb{Q}$. Em particular, $\omega^l \alpha^m \in \mathbb{Q} \subset \mathbb{R}$, de onde $\omega^l \in \mathbb{R}$. Mas isto ocorre se e somente se $\omega^l = \pm 1$, o que nos dá $\alpha^m \in \mathbb{Q}$. Seja $d = mdc(m, n)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = rm + sn$ e portanto:

$$\alpha^d = \alpha^{rm+sn} = (\alpha^m)^r \cdot (\alpha^n)^s = a^s \cdot (\alpha^m)^r \in \mathbb{Q}.$$

Tomando $b = \alpha^d$ e $k = \frac{n}{d}$ temos $k > 1$ pois d divide m e $m < n$. Obtemos então:

$$b^k = (\alpha^d)^k = \alpha^{dk} = \alpha^n = a$$

com $b \in \mathbb{Q}$, $b > 0$, $k \in \mathbb{N}$, $k > 1$ e ainda $k|n$.

Reciprocamente, suponhamos que $a = b^k$ com $b \in \mathbb{Q}$, $b > 0$, $k \in \mathbb{N}$, $k > 1$ e $n = kd$. Neste caso temos:

$$p(x) = x^n - a = x^{kd} - b^k = (x^d)^k - b^k = (x^d - b) \cdot f(x)$$

com $f(x) \in \mathbb{Q}[x]$ e portanto $x^n - a$ é redutível sobre $\mathbb{Q}[x]$. □

As próximas duas proposições também são resultados que serão usados para caracterizar as soluções da Equação 2.2.

Proposição 2.7. *Sejam* $a, b \in \mathbb{Q},\ a > 0,\ b > 0,\ n \in \mathbb{N}^*$. *Se* $s = a^{1/n} + b^{1/n} \in \mathbb{Q}$, *então* $a^{1/n}, b^{1/n} \in \mathbb{Q}$.

Demonstração: Provaremos o resultado por indução em n. Para $n = 1$ é trivial que $a^1, b^1 \in \mathbb{Q}$, pois por hipótese $a, b \in \mathbb{Q}$. Suponhamos agora que o resultado vale para $1 \leq k \leq n-1,\ k \in \mathbb{N}$, e vejamos que vale para $k = n$. Temos:

$$a = (s - b^{1/n})^n = \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} s^{n-i} b^{i/n} + s^n + (-1)^n b.$$

Logo, $b^{1/n}$ é raiz do seguinte polinômio não-nulo de grau $n-1$ $p(x) = s^n + (-1)^n b - a + \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} s^{n-i} x^i$. Seja $q(x)$ o polinômio mínimo de $b^{1/n}$. Sabemos que o grau de $q(x)$ é menor ou igual a $n-1$. Como $b^{1/n}$ é raiz de $x^n - b$, então $q(x)|x^n - b$ e portanto $x^n - b$ é redutível. Analogamente temos que $x^n - a$ é redutível. Usando o Lema 2.6 temos que existem $n_1, m_1 \in \mathbb{N},\ n_1, m_1 > 1$ e $a_1, b_1 \in \mathbb{Q},\ a_1, b_1 > 0$ tais que $n_1|n,\ m_1|n,\ a = {a_1}^{n_1}$ e $b = {b_1}^{m_1}$. Então $n = n_1 n_2 = m_1 m_2$. Suponhamos que n_1, m_1 são maximais com as propriedades acima. Temos três casos:

i) Se $n = n_1 = m_1$, então $a = {a_1}^n,\ b = {b_1}^n$, ou seja, $a^{1/n} = a_1, b^{1/n} = b_1 \in \mathbb{Q}$.

ii) Se $n_1 = m_1 < n$, então $n_2 = m_2 = m$ com $1 \leq m < n$. Como $a^{1/n} + b^{1/n} = {a_1}^{1/m} + {b_1}^{1/m} \in \mathbb{Q}$, pela hipótese de indução temos ${a_1}^{1/m} = a^{1/n}, {b_1}^{1/m} = b^{1/n} \in \mathbb{Q}$.

iii) Se $n_1 \neq m_1$, suponhamos $n_1 > m_1$. Notemos que ${b_1}^{1/m_2}$ é raiz de $p_1(x) = x^{m_2} - b_1$ e de $p_2(x) = (s-x)^{n_2} - a_1$. De fato,

$$s = a^{\frac{1}{n}} + b^{\frac{1}{n}} = a^{\frac{1}{n_1 n_2}} + b^{\frac{1}{m_1 m_2}} = (a^{\frac{1}{n_1}})^{\frac{1}{n_2}} + (b^{\frac{1}{m_1}})^{\frac{1}{m_2}} = {a_1}^{\frac{1}{n_2}} + {b_1}^{\frac{1}{m_2}}.$$

Então, $s - {b_1}^{1/m_2} = {a_1}^{1/n_2}$ e portanto $(s - {b_1}^{1/m_2})^{n_2} - a_1 = 0$. Como $n_2 < m_2$, temos que $x^{m_2} - b_1$ é redutível. Logo, pelo Lema 2.6, existem $b_2 \in \mathbb{Q},\ b_2 > 0$ e $m_3 \in \mathbb{N},\ m_3 > 1$ tais que $m_3 | m_2$ e $b_1 = {b_2}^{m_3}$, ou seja, $b = {b_2}^{m_1 m_3}$ com $m_1 m_3 | n,\ m_1 m_3 > 1$ e $m_1 m_3 > m_1$. Absurdo, pois m_1 é maximal.

□

Proposição 2.8. *Se $x, y, z \in \mathbb{N}^*,\ m \in \mathbb{Z}^*,\ n \in \mathbb{N}^*,\ mdc(m,n) = 1$ e $x^{m/n} + y^{m/n} = z^{m/n}$, então existem $d, x_1, y_1, z_1 \in \mathbb{N}^*$ tais que $x = d{x_1}^n, y = d{y_1}^n, z = d{z_1}^n$.*

Demonstração: Seja $d = mdc(x, y, z)$. Então $x = dx_2, y = dy_2, z = dz_2$, com $mdc(x_2, y_2, z_2) = 1$. Temos três casos:

i) Se $m = 1$, temos ${x_2}^{1/n} + {y_2}^{1/n} = {z_2}^{1/n}$, ou seja:

$$\left(\frac{x_2}{z_2}\right)^{1/n} + \left(\frac{y_2}{z_2}\right)^{1/n} = 1.$$

Logo, pela Proposição 2.7, $\left(\frac{x_2}{z_2}\right)^{1/n}$ e $\left(\frac{y_2}{z_2}\right)^{1/n} \in \mathbb{Q}$. Neste caso existem $p, q, r, s \in \mathbb{N}^*$ com $mdc(p,q) = 1$ e $mdc(r,s) = 1$ tais que:

$$\frac{x_2}{z_2} = \frac{p^n}{q^n}, \quad \frac{y_2}{z_2} = \frac{r^n}{s^n}.$$

Então, $x_2 q^n = z_2 p^n$ e $y_2 s^n = z_2 r^n$. Seja $z_1 = max\{r \in \mathbb{N}^* : r^n | z_2\}$. Podemos ver que $q \leq z_1 \leq z_2$. Como ${z_1}^n | z_2$, então existe $k \in \mathbb{N}^*$ tal que $z_2 = k{z_1}^n$. Portanto:

$$x_2 q^n = k{z_1}^n p^n,\ y_2 s^n = k{z_1}^n r^n \text{ onde } q^n | k{z_1}^n \text{ e } s^n | k{z_1}^n.$$

Vejamos que $q|z_1$ e $s|z_1$. Suponhamos por absurdo que $q \nmid z_1$. Então $q > 1$ e $q^n|k$ e portanto $z_2 = k'q^n {z_1}^n$. Daí, $(qz_1)^n|z_2$ e $qz_1 > z_1$, contradizendo a definição de z_1. Logo, $q|z_1$ e, analogamente, $s|z_1$. Então:

$$x_2 = k\left(\frac{z_1}{q}p\right)^n,\ y_2 = k\left(\frac{z_1}{s}r\right)^n,\ z_2 = k{z_1}^n$$

onde $x_1 = \frac{z_1}{q}p,\ y_1 = \frac{z_1}{s}r \in \mathbb{N}^*$. Mas $mdc(x_2, y_2, z_2) = 1$, então $k = 1$ e:

$$x = dx_2 = d{x_1}^n,\ y = dy_2 = d{y_1}^n,\ z = dz_2 = d{z_1}^n.$$

ii) Se $m > 1$, temos ${x_2}^{m/n} + {y_2}^{m/n} = {z_2}^{m/n}$, ou seja:

$$\left(\left(\frac{x_2}{z_2}\right)^m\right)^{1/n} + \left(\left(\frac{y_2}{z_2}\right)^m\right)^{1/n} = 1.$$

Logo, pela Proposição 2.7, $\left(\frac{x_2}{z_2}\right)^{m/n}$ e $\left(\frac{y_2}{z_2}\right)^{m/n} \in \mathbb{Q}$. Então, usando ${x_2}^m, {y_2}^m, {z_2}^m$ no lugar de x_2, y_2, z_2 e procedendo analogamente ao caso anterior obtemos:

$${x_2}^m = {x_3}^n,\ {y_2}^m = {y_3}^n,\ {z_2}^m = {z_3}^n$$

onde $x_3, y_3, z_3 \in \mathbb{N}^*$. Como $mdc(m, n) = 1$, então todo primo que aparece na fatoração de ${x_2}^m$ possui expoente divisível por mn. Logo, existe $x_1 \in \mathbb{N}^*$ tal que ${x_2}^m = {x_1}^{mn}$, ou seja, $x_2 = {x_1}^n$. Analogamente, $y_2 = {y_1}^n$ e $z_2 = {z_1}^n$, de onde segue o resultado.

iii) Se $m < 0$, temos ${x_2}^{m/n} + {y_2}^{m/n} = {z_2}^{m/n}$, ou seja:

$$\left(\left(\frac{x_2}{z_2}\right)^m\right)^{1/n} + \left(\left(\frac{y_2}{z_2}\right)^m\right)^{1/n} = 1.$$

Logo, pela Proposição 2.7, $\left(\frac{z_2}{x_2}\right)^{-m/n}$ e $\left(\frac{z_2}{y_2}\right)^{-m/n} \in \mathbb{Q}$. Procedendo analogamente ao caso anterior obtemos o resultado desejado.

□

Agora estamos prontos para a caracterização das soluções da Equação 2.2 para os casos $m = \pm 1$, $m = \pm 2$.

Proposição 2.9. *As soluções inteiras positivas de* $x^{1/n} + y^{1/n} = z^{1/n}$ *são da forma* $x = rp^n,\ y = rq^n,\ z = r(p+q)^n$, *com* $r, p, q \in \mathbb{N}^*$ *e* $mdc(p,q) = 1$.

Demonstração: Da Proposição 2.8 temos:

$$x = rp^n,\ y = rq^n,\ z = rs^n$$

com $p, q, r, s \in \mathbb{N}^*$ e $mdc(p,q,s) = 1$. Logo:

$$(rp^n)^{1/n} + (rq^n)^{1/n} = (rs^n)^{1/n}.$$

Daí temos diretamente que $s = p + q$, e portanto $z = r(p+q)^n$. □

Proposição 2.10. *Se* n *é ímpar, então as soluções inteiras de* $x^{2/n} + y^{2/n} = z^{2/n}$ *são da forma* $x = \pm r(p^2 - q^2)^n,\ y = \pm 2^n rp^n q^n,\ z = \pm r(p^2 + q^2)^n$ *ou* $x = \pm 2^n rp^n q^n,\ y = \pm r(p^2 - q^2)^n,\ z = \pm r(p^2 + q^2)^n$, *onde* $p, q, r \in \mathbb{Z},\ mdc(p,q) = 1$ *e* p *e* q *possuem paridade oposta.*

Demonstração: Da Proposição 2.8 temos $x = \pm r{x_1}^n,\ y = \pm r{y_1}^n,\ z = \pm r{z_1}^n$. Notemos que x_1, y_1, z_1 é solução de $x^2 + y^2 = z^2$. De fato:

$$(r{x_1}^n)^{2/n} + (r{y_1}^n)^{2/n} = r^{2/n} \cdot {x_1}^2 + r^{2/n} \cdot {y_1}^2 = r^{2/n}({x_1}^2 + {y_1}^2).$$

$$(r{z_1}^n)^{2/n} = r^{2/n} \cdot {z_1}^2.$$

Logo, ${x_1}^2 + {y_1}^2 = {z_1}^2$ e pelo Lema 2.1:

$$x_1 = (p^2 - q^2),\ y_1 = 2pq,\ z_1 = (p^2 + q^2) \text{ ou}$$

$$x_1 = 2pq,\ y_1 = (p^2 - q^2),\ z_1 = (p^2 + q^2)$$

onde $p, q \in \mathbb{Z},\ mdc(p,q) = 1$ e ainda p e q possuem paridade oposta. Então:

$$x = \pm r{x_1}^n = \pm r(p^2 - q^2)^n \text{ ou } x = \pm r{x_1}^n = \pm 2^n p^n q^n$$

$$y = \pm r{y_1}^n = \pm 2^n p^n q^n \text{ ou } y = \pm r{y_1}^n = \pm r(p^2 - q^2)^n$$

$$z = \pm r{z_1}^n = \pm (p^2 + q^2)^n$$

onde $p, q, r \in \mathbb{Z},\ mdc(p,q) = 1$ e p e q possuem paridade oposta. □

Proposição 2.11. *As soluções inteiras positivas não-nulas de* $x^{-1/n}+y^{-1/n} = z^{-1/n}$ *são da forma* $x = rp^n(p+q)^n,\ y = rq^n(p+q)^n,\ z = rp^nq^n$, *onde* $p, q, r \in \mathbb{N}^*$ *e* $mdc(p,q) = 1$.

Demonstração: Da Proposição 2.8 temos $x = r{x_1}^n,\ y = r{y_1}^n,\ z = r{z_1}^n$. Como x_1, y_1, z_1 é solução de $x^{-1} + y^{-1} = z^{-1}$, pela Proposição 2.2 temos:

$$x_1 = p(p+q),\ y_1 = q(p+q),\ z_1 = pq$$

onde $p, q \in \mathbb{Z}^*,\ mdc(p,q) = 1,\ p+q \neq 0$ e ainda p e q possuem paridade oposta. Então:

$$x = rp^n(p+q)^n,\ y = rq^n(p+q)^n,\ z = rp^nq^n$$

onde $p, q, r \in \mathbb{N}^*$ e $mdc(p,q) = 1$. □

Proposição 2.12. *As soluções inteiras não-nulas de* $x^{-2/n} + y^{-2/n} = z^{-2/n}$ *são da forma* $x = \pm r(p^4-q^4)^n,\ y = \pm 2^n rp^nq^n(p^2+q^2)^n,\ z = \pm 2^n rp^nq^n(p^2-q^2)^n$ *ou* $x = \pm 2^n rp^nq^n(p^2+q^2)^n,\ y = \pm r(p^4-q^4)^n,\ z = \pm 2^n rp^nq^n(p^2-q^2)^n$, *onde* $p, q, r \in \mathbb{Z}^*,\ |p| \neq |q|,\ mdc(p,q) = 1$ *e* p *e* q *possuem paridade oposta.*

Demonstração: Analogamente, da Proposição 2.8 temos $x = \pm r{x_1}^n,\ y = \pm r{y_1}^n,\ z = \pm r{z_1}^n$. Como x_1, y_1, z_1 é solução de $x^{-2} + y^{-2} = z^{-2}$, pela Proposição 2.3 temos:

$$x_1 = \pm(p^4-q^4),\ y_1 = \pm 2pq(p^2+q^2),\ z_1 = \pm 2pq(p^2-q^2) \text{ ou}$$

$$x_1 = \pm 2pq(p^2+q^2),\ y_1 = \pm(p^4-q^4),\ z_1 = \pm 2pq(p^2-q^2)$$

onde $p, q \in \mathbb{Z}^*,\ |p| \neq |q|,\ mdc(p,q) = 1$ e p e q possuem paridade oposta. Então:

$$x = \pm r(p^4-q^4)^n,\ y = \pm 2^n rp^nq^n(p^2+q^2)^n,\ z = \pm 2^n rp^nq^n(p^2-q^2)^n \text{ ou}$$

$$x = \pm 2^n rp^nq^n(p^2+q^2)^n,\ y = \pm r(p^4-q^4)^n,\ z = \pm 2^n rp^nq^n(p^2-q^2)^n.$$

□

Analogamente ao caso dos expoentes negativos, também podemos relacionar as soluções da Equação 2.2 com as soluções da equação $x^{|m|} + y^{|m|} = z^{|m|}$, conforme descreve a proposição abaixo:

Proposição 2.13. *Seja $m \in \mathbb{Z}^*$. Então as equações $x^{m/n} + y^{m/n} = z^{m/n}$ e $x^{|m|} + y^{|m|} = z^{|m|}$ possuem solução inteiras positivas não-nulas simultaneamente.*

Demonstração: Seja (x_0, y_0, z_0) solução de $x^{m/n} + y^{m/n} = z^{m/n}$. Então, pela Proposição 2.8, temos:

$$x_0 = d{x_1}^n,\ y_0 = d{y_1}^n,\ z_0 = d{z_1}^n.$$

Se $m > 0$, então (x_1, y_1, z_1) é solução de $x^{|m|} + y^{|m|} = z^{|m|}$. Se $m < 0$, então (x_1, y_1, z_1) é solução de $x^m + y^m = z^m$. Mas, pela Proposição 2.4, existe (x_2, y_2, z_2) solução de $x^{-m}+y^{-m} = z^{-m}$, ou seja, solução de $x^{|m|}+y^{|m|} = z^{|m|}$.

Reciprocamente, seja (x_1, y_1, z_1) solução de $x^{|m|} + y^{|m|} = z^{|m|}$. Se $m > 0$, então $(x_1 = x_2, y_1 = y_2, z_1 = z_2)$ é solução de $x^m + y^m = z^m$. Se $m < 0$, então (x_1, y_1, z_1) é solução de $x^{-m} + y^{-m} = z^{-m}$. Então, pela Proposição 2.4, existe (x_2, y_2, z_2) solução de $x^m + y^m = z^m$. Sejam:

$$x_0 = {x_2}^n,\ y_0 = {y_2}^n,\ z_0 = {z_2}^n.$$

Temos que (x_0, y_0, z_0) é solução de $x^{m/n} + y^{m/n} = z^{m/n}$. □

Este resultado garante, juntamente com o Teorema 0.1, que os casos analisados anteriormente ($m = \pm 1,\ m = \pm 2$) são os únicos em que a Equação 2.2 possui solução inteira, conforme afirma o resultado abaixo:

Teorema 2.14. *Sejam $m, n \in \mathbb{Z}^*$ com $n \geq 2$ tais que $mdc(m, n) = 1$. Então $x^{m/n} + y^{m/n} = z^{m/n}$ não tem solução inteira com $xyz \neq 0$ se $m \neq \pm 1, \pm 2$.*

Capítulo 3

O Caso Complexo

Neste capítulo vamos mostrar a segunda generalização desejada do Último Teorema de Fermat, dada pelo teorema a seguir:

Teorema 3.1. *Sejam m e n números inteiros positivos primos entre si com $m > 2$. Então a equação $x^m + y^m = z^m$ possui uma solução complexa (a, b, c) com $a^n, b^n, c^n \in \mathbb{Z}$ se e somente se n é divisível por 6. Neste caso, $a^n = b^n = c^n$.*

Vale ressaltar que na prova deste teorema trabalharemos com raízes n-ésimas dentro do conjunto dos números complexos. No Capítulo 2 foi apresentada uma versão deste resultado que, restringindo as raízes n-ésimas àquelas que estão dentro do conjunto dos números reais, trabalha também com os casos em que $m = 1$ e $m = 2$.

Observação 3.2. Cometendo um abuso de notação e fazendo $a_1 = a^n$, $b_1 = b^n$, $c_1 = c^n$ temos que (a_1, b_1, c_1) é solução de $x^{m/n} + y^{m/n} = z^{m/n}$, ou seja, podemos pensar no Teorema 3.1 como uma generalização para expoentes racionais do Último Teorema de Fermat (que se obtém tomando $n = 1$).

Observação 3.3. Notemos que a equação $x^m + y^m = z^m$ sempre possui solução complexa, pois $\mathbb{C}$ é algebricamente fechado. No entanto, com o Teorema 3.1 estamos garantindo a existência de uma solução muito especial.

3.1 Exemplos

Antes de provar o Teorema 3.1 mostraremos alguns exemplos para ilustrar o resultado.

Exemplo 3.4. Consideremos $m = 5$ e $n = 6$ e vejamos que $(e^{\pi i/3}, e^{-\pi i/3}, 1)$ é uma solução de $x^5 + y^5 = z^5$ tal que $(e^{\pi i/3})^6,\ (e^{-\pi i/3})^6,\ 1^6 \in \mathbb{Z}$. De fato:

$$\begin{aligned}(e^{\pi i/3})^5 + (e^{-\pi i/3})^5 &= e^{5\pi i/3} + e^{-5\pi i/3} = e^{-\pi i/3} + e^{\pi i/3} \\ &= (\cos -\pi/3 + i \operatorname{sen} -\pi/3) + (\cos \pi/3 + i \operatorname{sen} \pi/3) \\ &= 2\cos \pi/3 = 2(1/2) = 1 = 1^5.\end{aligned}$$

Exemplo 3.5. Ainda para $m = 5$ e $n = 6$, consideremos $z \in \mathbb{Z}$. Seja $\sqrt[6]{|z|}$ a raiz sexta real de $|z|$. Temos $z = \varepsilon|z|$, com $\varepsilon = 1$ ou $\varepsilon = -1$. Tome $a = \varepsilon\sqrt[6]{|z|}e^{\pi i/3}$, $b = \varepsilon\sqrt[6]{|z|}e^{-\pi i/3}$ e $c = \varepsilon\sqrt[6]{|z|}\cdot 1$. Neste caso, $a^6 = b^6 = c^6 = |z|$ são números inteiros e ainda usando o exemplo anterior temos:

$$\begin{aligned}a^5 + b^5 &= (\varepsilon\sqrt[6]{|z|}e^{\pi i/3})^5 + (\varepsilon\sqrt[6]{|z|}e^{-\pi i/3})^5 \\ &= \varepsilon(\sqrt[6]{|z|})^5 \left((e^{\pi i/3})^5 + (e^{-\pi i/3})^5\right) = \varepsilon(\sqrt[6]{|z|})^5 \cdot 1^5 = c^5.\end{aligned}$$

Exemplo 3.6. Considerando $m = 7$ e $n = 12$ e também vejamos que $(e^{\pi i/3}, e^{-\pi i/3}, 1)$ é uma solução de $x^7 + y^7 = z^7$ tal que $(e^{\pi i/3})^{12},\ (e^{-\pi i/3})^{12},\ 1^{12} \in \mathbb{Z}$. De fato:

$$\begin{aligned}(e^{\pi i/3})^7 + (e^{-\pi i/3})^7 &= e^{7\pi i/3} + e^{-7\pi i/3} = e^{-\pi i/3} + e^{\pi i/3} \\ &= (\cos -\pi/3 + i \operatorname{sen} -\pi/3) + (\cos \pi/3 + i \operatorname{sen} \pi/3) \\ &= 2\cos \pi/3 = 2(1/2) = 1 = 1^7.\end{aligned}$$

Logo, analogamente ao exemplo anterior, $\left(\varepsilon\sqrt[12]{|z|}e^{\pi i/3}, \varepsilon\sqrt[12]{|z|}e^{-\pi i/3}, \varepsilon\sqrt[12]{|z|}\right)$ é solução de $x^7 + y^7 = z^7$ tal que $a^{12} = b^{12} = c^{12} = |z|$ para todo $z \in \mathbb{Z}$.

3.2 O Caso das Raízes Reais

Esta seção tem como objetivo desenvolver alguns resultados que nos levarão a prova do teorema no caso em que tomamos raízes n-ésimas reais.

Fixado um inteiro positivo n, chamaremos de T_n o conjunto dado por

$$T_n = \{z \in \mathbb{C} / z^n \in \mathbb{Q}, z^n > 0\}$$

e de $T_{n,\mathbb{R}}$ a intersecção de T_n com o conjunto dos números reais.

Lema 3.7. *Seja $\alpha \in \mathbb{C}$. Se α^m é um elemento de $\mathbb{Q}$ e $|\alpha^k|$ não é um elemento de $\mathbb{Q}$ para $k < m$, então $x^m - \alpha^m$ é o polinômio mínimo de α sobre $\mathbb{Q}$.*

Demonstração: Seja γ uma raiz m-ésima primitiva da unidade. Temos:

$$x^m - \alpha^m = \prod_{j=1}^{m} (x - \gamma^j \alpha).$$

Pela Proposição 1.11, o polinômio mínimo de α sobre $\mathbb{Q}$, $p_\alpha(x) = x^r + b_{r-1}x^{r-1} + ... + b_0$, divide $x^m - \alpha^m$, o que nos dá $m \geq r$. Como $\mathbb{C}[x]$ é um domínio de fatoração única, sabemos que b_0 é o produto de r raízes de $x^m - \alpha^m$ e portanto $b_0 = \gamma^s \alpha^r$ para algum inteiro s. Mas b_0 é racional e $|b_0| = |\alpha^r|$, então $r \geq m$, pois por hipótese $|\alpha^k| \notin \mathbb{Q}$ para $k < m$. Logo, $r = m$ e $p_\alpha(x) = x^m - \alpha^m$. □

Usando o Lema 3.7 obtemos:

Proposição 3.8. *Seja n um inteiro positivo. Se $a, b \in T_{n,\mathbb{R}}$ são tais que $a + b = 1$, então $a, b \in \mathbb{Q}$.*

Demonstração: Seja k o menor inteiro positivo tal que $|a^k| = \pm a^k \in \mathbb{Q}$. Pelo Lema 3.7, $p_a(x) = x^k - a^k$. Notemos que $a = 1 - b$ também é raiz de $(1-x)^k - b^k$ e daí $x^k - a^k$ divide $(1-x)^k - b^k$. Como estes polinômios têm o mesmo grau, então eles diferem apenas por uma constante multiplicada. Assim:

$$\begin{aligned}(1-x)^k - b^k &= 1 + c_1 x + ... + c_{k-1}x^{k-1} + c_k x^k - b^k \\ &= c(x^k - a^k) = cx^k - ca^k.\end{aligned}$$

Mas c_j são os coeficientes do binômio de Newton no desenvolvimento de $(1-x)^k$, e portanto $c_j \neq 0$ para todo $j = 1, ..., k$. Temos então, de um lado da igualdade um polinômio com termos de grau $0, 1, 2, ..., k$ e de outro lado um polinômio com apenas termos de grau 0 e k. Logo, $k = 1$ e $a \in \mathbb{Q}$. Como $b = 1 - a$, temos também que $b \in \mathbb{Q}$. □

Chegamos agora ao resultado que resolve o caso real.

Proposição 3.9. *Sejam m e n inteiros positivos tais que $mdc(m,n) = 1$ e $m > 2$. Então $x^m + y^m = 1$ não possui soluções em $T_{n,\mathbb{R}}$.*

Demonstração: Por absurdo, suponhamos que existam $a, b \in T_{n,\mathbb{R}}$ tais que $a^m + b^m = 1$. Como $(a^m)^n = (a^n)^m$ e $(b^m)^n = (b^n)^m \in \mathbb{Q}$, pela Proposição 3.8 temos $a^m, b^m \in \mathbb{Q}$. Mas $a, b \in T_{n,\mathbb{R}}$ nos dá $a^n, b^n \in \mathbb{Q}$. Logo, $a^{mdc(m,n)} = a \in \mathbb{Q}$ e $b^{mdc(m,n)} = b \in \mathbb{Q}$. Obtemos então, $a = \dfrac{t}{u},\ b = \dfrac{z}{w}$, com $t, u, z, w \in \mathbb{Z}$, e portanto:

$$1 = a^m + b^m = \frac{t^m}{u^m} + \frac{z^m}{w^m} = \frac{t^m w^m + z^m u^m}{u^m w^m} = \frac{(tw)^m + (zu)^m}{(uw)^m}.$$

Mas daí obtemos diretamente que $(uw)^m = (tw)^m + (zu)^m$, o que é absurdo pelo Teorema 0.1. □

3.3 Alguns Lemas Importantes

Esta seção tem como objetivo provar alguns lemas que serão usados para mostrar o teorema desejado.

Lema 3.10. *Sejam m e n dois inteiros positivos e seja a um número real em $K = \mathbb{Q}(e^{2\pi i/n})$ tal que a^m é racional. Então a^2 também é racional.*

Demonstração: Sejam m e n inteiros positivos e seja $a \in K$ tal que a^m é racional. Pela Proposição 1.55, sabemos que o grupo de Galois de $K : \mathbb{Q}$ é abeliano. Logo, todo subgrupo é normal. Em particular, se $F = K \cap \mathbb{R}$ temos $\Gamma(K : F) \lhd \Gamma(K : \mathbb{Q})$. Temos então, pelo Teorema 1.54, que F é o corpo de decomposição para algum polinômio em $\mathbb{Q}[x]$. Seja k o menor inteiro positivo tal que $a^k \in \mathbb{Q}$. Pelo Lema 3.7 temos que o polinômio mínimo de a em $\mathbb{Q}[x]$ é $x^k - a^k$ e portanto este polinômio é irredutível sobre $\mathbb{Q}$. Como $a \in F$, pela Proposição 1.32 todas as raízes de $x^k - a^k$ pertencem a F e logo são reais. Mas sabemos que as raízes deste polinômio são da forma $\gamma^j a$, onde γ é uma raiz k-ésima primitiva da unidade. Logo, para que estas raízes sejam todas reais precisamos ter $k \leq 2$ e portanto $a^2 \in \mathbb{Q}$. □

Lema 3.11. *Se n é um inteiro positivo e α é um número real, então* $2\cos(n\alpha) = \sum_{j=0}^{n} a_j(2\cos\alpha)^j$, *com* $a_n = 1$ *e* $a_j \in \mathbb{Z}$.

Demonstração: Primeiramente notemos que:

$$\cos(n\alpha) = \cos((n-1)\alpha + \alpha) = \cos((n-1)\alpha)\cos\alpha - \operatorname{sen}((n-1)\alpha)\operatorname{sen}\alpha,$$

$$\cos((n-2)\alpha) = \cos((n-1)\alpha - \alpha) = \cos((n-1)\alpha)\cos\alpha + \operatorname{sen}((n-1)\alpha)\operatorname{sen}\alpha.$$

Logo, somando as duas equações obtemos:

$$\cos(n\alpha) + \cos((n-2)\alpha) = 2\cos((n-1)\alpha)\cos\alpha.$$

$$\cos(n\alpha) = 2\cos((n-1)\alpha)\cos\alpha - \cos((n-2)\alpha).$$

Agora provaremos o resultado por indução. Para $n = 1$ temos claramente $2\cos(\alpha) = \sum_{j=0}^{1} a_j(2\cos\alpha)^j$, com $a_1 = 1$ e $a_0 = 0$. Suponhamos que o resultado vale até $n-1$ e vejamos que vale para n.

$$2\cos(n\alpha) = 2\cos((n-1)\alpha)2\cos\alpha - 2\cos((n-2)\alpha). \tag{3.1}$$

Mas, pela hipótese de indução, existem $b_i, c_j \in \mathbb{Z}$ com $b_{n-1} = c_{n-2} = 1$ tais que:

$$2\cos((n-1)\alpha) = \sum_{j=0}^{n-1} b_j(2\cos\alpha)^j$$

e

$$2\cos((n-2)\alpha) = \sum_{j=0}^{n-2} c_j(2\cos\alpha)^j.$$

Assim, substituindo as equações anteriores em 3.1, obtemos:

$$\begin{aligned} 2\cos(n\alpha) &= \sum_{j=0}^{n-1} b_j(2\cos\alpha)^j.2\cos\alpha - \sum_{j=0}^{n-2} c_j(2\cos\alpha)^j \\ &= \sum_{j=0}^{n-1} b_j(2\cos\alpha)^{j+1} - \sum_{j=0}^{n-2} c_j(2\cos\alpha)^j \\ &= \sum_{j=1}^{n-1} (b_{j-1} - c_j)(2\cos\alpha)^j + c_0 + b_{n-1}(2\cos\alpha)^n. \end{aligned}$$

Finalmente, tomando $a_0 = c_0$, $a_i = b_{i-1} - c_i$ para $1 \leq i \leq n-1$ e $a_n = b_{n-1}$, temos o resultado. □

Lema 3.12. *Sejam k, n inteiros positivos. Se temos $\cos(2k\pi/n) \in \mathbb{Q}$, então $2\cos(2k\pi/n) \in \mathbb{Z}$.*

Demonstração: Seja $\alpha = 2k\pi/n$. Pelo Lema 3.11, existem $a_j \in \mathbb{Z}$ para $0 \leq j \leq n-1$ e $a_n = 1$ tais que:

$$2 = 2\cos(2k\pi) = 2\cos(n\alpha) = \sum_{j=0}^{n} a_j (2\cos\alpha)^j.$$

Então:

$$\sum_{j=0}^{n} a_j (2\cos\alpha)^j - 2 = 0.$$

Logo, $2\cos\alpha$ é raiz de um polinômio mônico em $\mathbb{Z}[x]$. Temos daí que, se $2\cos\alpha = p/q \in \mathbb{Q}$, então q divide 1 e portanto $2\cos\alpha \in \mathbb{Z}$. □

3.4 O Teorema Principal

Nesta seção finalmente provaremos o Teorema 3.1 utilizando os resultados provados anteriormente. Para isto começaremos com duas proposições importantes.

Proposição 3.13. *Sejam n um inteiro positivo e $x_1, x_2 \in T_n = \{z \in \mathbb{C}/z^n \in \mathbb{Q}, z^n > 0\}$ tais que $x_1 + x_2 = 1$. Então $x_1, x_2 \in \mathbb{Q}$ ou $x_1 = a_1 e^{\pm i\theta_1}$ e $x_2 = a_2 e^{\pm i\theta_2}$, onde $a_1, a_2, \theta_1, \theta_2$ pertencem à tabela a seguir:*

θ_1	θ_2	a_1	a_2
$2\pi/3$	$\pi/6$	1	$\sqrt{3}$
$\pi/6$	$\pi/6$	$1/\sqrt{3}$	$1/\sqrt{3}$
$\pi/2$	$\pi/4$	1	$\sqrt{2}$
$\pi/4$	$\pi/4$	$1/\sqrt{2}$	$1/\sqrt{2}$
$\pi/2$	$\pi/3$	$\sqrt{3}$	2
$\pi/2$	$\pi/6$	$1/\sqrt{3}$	$2/\sqrt{3}$
$\pi/3$	$\pi/6$	$1/2$	$\sqrt{3}/2$
$\pi/3$	$\pi/3$	1	1

Demonstração: Se $x_1, x_2 \in \mathbb{R}$, então, pela Proposição 3.8, $x_1, x_2 \in \mathbb{Q}$. Se $x_1 \notin \mathbb{R}$, então $x_2 = 1 - x_1 \notin \mathbb{R}$. Logo:

$$x_1 = a_1 e^{i\psi_1}, \quad x_2 = a_2 e^{i\psi_2}$$

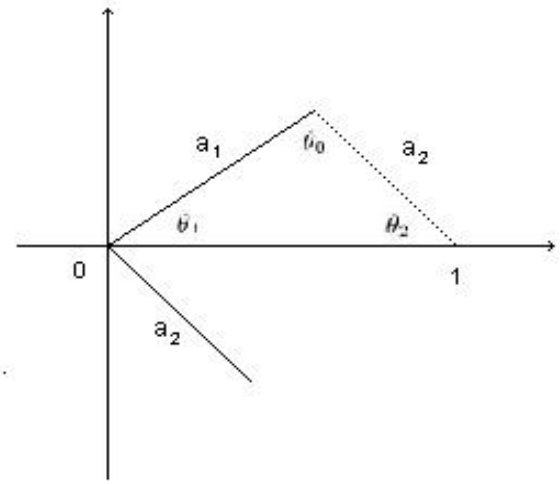
com $a_1, a_2 \in \mathbb{R}_+$ e $-\pi < \psi_1, \psi_2 < \pi$. Como a parte imaginária de $x_1 + x_2$ é igual a zero, temos que $\operatorname{sen}\psi_1$ e $\operatorname{sen}\psi_2$ têm sinais opostos. Podemos então assumir que $0 < \psi_1 < \pi$ e $-\pi < \psi_2 < 0$. Fazendo $\theta_1 = \psi_1$ e $\theta_2 = -\psi_2$, temos:

$$x_1 = a_1 e^{i\theta_1}, \quad x_2 = a_2 e^{-i\theta_2}$$

com $0 < \theta_1, \theta_2 < \pi$. Como $x_1, x_2 \in T_n$, temos que ${x_1}^n, {x_2}^n \in \mathbb{Q}$ e portanto, para $j = 1, 2$:

$${x_j}^n = {a_j}^n e^{\pm ni\theta_j} = {a_j}^n(\cos(\pm n\theta_j) + i\operatorname{sen}(\pm n\theta_j)) \in \mathbb{Q}.$$

Logo, $\operatorname{sen}(\pm n\theta_j) = 0$, de onde concluímos que $\pm n\theta_j = k_j\pi$, ou seja, $\theta_j = k_j\pi/n$. Daí, temos também $\cos(\pm n\theta_j) = \cos(k_j\pi) = \pm 1$ e portanto ${a_j}^n \in \mathbb{Q}$, ou seja, $a_j \in T_{n,\mathbb{R}}$. Sabendo que $x_1 + x_2 = 1$ e colocando estes números no plano complexo, obtemos o triângulo de vértices 0, 1 e x_1 conforme a figura abaixo.



Seja $\theta_0 \in (0, \pi)$ dado por $\theta_0 = \pi - \theta_1 - \theta_2$. Então:

$$\theta_0 = \pi - \frac{k_1\pi}{n} - \frac{k_2\pi}{n} = \frac{\pi(n - k_1 - k_2)}{n} = \frac{k_0\pi}{n}.$$

Sabendo que $\operatorname{sen}\theta_j = \dfrac{e^{i\theta_j} - e^{-i\theta_j}}{2i}$, onde $\theta_j = k_j\pi/n = 2k_j\pi/2n$ para $j = 0, 1, 2$, e que i é uma raiz quarta da unidade concluímos que $\operatorname{sen}\theta_j \in \mathbb{Q}(e^{2\pi i/4n})$.

Aplicando a Lei dos Senos no triângulo acima, obtemos ainda:

$$\frac{a_2}{1} = \frac{\operatorname{sen}\theta_1}{\operatorname{sen}\theta_0}, \quad \frac{a_1}{1} = \frac{\operatorname{sen}\theta_2}{\operatorname{sen}\theta_0}.$$

Logo, $a_1, a_2 \in \mathbb{Q}(e^{2\pi i/4n}) \cap \mathbb{R}$ e usando o Lema 3.10 concluímos ${a_1}^2, {a_2}^2 \in \mathbb{Q}$.

Aplicando a Lei dos Cossenos no mesmo triângulo temos:

$$\cos\theta_1 = \frac{{a_1}^2 + 1 - {a_2}^2}{2a_1}, \ \cos\theta_2 = \frac{{a_2}^2 + 1 - {a_1}^2}{2a_2}.$$

Como ${a_1}^2, {a_2}^2 \in \mathbb{Q}$ e $\cos(2\theta) = 2\cos^2\theta - 1$ temos $\cos(2\theta_j) \in \mathbb{Q}$. Então, usando o Lema 3.12 temos $2\cos(2\theta_j) \in \mathbb{Z}$, o que nos dá $2\cos(2\theta_j) \in \{0, \pm 1, \pm 2\}$, ou seja, $\cos(2\theta_j) \in \{0, \pm 1/2, \pm 1\}$.

Como $0 < \theta_j < \pi$, temos que $2\theta_j \in \left\{\dfrac{\pi}{3}, \dfrac{\pi}{2}, \dfrac{2\pi}{3}, \pi, \dfrac{4\pi}{3}, \dfrac{3\pi}{2}, \dfrac{5\pi}{3}\right\}$ e portanto:

$$\theta_j \in \left\{\frac{2\pi}{12}, \frac{3\pi}{12}, \frac{4\pi}{12}, \frac{6\pi}{12}, \frac{8\pi}{12}, \frac{9\pi}{12}, \frac{10\pi}{12}\right\}.$$

Suponhamos que $\theta_1 \geq \theta_2$. Temos as seguintes possibilidades para (θ_1, θ_2):

$$\left\{\left(\frac{\pi}{3}, \frac{\pi}{3}\right), \left(\frac{\pi}{4}, \frac{\pi}{4}\right), \left(\frac{\pi}{6}, \frac{\pi}{6}\right), \left(\frac{\pi}{2}, \frac{\pi}{3}\right), \left(\frac{\pi}{2}, \frac{\pi}{4}\right), \left(\frac{\pi}{2}, \frac{\pi}{6}\right), \left(\frac{\pi}{3}, \frac{\pi}{6}\right), \left(\frac{2\pi}{3}, \frac{\pi}{6}\right)\right\}$$

A partir destes valores de (θ_1, θ_2) basta analisar os triângulos obtidos com estes ângulos para chegarmos à tabela:

Triângulo	θ_1	θ_2	a_1	a_2
$30° - 30° - 120°$	$2\pi/3$	$\pi/6$	1	$\sqrt{3}$
	$\pi/6$	$\pi/6$	$1/\sqrt{3}$	$1/\sqrt{3}$
$45° - 45° - 90°$	$\pi/2$	$\pi/4$	1	$\sqrt{2}$
	$\pi/4$	$\pi/4$	$1/\sqrt{2}$	$1/\sqrt{2}$
$30° - 60° - 90°$	$\pi/2$	$\pi/3$	$\sqrt{3}$	2
	$\pi/2$	$\pi/6$	$1/\sqrt{3}$	$2/\sqrt{3}$
	$\pi/3$	$\pi/6$	$1/2$	$\sqrt{3}/2$
$60° - 60° - 60°$	$\pi/3$	$\pi/3$	1	1

□

Proposição 3.14. *Sejam $m, n \in \mathbb{Z}_+$ com $mdc(m,n) = 1$ e $m > 2$. Então existem $x, y \in T_n$ tais que $x^m + y^m = 1$ se e somente se 6 divide n e neste caso $x^n = y^n = 1$.*

Demonstração: Sejam $x, y \in T_n$ tais que $x^m + y^m = 1$ e sejam $\alpha = x^m, \beta = y^m$. Como $\alpha + \beta = 1$, então pela Proposição 3.13 temos as seguintes possibilidades:

i) $\alpha, \beta \in \mathbb{Q}$. Como $x^n \in \mathbb{Q}$ e $x \in T_m$, temos $x^m, x^n \in \mathbb{Q}$ de onde $x^{mdc(m,n)} = x^1 = x \in \mathbb{Q}$. Analogamente obtemos $y \in \mathbb{Q}$. Absurdo, pois $x^n + y^n = 1$, contrariando o Teorema 0.1.

ii) $\alpha = a_1 e^{i\theta_1} = x^m, \beta = a_2 e^{-i\theta_2} = y^m$ com a_i, θ_i tomando valores da tabela anterior para $i = 1, 2$. Como $y \in T_n$, temos:

$$a_2{}^{n/m} = |y^n| \in \mathbb{Q}.$$

Logo, $a_2{}^n$ é a m-ésima potência de um racional. Mas $mdc(m,n) = 1$, então analisando os valores da tabela obtida na Proposição 3.13, concluímos que $a_2 = 1$, cujos únicos correspondentes são $a_1 = 1$ e $\theta_1 = \theta_2 = \pi/3$. Então $\alpha = e^{\pi i/3}, \beta = e^{-\pi i/3}$. Como $\alpha^n = (x^m)^n = (x^n)^m \in \mathbb{Q}$, temos $\alpha \in T_n$ e portanto $\alpha^n = e^{n\pi i/3} \in \mathbb{Q}_+$. Logo, $6|n$ e $\alpha^n = \beta^n = 1$, nos dando ainda $x^n = 1$, pois $x^n = \alpha^{n/m} \in \mathbb{Q}_+$ é uma raiz m-ésima da unidade. Analogamente temos que $y^n = 1$.

Reciprocamente, suponhamos que 6 divide n e vejamos que existem soluções para a equação. Sejam $x = e^{m\pi i/3}, y = e^{-m\pi i/3}$. Então:

$$x^n = e^{6km\pi i/3} = e^{2km\pi i} = 1.$$

$$y^n = e^{-6km\pi i/3} = e^{-2km\pi i} = 1.$$

Das igualdades acima obtemos $x, y \in T_n$. Como $1 = mdc(m,n) = mdc(m,6)$, temos $m \equiv \pm 1 \ (mod\ 6)$ e portanto $m^2 \equiv \pm 1 \ (mod\ 6)$, nos dando $m^2 = 6q \pm 1$. Logo:

$$x^m + y^m = e^{m^2\pi i/3} + e^{-m^2\pi i/3} = e^{(6q\pm 1)\pi i/3} + e^{-(6q\pm 1)\pi i/3} = e^{\pm \pi i/3} + e^{\mp \pi i/3} = 1.$$

□

Finalmente estamos prontos para demonstrar o Teorema 3.1.

Demonstração de 3.1: Suponhamos que 6 divide n. Pela Proposição 3.14, $x^m + y^m = 1$ possui solução (a, b) em T_n tal que $a^n = b^n = 1$. Então $a^m + b^m = 1 = 1^m$, e portanto $(a, b, 1)$ é uma solução de $x^m + y^m = z^m$ tal que $a^n = b^n = 1^n$, ou seja, $x^m + y^m = z^m$ possui solução da forma desejada.

Reciprocamente, suponhamos que (a, b, c) é solução de $x^m + y^m = z^m$ e que $a^n, b^n, c^n \in \mathbb{Z}$. Logo,

$$a^m + b^m = c^m.$$

Obtemos então:

$$1 = \frac{a^m}{c^m} + \frac{b^m}{c^m}.$$

Daí, $\left(\frac{a}{c}, \frac{b}{c}\right)$ é solução de $x^m + y^m = 1$, onde $\frac{a}{c}, \frac{b}{c} \in T_n$. Portanto, estamos nas hipóteses da Proposição 3.14 e daí temos que 6 divide n e ainda:

$$1 = \left(\frac{a}{c}\right)^n = \left(\frac{b}{c}\right)^n.$$

Obtemos então $a^n = b^n = c^n$. □

Capítulo 4

A Generalização para Expoentes Inteiros Gaussianos

O objetivo deste capítulo é generalizar o Último Teorema de Fermat para expoentes inteiros gaussianos, sem a necessidade de hipóteses adicionais. Para isto, começaremos provando alguns lemas.

Lema 4.1. $e^{2i\theta} - 2\cos\theta e^{i\theta} + 1 = 0$, *para todo* $\theta \in \mathbb{R}$.

Demonstração: Sabemos que $e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$, então:

$$\begin{aligned} e^{2i\theta} - 2\cos\theta e^{i\theta} + 1 &= (\cos\theta + i\,\mathrm{sen}\,\theta)^2 - 2\cos\theta(\cos\theta + i\,\mathrm{sen}\,\theta) + 1 \\ &= \cos^2\theta + 2i\,\mathrm{sen}\,\theta\cos\theta - \mathrm{sen}^2\theta - 2\cos^2\theta - 2i\,\mathrm{sen}\,\theta\cos\theta \\ &+ 1 = -\cos^2\theta - \mathrm{sen}^2\theta + 1 = -1 + 1 = 0. \end{aligned}$$

□

Lema 4.2. *Sejam* $n, m \in \mathbb{Z},\ m \neq 0$. *Então:*

i) $|x^{n+im} + y^{n+im}|^2 = x^{2n} + y^{2n} + 2x^n y^n \cos\theta$, *com* $\theta = m\log(\frac{x}{y})$.

ii) $|z^{n+im}|^2 = z^{2n}$.

Demonstração:

i) $|x^{n+im}+y^{n+im}|^2 = |x^n e^{\log(x^{im})}+y^n e^{\log(y^{im})}|^2 = |x^n e^{im\log x}+y^n e^{im\log y}|^2 =$
$|x^n(\cos(m\log x)+i\,\mathrm{sen}(m\log x))+y^n(\cos(m\log y)+i\,\mathrm{sen}(m\log y))|^2 =$
$|x^n\cos(m\log x)+y^n\cos(m\log y)+i(x^n\,\mathrm{sen}(m\log x)+y^n\,\mathrm{sen}(m\log y))|^2 =$
$(x^n\cos(m\log x)+y^n\cos(m\log y))^2+(x^n\,\mathrm{sen}(m\log x)+y^n\,\mathrm{sen}(m\log y))^2 =$
$x^{2n}\cos^2(m\log x)+2x^ny^n\cos(m\log x)\cos(m\log y)+y^{2n}\cos^2(m\log y)+$
$x^{2n}\,\mathrm{sen}^2(m\log x)+2x^ny^n\,\mathrm{sen}(m\log x)\,\mathrm{sen}(m\log y)+y^{2n}\,\mathrm{sen}^2(m\log y) =$
$x^{2n}+y^{2n}+2x^ny^n\cos(m\log x-m\log y) = x^{2n}+y^{2n}+2x^ny^n\cos\theta$, com
$\theta = m\log(\frac{x}{y})$.

ii) $|z^{n+im}|^2 = |z^n\cdot z^{im}|^2 = |z^n e^{\log(z^{im})}|^2 = |z^n e^{im\log z}|^2 = |z^n(\cos(m\log z)+$
$i\,\mathrm{sen}(m\log z))|^2 = z^{2n}(\cos^2(m\log z))+z^{2n}(\mathrm{sen}^2(m\log z)) = z^{2n}$.

□

Para provar o Teorema 4.4, necessitamos do seguinte teorema:

Teorema 4.3. (Gelfond-Schneider) *Sejam $\alpha,\beta\in\mathbb{C}$ tais que α é algébrico e $\alpha\neq 0,1$ e β é algébrico mas não é racional. Então α^β é transcendente.*

Demonstração: Ver [3]. □

Este teorema, que não será provado nesta dissertação, respondeu em 1934-1935 por Gelfond e Schneider um dos 23 problemas propostos por Hilbert na conferência do Congresso Internacional de Matemática de Paris em 1900.

Finalmente estamos prontos para provar o teorema desejado.

Teorema 4.4. *Sejam $m,n\in\mathbb{Z}$ com $m\neq 0$. Então a equação*

$$x^{n+im}+y^{n+im}=z^{n+im}$$

não possui soluções inteiras não-nulas.

Demonstração: Suponhamos por absurdo que existem x,y,z inteiros não-nulos tais que $x^{n+im}+y^{n+im}=z^{n+im}$. Logo, tomando o módulo complexo ao quadrado calculado no Lema 4.2 obtemos:

$$x^{2n}+y^{2n}+2x^ny^n\cos\theta = z^{2n},\ \text{com}\ \theta = m\log\left(\frac{x}{y}\right).$$

Concluímos então que:

$$\cos\theta = \frac{z^{2n} - x^{2n} - y^{2n}}{2x^n y^n} \in \mathbb{Q}.$$

Além disso, pelo Lema 4.1, $e^{2i\theta} - 2\cos\theta e^{i\theta} + 1 = 0$ para todo θ real. Portanto, para $\theta = m\log(\frac{x}{y})$ temos que $e^{i\theta}$ é raiz de $x^2 - 2\cos\theta x + 1 \in \mathbb{Q}[x]$ e portanto é algébrico. Mas,

$$e^{i\theta} = e^{im\log(\frac{x}{y})} = \left(e^{\log(\frac{x}{y})}\right)^{im} = \left(\frac{x}{y}\right)^{im}$$

e im é um complexo algébrico não-racional então, pelo Teorema 4.3, temos que $x = y$ (já que $x, y, z \neq 0$). Temos então que $2x^{n+im} = z^{n+im}$, ou seja, $(\frac{z}{x})^{n+im} = 2$. Aplicando novamente o Teorema 4.3 temos $z = x$, o que nos dá $2x^{n+im} = x^{n+im}$, com $x \neq 0$. Absurdo. □

Bibliografia

[1] Baker, A., "*Transcendental Number Theory*", Cambridge University Press (2nd edition), Cambridge, 1979.

[2] Bennett, C. D., Glass, A. M. W., Székely, G. J., "*Fermat's last theorem for rational exponents*", Monthly 111 (2004) 322-329.

[3] Gelfond, A. O., "*Sur le septième problème de Hilbert*", I.A.N. 7 (1934), 623-30; D.A.N. 2 (1934), 1-6.

[4] Lang, S., "*Algebra*", Addison-Wesley Publishing Company, Reading, Massachusetts, 1965.

[5] Stewart, I., "*Galois Theory*", 2nd ed., Chapman & Hall, London, 1989.

[6] Taylor, R., Wiles, A., "*Ring-theoretic properties of certain Hecke algebras*", Ann. Math. 141 (1995) 553-572.

[7] Tomescu, D., Vulpescu-Jalea, F., "*On the Fermat's equation with rational exponents*", Bull. Math. Soc. Sci. Math R. S. Roumanie (N.S.) 34 (82) (1990) 187-192.

[8] Tschebotaröw, N., "*Grundzüge der Galoissehen Theorie*", P. Noordhoff N. V., Groningen-Djakarta, 1950.

[9] Wiles, A., "*Modular elliptic curves and Fermat's last theorem*", Ann. Math. 141 (1995) 443-551.

[10] Zuehlke, J., "*Fermat's last theorem for Gaussian integer exponents*", Monthly 106 (1999) 49.