vada por forma que o produto da espessura pela secção eficaz de difusão macroscópica seja finita, nomeadamente $0{,}71 - 0{,}33 = 0{,}38$. A solução do problema da difusão com tal elemento dispersivo entre o meio multiplicativo e o completamente absorvente que o rodeia, apresenta para o interior do meio multiplicativo (o elemento de combustível) o mesmo fluxo que o calculado por INÖNÜ. Considerando a variação de fluxo neutrónico nas vizinhanças da fronteira entre dois meios diferentes, verifica-se que é pouco provável que a introdução de uma superfície dispersiva explique adequadamente em todos os casos as perturbações no fluxo dessa vizinhança. Ainda preferível, em geral, é o considerar-se em adição à superfície dispersiva uma superfície absorvente, positiva ou negativa. De facto, para dividir a absorpção responsável pela variação do fluxo entre os dois meios, será necessário atribuir parte da absorpção superficial a um, parte ao outro meio, isto é, será necessário introduzir duas superfícies absorventes. Juntamente com a superfície dispersiva, dever-se-ia reproduzir desta forma o efeito das perturbações junto das fronteiras em termos da teoria da difusão.

10. Conclusão

O objectivo destas observações é o de exprimir a ideia de que a ciência dos reactores pode ser altamente auxiliada pela atenção dos matemáticos por estes problemas; mas também a convicção de que os matemáticos encontrarão muito interessantes problemas na ciência dos reactores.

Decomposição de ideais em ideais primos: teoria de Kummer-Dedekind

por **Ubiratan D'Ambrosio**
Faculdade de Filosofia, Ciências, Letras de Rio Claro, S. P., Brasil

0. O teorema fundamental da teoria dos ideais estabelece a decomposição única de ideais não triviais num produto de ideais primos [1, pág. 43](+), isto é,

$$\mathfrak{A} = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdot \cdots \cdot \mathfrak{P}_g^{e_g}.$$

Como se verifica, a demonstração do teorema não nos dá nenhum processo de determinar efectivamente tal decomposição.

Para efectuar a decomposição, sendo $\mathfrak{A} = (\alpha_1, \alpha_2, \cdots, \alpha_r)$ basta conhecer a decomposição dos ideais principais (α_i), pois $\mathfrak{A}$ se obtém como m. d. c. dêstes [1, pág. 43], que pode ser calculado com facilidade a partir das decomposições de $(\alpha_1), (\alpha_2), \cdots, (\alpha_r)$. [2, pág. 110].

Para decompor (α), observamos que $(\alpha) \mid N(\alpha)$, e sendo $N(\alpha)$ racional inteiro, temos $N(\alpha) = p_1^{a_1} \cdot \cdots \cdot p_s^{a_s}$. Então só entram na decomposição de (α) os ideais primos $\mathfrak{P}$ que entram na decomposição dos (p_i); efectuando então a decomposição dos números primos racionais (++) em ideais primos, obtemos os ideais primos do corpo.

(+) Os números em colchetes referem-se à bibliografia. A notação adotada é em geral a usada em [1].

(++) Por números primos racionais queremos dizer ideais principais gerados por números primos racionais.

Exporemos em **1.** e **2.** a teoria da decomposição conforme foi desenvolvida por Dedekind, generalizando os estudos de Kummer, que se restringiu a corpos ciclotômicos. Não desenvolveremos a teoria em toda sua generalidade, explicitando as restrições e indicando o desenvolvimento mais geral em **3.**

1. Consideremos o corpo $Q(\theta)$, extensão de grau n do corpo Q, dos números racionais. Suponhamos que a base natural $1, \theta, \theta^2, \cdots, \theta^{n-1}$ seja uma base inteira de $Q(\theta)$, o que nem sempre acontece. Conforme veremos em **3.** os resultados aqui obtidos podem ser estendidos aos casos em que isso não se dá.

Todo α inteiro do corpo pode ser escrito então como $\alpha = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$, com os c_i racionais inteiros.

Seja $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ a equação do corpo de θ.

Seja p um primo racional, com decomposição $(p) = \mathfrak{P}_1^{e_1} \cdot \cdots \cdot \mathfrak{P}_g^{e_g}$ onde os $\mathfrak{P}_i$ são ideais primos em $Q(\theta)$.

Sendo $N((p)) = |N(\mathfrak{P}_1)|^{e_1} \cdots |N(\mathfrak{P}_g)|^{e_g}$, e $N((p)) = p^n$, temos $p^n = |N(\mathfrak{P}_1)|^{e_1} \cdot |N(\mathfrak{P}_2)|^{e_2} \cdots |N(\mathfrak{P}_g)|^{e_g}$, e então $N(\mathfrak{P}_i) = p^{f_i}$, com $f_i \leq n \cdot f_i$ é chamado *grau* de $\mathfrak{P}_i$ e e_i é chamado *ordem de ramificação* de $\mathfrak{P}_i$. Assim, $n = e_1 f_1 + \cdots + e_g f_g$.

DEFINIÇÃO. Consideremos o ideal $\mathfrak{A}$ tal que $\mathfrak{A}/(p)$ e $\mathfrak{A} \neq (1)$ e sejam $\gamma_1 \cdot \gamma_2, \cdots, \gamma_k$ inteiros do corpo. Diremos que $\gamma_1 \cdot \gamma_2, \cdots, \gamma_k$ são linearmente independentes mod $\mathfrak{A}$ quando $\sum_1^k{}_m x_m \gamma_m \equiv 0 \pmod{\mathfrak{A}}$, com x_m racionais inteiros implica $x_m \equiv 0 \pmod p$ $(m = 1, 2, \cdots, k)$. Caso contrário $\gamma_1 \cdot \gamma_2, \cdots, \gamma_k$ serão ditos linearmente dependentes mod $\mathfrak{A}$.

Observemos que a independência linear dos inteiros $\gamma_1, \gamma_2, \cdots, \gamma_k$ fica estabelecida uma vez fixado $\mathfrak{A}$, pois o número primo p fica unìvocamente determinado por $\mathfrak{A}$ (+).

TEOREMA. *Sendo* $N(\mathfrak{A}) = p^f$, *o número máximo de inteiros do corpo linearmente independentes mod* $\mathfrak{A}$ *é igual a* f.

Observemos de início que $1 \leq f \leq n$. De facto, $\mathfrak{A}/(p)$ logo $(p) = \mathfrak{A} \cdot \mathfrak{B}$; então $N((p)) = N(\mathfrak{A}) \cdot N(\mathfrak{B})$, logo $p^n = p^f \cdot N(\mathfrak{B})$. Como $\mathfrak{A} \neq (1)$, $1 \leq f \leq n$.

Para a demonstração do teorema utilizaremos dois lemas.

LEMA 1. *Sendo* f' *o número máximo de inteiros do corpo linearmente independentes mod* $\mathfrak{A}$, *temos* $1 \leq f' \leq f$.

DEMONSTRAÇÃO. 1 é linearmente independente mod $\mathfrak{A}$, pois $x \cdot 1 \equiv 0 \pmod{\mathfrak{A}}$ implica $x \equiv 0 \pmod p$. De facto, se assim não fosse, isto é, se $x \not\equiv 0 \pmod p$, existiriam racionais inteiros u e v, tais que $u\,x + v \cdot p = 1$ e então, como $\mathfrak{A} \mid (x)$ e $\mathfrak{A} \mid (p)$, teríamos $\mathfrak{A} \mid (1)$, o que é absurdo, pois $\mathfrak{A} \neq (1)$. Logo $f' \geq 1$.

Sejam $\gamma_1, \gamma_2, \cdots, \gamma_{f'}$ inteiros do corpo linearmente independentes mod $\mathfrak{A}$. Então $y_1\gamma_1 + y_2\gamma_2 + \cdots + y_{f'}\gamma_{f'}$ com $0 \leq y_i < p$ formam $p^{f'}$ classes de restos incôngruas mod $\mathfrak{A}$, pois se $\sum_1^{f'}{}_i y_i' \gamma_i \equiv \sum_1^{f'}{}_i y_i'' \gamma_i \pmod{\mathfrak{A}}$, com $0 \leq y_i', y_i'' < p$, então $\sum_1^{f'}{}_i (y_i' - y_i'')\gamma_i \equiv 0 \pmod{\mathfrak{A}}$ e $y_i' - y_i'' \equiv 0 \pmod p$, e $\sum_1^{f'}{}_i y_i' \gamma_i$ e $\sum_1^{f'}{}_i y_i'' \gamma_i$ coincidiriam. Como o número de clas-

---

(+) De facto, se existissem, p e q tais que $\mathfrak{A}/(p)$ e $\mathfrak{A}/(q)$, sendo p e q primos entre si existiriam r e s tais que $pr + qs = 1$ e $\mathfrak{A} \mid (1)$, contra a hipótese.

ses incôngruas mod $\mathfrak{A}$ é $N(\mathfrak{A})$ [1, pág. 51], temos $p^{f'} \leq p^f$, e daí $f' \leq f$.

Notemos que não é possível concluir que $f' = f$, pois não se pode afirmar que $y_1\gamma_1 + y_2\gamma_2 + \cdots + y_{f'}\gamma_{f'}$ dão todas as classes de restos mod $\mathfrak{A}$ quando $0 \leq y_i < p$. Isto acontece efectivamente, como veremos a seguir.

LEMA 2. *Sejam* $\gamma_1, \gamma_2, \cdots, \gamma_{f'}$ *linearmente independentes mod* $\mathfrak{A}$, *onde* f' *é o número máximo de inteiros do corpo nessas condições. Então cada inteiro do corpo pode ser escrito como* $\gamma \equiv \sum_1^{f'} x_m \gamma_m \pmod{\mathfrak{A}}$, *com* x_m *racionais inteiros unìvocamente determinados mod* p.

DEMONSTRAÇÃO. $\gamma_1, \gamma_2, \cdots, \gamma_{f'}, \gamma$ são linearmente dependentes mod $\mathfrak{A}$, isto é, pode-se ter $y_1\gamma_1 + \cdots + y_{f'}\gamma_{f'} + y\gamma \equiv 0 \pmod{\mathfrak{A}}$ com nem todos $y_1, y_2, \cdots, y_{f'}, y$ divisíveis por p. Mais explìcitamente, é $y \not\equiv 0 \pmod p$. Então existe um único racional inteiro z tal que $zy \equiv -1 \pmod p$. Logo

$$-zy\gamma \equiv zy_1\gamma_1 + \cdots + zy_{f'}\gamma_{f'} \equiv 0 \pmod{\mathfrak{A}}$$

e fazendo $x_i = zy_i$, temos $\gamma \equiv x_1\gamma_1 + \cdots + x_{f'}\gamma_{f'} \pmod{\mathfrak{A}}$. A representação é única, pois se $\gamma \equiv u_1\gamma_1 + \cdots + u_{f'}\gamma_{f'} \pmod{\mathfrak{A}}$, então $(x_1 - u_1)\gamma_1 + \cdots + (x_{f'} - u_{f'})\gamma_{f'} \equiv 0 \pmod{\mathfrak{A}}$ e pela independência linear de $\gamma_1, \gamma_2, \cdots, \gamma_{f'}$ temos $x_i \equiv u_i \pmod p$ $(i = 1, \cdots, f')$.

Então os $p^{f'}$ números $y_1\gamma_1 + \cdots + y_{f'}\gamma_{f'}$, com $0 \leq y_i < p$, formam um sistema de representantes das classes de restos mod $\mathfrak{A}$, pois são incongruos mod $\mathfrak{A}$ (lema 1) e todo inteiro do corpo é côngruo a um deles (lema 2). Como o número de classes de restos mod $\mathfrak{A}$ é $N(\mathfrak{A})$, temos $p^{f'} = p^f$, e $f = f'$, o que demonstra o teorema.

2. Voltemos ao problema da determinação dos ideais primos que aparecem na decomposição $(p) = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdot \cdots \cdot \mathfrak{P}_g^{e_g}$. Faremos, neste parágrafo $\mathfrak{P}_1 = \mathfrak{P}$ e $e_1 = e$.

Seja f o número máximo de potências de θ linearmente independentes mod $\mathfrak{P}$, isto é, o corpo $Q[\theta]/\mathfrak{P}$ é extensão de grau f do corpo Z/p. Pelo teorema demonstrado em 1. sabemos que f é o grau do ideal $\mathfrak{P}$ em (p). Podemos tomar como as f potências de θ linearmente independentes mod $\mathfrak{P}$ as f primeiras. De facto, $1, \theta, \theta^2 \ldots \ldots \theta^{f-1}, \theta^f$ são linearmente dependentes e θ^f é combinação linear de $1, \theta, \theta^2, \ldots, \theta^{f-1}$, bem como $\theta^h, \forall h > f$. Logo, $1, \theta, \theta^2, \ldots, \theta^{f-1}$ são linearmente independentes mod $\mathfrak{P}$.

Seja $L(\theta) = b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{f-1}\theta^{f-1} + b_f\theta^f \equiv 0 \pmod{\mathfrak{P}}$, com os b_i racionais inteiros, nem todos divisíveis por p, em particular com $b_f \not\equiv 0 \pmod p$, e como estamos trabalhando num corpo, pode-se tomar $b_f = 1$.

Consideremos o polinómio $L(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{f-1}x^{f-1} + x^f$, com coeficientes em Z/p.

Como $f \leq n$, podemos dividir $f(x)$ por $L(x)$, e reduzir mod p, obtendo $f(x) \equiv L(x) \cdot G(x) + H(x) \pmod p \cdot (')$.

Observemos que se vale (') temos

$$f(x) - L(x) \cdot G(x) - H(x) = p \cdot \Phi(x),$$

onde $\Phi(x)$ é um polinómio com coeficientes em Z e então $f(\theta) - L(\theta) \cdot G(\theta) - H(\theta) = p \cdot \Phi(\theta)$, com $\Phi(\theta) \in Q[\theta]$. Mas $\mathfrak{P}/(p)$, logo $(p) \subset \mathfrak{P}$ e $p \cdot \Phi(\theta)$ é um elemento de $\mathfrak{P}$, e então $f(\theta) \equiv L(\theta) \cdot G(\theta) + H(\theta) \bmod \mathfrak{P}$.

Sendo $f(\theta) \equiv 0 \pmod{\mathfrak{P}}$ e $L(\theta) \equiv 0 \pmod{\mathfrak{P}}$, temos $H(\theta) \equiv 0 \pmod{\mathfrak{P}}$, com grau de $H(x)$ menor que f. Mas então, sendo $H(x) = r_0 + r_1 x + \cdots + r_{f-1}x^{f-1}$ temos $r_i \equiv 0 \pmod p$ $(i = 0, 1, \cdots, f-1)$, pois o número máximo de potências de θ linearmente independentes mod $\mathfrak{P}$ é f. Então $H(x) \equiv 0 \pmod p$, e $f(x) \equiv L(x) \cdot G(x) \pmod p$.

Façamos $(p, L(\theta)) = \mathfrak{A}$. Vamos ver que $\mathfrak{P} = \mathfrak{A}$.

É imediato que $\mathfrak{A} \subset \mathfrak{P}$, pois $p \in \mathfrak{P}$ e $L(\vartheta) \in \mathfrak{P}$.

Para demonstrar que $\mathfrak{P} \subset \mathfrak{A}$, tomemos um qualquer $\beta \in \mathfrak{P}$. Temos $\beta = B(\theta)$, onde $B(x)$ é um polinómio com coeficientes em Z. Dividindo $B(x)$ por $L(x)$, e reduzindo mod p, obteremos $B(x) \equiv L(x) \cdot G'(x) + H'(x) \pmod{p}$, com grau de $H'(x)$ menor que f. Então $B(\theta) \equiv L(\theta) \cdot G'(\theta) + H'(\theta) \pmod{\mathfrak{P}}$. Como $\beta \in \mathfrak{P}$, temos $B(\theta) \equiv 0 \pmod{\mathfrak{P}}$ e $L(\theta) \equiv 0 \pmod{\mathfrak{P}}$. $\therefore H'(\theta) \pmod{\mathfrak{P}}$, logo $H'(x) \equiv 0 \pmod{p}$. Então $B(x) \equiv L(x) \cdot G'(x) \pmod{p}$, isto é, $B(x) = L(x) \cdot G'(x) + p \cdot \Phi(x)$ e $B(\theta) = L(\theta) \cdot G'(\theta) + p\ \Phi(\theta)$, com $G'(\theta)$ e $\Phi(\theta)$ inteiros do corpo. Isto equivale a dizer que um elemento qualquer de $\mathfrak{P}$ pode ser escrito como $\beta = \mu \cdot L(\theta) + \nu \cdot p$, com $\mu, \nu \in Q[\theta]$, logo $\beta \in \mathfrak{A}$, ou seja $\mathfrak{P} \subset \mathfrak{A}$. Então $\mathfrak{P} = \mathfrak{A}$.

Se a ordem de ramificação de $\mathfrak{P}$ em (p) for maior que 1, temos $\mathfrak{P} / L(\theta)$ e $\mathfrak{P}^2 / L(\theta)$. De facto, $\mathfrak{P} = (p, L(\theta))$. Se $\mathfrak{P}^2 / L(\theta)$, como $\mathfrak{P}^2 / (p)$, $\mathfrak{P}^2$ dividiria $\mathfrak{P}$, o que só é possível se $\mathfrak{P} = (1)$.

Sendo $f(x) \equiv L(x) \cdot G(x) \pmod{p}$ temos $f(\theta) \equiv L(\theta) \cdot G(\theta) \pmod{\mathfrak{P}^2}$, pelo visto anteriormente, e como $f(\theta) \equiv 0 \pmod{\mathfrak{P}^2}$, temos $\mathfrak{P}^2 / L(\theta) \cdot G(\vartheta)$. Mas $\mathfrak{P}^2 / L(\theta)$, logo $\mathfrak{P} / G(\theta)$.

Como $n \geq 2 \cdot f$, de $f(x) \equiv L(x) \cdot G(x) \pmod{p}$ temos que grau de $G(x)$ é $\geq f$. Então dividindo $G(x)$ por $L(x)$ temos $G(x) \equiv L(x) \cdot G_2(x) + H_2(x) \pmod{p}$ e

$$G(\theta) \equiv L(\theta) \cdot G_2(\theta) + H_2(\vartheta) \pmod{\mathfrak{P}}$$

e anàlogamente ao que foi feito para $f(x)$, temos $H_2(x) \equiv 0 \pmod{p}$. Logo

$$f(x) \equiv |L(x)|^2 \cdot G_2(x) \pmod{p}.$$

Assim sucessivamente, teremos

$$f(x) \equiv |L(x)|^e \cdot G_e(x) \pmod{p},$$

com grau de $G_e(x)$ igual a $n - e \cdot f$.

Considerando agora $\mathfrak{P}_2$, seja f_2 o número máximo de potências de θ linearmente independentes mod $\mathfrak{P}_2$, e $L_2(\theta) = d_0 + d_1 \theta + d_2 \theta^2 + \cdots + d_{f_1 - 1} \theta^{f_1 - 1} + \theta^{f_1} \equiv 0 \pmod{\mathfrak{P}_2}$, com $d_i \in Z/p$.

Sendo $n - e \cdot f \geq f_2$, podemos repetir o processo para $G_e(x)$, obtendo

$$G_e(x) \equiv |L_2(x)|^{e_1} \cdot G_{e_2}(x) \pmod{p}$$

e

$$\mathfrak{P}_2 = (p, L_2(\theta)).$$

Assim $f(x) \equiv |L(x)|^e \cdot |L_2(x)|^{e_1} \cdot G_{e_2}(x) \pmod{p}$.

Sucessivamente, chegaríamos a

$$f(x) \equiv |L(x)|^e \cdot |L_2(x)|^{e_1} \cdot \cdots \cdot |L_g(x)|^{e_g} \cdot G_{e_g}(x) \pmod{p}.$$

Mas $G_{e_g}(x)$ tem o grau 0 pois $n = e \cdot f + e_2 \cdot f_2 + \cdots + e_g \cdot f_g$, e podemos tomá-lo igual a 1.

Ainda, os ideais $\mathfrak{P}, \mathfrak{P}_2, \cdots, \mathfrak{P}_g$ são distintos. De facto, se $\mathfrak{P}_i = \mathfrak{P}_k$, teríamos $L_i(\theta) \in \mathfrak{P}_k$, logo $L_i(\theta) = A(\theta) \cdot p + B(\theta) \cdot L_k(\theta)$, com $A(\theta)$ e $B(\theta)$ elementos de $Q[\theta]$ e então $L_i(\vartheta) \equiv L_k(\theta) \cdot B(\theta) \pmod{p}$, e $L_i(x) \equiv L_k(x) \cdot B(x) \pmod{p}$, e $L_i(x)$ não seria irredutível mod p.

Podemos então enunciar o importante resultado devido a Kummer (para corpos ciclotómicos) e generalizado por Dedekind:

«A decomposição de p em ideais primos de $Q(\theta)$ pode ser determinada pela decomposição de $f(x)$, equação do corpo de θ, em polinómios $L_i(x)$, irredutíveis mod p, com coeficientes em Z/p, cada ideal sendo dado por $\mathfrak{P}_i = (p, L_i(\vartheta))$; sendo $f(x) \equiv |L_1(x)|^{e_1} \cdot |L_2(x)|^{e_2} \cdot \cdots \cdot |L_g(x)|^{e_g} \pmod{p}$ temos $(p) = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdot \cdots \cdot \mathfrak{P}_g^{e_g}$, grau $L_i(x) = f_i =$ grau $\mathfrak{P}_i$».

3. Vamos indicar o desenvolvimento da teoria sem a condição imposta no início de 1. de ser a base natural uma base inteira. Não faremos o desenvolvimento geral neste número, limitando-nos a apresentar o problema.

Sendo $1, \theta, \theta^2, \theta^3, \cdots, \theta^{n-1}$ uma base não inteira, tomemos a base inteira $\Omega_1, \Omega_2, \cdots, \Omega_n$ [1, pág. 20]. Então todo inteiro do corpo pode ser escrito como combinação linear de $\Omega_1, \Omega_2, \cdots, \Omega_n$ com coeficientes em Z. Em particular, temos $\theta^{i-1} = c_{i,1}\Omega_1 + c_{i,2}\Omega_2 + \cdots + c_{i,n}\Omega_n$, com $c_{i,j} \in Z$, e

$$D(1, \theta, \theta^2, \cdots, \theta^{n-1}) = |c_{i,j}|^2 \cdot D(\Omega_1, \Omega_2, \cdots, \Omega_n)$$

onde

$$D(1, \theta, \theta^2, \cdots, \theta^{n-1}) \text{ e } D(\Omega_1, \Omega_2, \cdots, \Omega_n)$$

são respectivamente os descriminantes das bases $1, \theta, \theta^2, \cdots, \theta^{n-1}$ e $\Omega_1, \Omega_2, \cdots, \Omega_n$, sendo o segundo o discriminante do corpo, d, invariante [1, pág. 23]. O determinante da transformação, $|c_{ij}|$, é distinto de zero e depende apenas de θ. É chamado *índice* de θ e será representado por J. Assim, $D(1, \theta, \theta^2, \cdots, \theta^{n-1}) = J^2 \cdot d$.

Consideremos os elementos de $Q[\theta]$ da forma $w = \sum_0^{n-1} {}_i\, b_i \theta^i$, com $b_i \in Z$. Eles formam um anel $\mathfrak{D} \subset Q[\theta]$. Se $J = \pm 1$, $\mathfrak{D} = Q[\theta]$. Este foi o caso estudado em 1.1.

Se $J \neq \pm 1$, observemos de início que a representação dos elementos de $\mathfrak{D}$ pode ser feita mediante um polinómio $g(x)$ de grau qualquer, com coeficientes em Z. De facto, $g(x) = f(x) \cdot q(x) + r(x)$ com grau de $r(x)$ igual a $n-1$. Então, $g(\theta) = f(\theta) \cdot q(\theta) + r(\theta)$ logo $g(\theta) = r(\theta)$, e $r(\theta)$ é um elemento da forma $\sum_0^{n-1} {}_i\, b_i \theta^i$.

Um racional primo p será dito de *primeira espécie* se $p \nmid J$ e de *segunda espécie* se $p \mid J$.

Seja $w = d_1\Omega_1 + \cdots + d_n\Omega_n$, com

$$d_i = c_{1,i}b_0 + c_{2,i}b_1 + \cdots + c_{n,i}b_{n-1} \quad (i = 1, \cdots, n).$$

Seja p um primo racional de 1.ª espécie e $w \equiv 0 \pmod p$. Então $p \mid d_i$. Resolvendo o sistema

$$(s) \quad \begin{cases} d_1 = c_{1,1}b_0 + \cdots + c_{n,1}b_{n-1} \\ d_2 = c_{1,2}b_1 + \cdots + c_{n,2}b_{n-1} \\ \cdots\cdots\cdots\cdots\cdots \\ d_n = c_{1,n}b_0 + \cdots + c_{n,n}b_{n-1} \end{cases}$$

pela regra de CRAMER, $b_0 \cdot J = \Delta_0$, $b_1 \cdot J = \Delta_1, \cdots, b_{n-1} \cdot J = \Delta_{n-1}$, onde os Δ_i são combinações lineares dos $d_1, d_2, \cdots, d_n$, conforme o desenvolvimento do determinante segundo a $i+1$ — ésima coluna, logo $p \mid \Delta_i$ e $p \mid b_i \cdot J$. Como $p \nmid J$, $p \mid b_i$ $(i = 0, \cdots, n-1)$.

Sejam w_1, $w_2 \in \mathfrak{D}$ e $w_1 = b_0^{(1)} + b_1^{(1)}\theta + \cdots + b_{n-1}^{(1)}\theta^{n-1}$ e $w_2 = b_0^{(2)} + b_1^{(2)}\theta + \cdots + b_{n-1}^{(2)}\theta^{n-1}$. Será $w_1 \equiv w_2 \pmod p$ se e sòmente se $b_i^{(1)} \equiv b_i^{(2)} \pmod p$, pelo que acabamos de ver.

Temos então p^n números inteiros w incôngruos mod p em $\mathfrak{D}$. Em $Q[\theta]$ temos também p^n classes de inteiros mod p. Como $\mathfrak{D} \subset Q[\theta]$, podemos tomar como representantes das classes de $\mathfrak{D}/p$ elementos de $Q[\theta]/p$, e aplicar o mesmo desenvolvimento de 2. [3, pág. 54]. A teoria é então válida para primos de 1.ª espécie.

Se $p \mid J$, isto é, p é de 2.ª espécie, em (s) podemos determinar uma solução $b_0, b_1, \cdots, b_{n-1}$ onde nem todos os b_i são divisíveis por p. Então pode-se dar o caso em que $w_1 \equiv w_2 \pmod p$ e $b_i^{(1)} \not\equiv b_i^{(2)} \pmod p$, e em $\mathfrak{D}$ teremos um número de inteiros incôngruos mod p menor que p, e não é possível então estabelecer a correspondência entre $\mathfrak{D}/p$ e $Q[\theta]/p$.

A teoria desenvolvida para primos racionais de 1.ª espécie, embora não fosse válida para primos de 2.ª espécie, seria satisfatória se dado um número primo racional qualquer p, existisse um inteiro θ no corpo tal que seu índice fosse não divisível por p. Mas existem corpos, como mostrou DEDEKIND [4, pág. 234], onde um número primo racional p divide o índice de todos os inteiros do corpo.

Öystein Ore, usando congruências de funções com relação à potência de um número primo, estendeu o método obtendo uma teoria da decomposição válida sem excepção. [3, pág. 58].

1.4 — Aplicaremos a teoria desenvolvida na decomposição de um número primo racional num corpo quadrático $Q(\sqrt{a})$.

Distinguiremos dois casos: $a \equiv 2,3 \pmod 4$ e $a \equiv 1 \pmod 4$.

No 1.º caso, uma base inteira é $1, \sqrt{a}$ e o discriminante do corpo é $d = 4a$. A equação do corpo de $\sqrt{a}$ é $f(x) = x^2 - a$.

Consideremos um primo racional $p \neq 2$. Então a decomposição de $f(x) \bmod p$ se faz do seguinte modo:

i) $(a/p) = +1$ (+). $f(x) \equiv (x - x_1) \cdot (x - x_2) \pmod p$ e sendo $x_1 = -x_2$ tem-se $f(x) \equiv (x - x_1) \cdot (x + x_1) \pmod p$. Então $L_1(x) = x - x_1$ e $L_2(x) = x + x_1$, logo $L_1(\sqrt{a}) = \sqrt{a} - x_1$ e $L_2(\sqrt{a}) = \sqrt{a} + x_1$ e $\mathfrak{P}_1 = (p, x_1 - \sqrt{a})$ e $\mathfrak{P}_2 = (p, x_1 + \sqrt{a})$.

ii) $(a/p) = -1$. $f(x)$ não se decompõe $\bmod p$, isto é, (p) é um ideal primo de $Q(\sqrt{a})$, com grau $f = 2$.

iii) $(a/p) = 0$. Então $f(x) \equiv x^2 \pmod p$ e $L_1(x) = L_2(x) = x$, logo $g = 1$, $f = 1$, $e = 2$ e $L(\sqrt{a}) = \sqrt{a}$. Então $\mathfrak{P} = (p, \sqrt{a})$.

Se $p = 2$, teremos:

iv) se $a \equiv 3 \pmod 4$, ou $a \equiv 1 \pmod 2$, $x^2 - a \equiv 0 \pmod 2$ se decompõe em $(x - 1) \cdot (x + 1) \pmod 2$, e sendo

$-1 \equiv +1 \pmod 2$, $L_1(x) = L_2(x) = (x + 1)$,

logo $g = e = 1$ e $L(\sqrt{a}) = (\sqrt{a} + 1)$. Então $\mathfrak{P} = (2, \sqrt{a} + 1)$.

(+) (a/p) é o símbolo de Legendre, $= +1$ se a é resto quadrático $\bmod p$, $= -1$ se a é não-resto quadrático $\bmod p$ e $= 0$ se a é múltiplo de p.

v) se $a \equiv 2 \pmod 4$, isto é, $a \equiv 0 \pmod 2$, $x^2 - a \equiv 0 \pmod 2$ se decompõe em $x \cdot x \pmod 2$, logo $g = 1$, $e = 2$ e $L(x) = x$ e $L(\sqrt{a}) = \sqrt{a}$. Então $\mathfrak{P} = (2, \sqrt{a})$.

No 2.º caso, isto é, $a \equiv 1 \pmod 4$, uma base inteira é $1, \dfrac{1 + \sqrt{a}}{2}$ e o discriminante do corpo é $d = a$.

A equação do corpo de $\dfrac{1 + \sqrt{a}}{2}$ é $f(x) = x^2 - x + \dfrac{1 - a}{2}$.

Seja $p \neq 2$, primo racional. Então $f(x)$ se decompõe $\bmod p$ do seguinte modo:

vi) $(a/p) = +1$. Fazendo $f(x) \equiv (2x - 1)^2 - a \pmod p$, $f(x) \equiv (2x - 1 - x_1) \cdot (2x - 1 + x_1) \pmod p$. Então $L_1\left(\dfrac{1 + \sqrt{a}}{2}\right) = \left(2 \cdot \left(\dfrac{1 + \sqrt{a}}{2}\right) - 1 - x_1\right) = (\sqrt{a} - x_1)$ e $L_2\left(\dfrac{1 + \sqrt{a}}{2}\right) = (\sqrt{a} + x_1)$. Logo $\mathfrak{P}_1 = (p, x_1 - \sqrt{a})$ e $\mathfrak{P}_2 = (p, x_1 + \sqrt{a})$.

vii) $(a/p) = -1$. $f(x)$ não se decompõe $\bmod p$, logo (p) é um ideal primo de $Q(\sqrt{a})$.

viii) $(a/p) = 0$. $f(x) \equiv (2x - 1)^2 \pmod p$. Então $g = 1$, $e = 2$ e $L(x) = (2x - 1)$, logo $L\left(\dfrac{1 + \sqrt{a}}{2}\right) = \sqrt{a}$, e $\mathfrak{P} = (p, \sqrt{a})$.

Se $p = 2$, fazemos $f(x) = x^2 - x + \dfrac{1 - a}{4}$. Então,

ix) se $a \equiv 1 \pmod 8$, logo $\dfrac{1 - a}{4}$ é par, $f(x) \equiv x^2 - x \pmod 2$ e se decompõe em $x \cdot (x - 1)$, logo $L_1\left(\dfrac{1 + \sqrt{a}}{2}\right) = \dfrac{1 + \sqrt{a}}{2}$ e $L_2\left(\dfrac{1 + \sqrt{a}}{2}\right) = \dfrac{1 - \sqrt{a}}{2}$ e $\mathfrak{P}_1 = \left(2, \dfrac{1 + \sqrt{a}}{2}\right)$ e $\mathfrak{P}_2 = \left(2, \dfrac{1 - \sqrt{a}}{2}\right)$.

x) se $a \equiv 5 \pmod 8$, logo $\frac{1-a}{4}$ é ímpar, $f(x)$ não se decompõe mod 2, e (p) é ideal primo em $Q(\sqrt{a})$.

5. Um problema de fundamental importância para a decomposição de ideais é saber se na decomposição do ideal (p) em $Q(\vartheta)$ alguns factores ideais $\mathfrak{P}_i$ aparecem repetidos ou se todos são distintos. Em outros termos, se é algum $e_i > 1$. No caso de serem todos os $e_i = 1$, (p) diz-se *não ramificado*. Caso contrário, diz se *ramificado*.

A resposta ao problema é dada pelo seguinte teorema, devido a DEDEKIND [5]:

«*Dado o número primo racional* p, *a condição necessária e suficiente para que exista um ideal primo* $\mathfrak{P}$ *cujo quadrado divida* p *é que* p *divida* d, *sendo* d *o discriminante do corpo*».

Notemos que num corpo quadrático o teorema se verifica fàcilmente mediante os resultados de **4**.

De facto, (p) é o quadrado de um ideal primo nos casos iii, iv, v e viii, e sòmente nesses casos. E nestes casos, e sòmente nestes, p/d.

Vamos, partindo da decomposição feita em **2.**, demonstrar este teorema, seguindo em linhas gerais o desenvolvimento de ZOLOTAREFF [6]. Naturalmente as observações feitas em **3.** quanto à generalidade da decomposição mantêm-se para a demonstração que faremos, isto é, nos restringiremos a números primos de 1.ª espécie em $Q(\vartheta)$. No entretanto, logo a seguir generalizaremos a demonstração.

No corpo $Q(\vartheta)$, extensão de grau n de Q, considerado o inteiro $\alpha = g(\vartheta)$, representaremos os conjugados de α por $\alpha^{(i)} = g(\vartheta^{(i)})$, onde os $\vartheta^{(i)}$ são os conjugados de ϑ.

Norma de α é o número racional inteiro

$$N(\alpha) = g(\vartheta) \cdot g(\vartheta^{(1)}) \cdot \ldots \cdot g(\vartheta^{(n-1)}).$$

LEMA 1. *Sendo* f_i *o grau de* $L_i(x)$ *e* $\psi(x)$ *um polinómio com coeficientes em* Z, *vale*

$$N(L_i(\vartheta)) = (-1)^{nf_i} \cdot p^{f_i} \cdot \psi(\lambda_1) \cdot \ldots \cdot \psi(\lambda_{f_i}).$$

DEMONSTRAÇÃO. Seja $L_i(x) = (x-\lambda_1) \cdot (x-\lambda_2) \cdot \ldots \cdot (x-\lambda_{f_i})$. Então $N(L_i(\vartheta)) = L_i(\vartheta) \cdot L_i(\vartheta^{(1)}) \cdot \ldots \cdot L_i(\vartheta^{(n-1)}) = (\vartheta-\lambda_1) \cdot \ldots \cdot (\vartheta-\lambda_{f_i}) \cdot (\vartheta^{(1)}-\lambda_1) \cdot \ldots \cdot (\vartheta^{(1)}-\lambda_{f_i}) \cdot \ldots \cdot (\vartheta^{(n-1)}-\lambda_1) \cdot \ldots \cdot (\vartheta^{(n-1)}-\lambda_{f_i}) = (-1)^{nf_i} \cdot f(\lambda_1) \cdot \ldots \cdot f(\lambda_{f_i})$. Mas sendo $f(x) \equiv |L_1(x)|^{e_1} \cdot \ldots \cdot |L_g(x)|^{e_g} \pmod p$, isto é, $f(x) = |L_1(x)|^{e_1} \cdot \ldots \cdot |L_g(x)|^{e_g} + p \cdot \psi(x)$, com $\psi(x)$ um polinómio com coeficientes em Z, temos

$$f(\lambda_1) \cdot \ldots \cdot f(\lambda_{f_i}) = p^{f_i} \cdot \psi(\lambda_1) \cdot \ldots \cdot \psi(\lambda_{f_i})$$

e portanto

$$N(L_i(\vartheta)) = (-1)^{nf_i} \cdot p^{f_i} \cdot \psi(\lambda_1) \cdot \ldots \cdot \psi(\lambda_{f_i}).$$

COROLÁRIO. $N(L_i(\vartheta)) \equiv 0 \pmod{p^{f_i}}$ (+).

LEMA 2. *Condição necessária e suficiente para que* $p / N(\alpha)$, *onde* $\alpha = g(\vartheta)$, *é que* $g(x)$ *contenha como factor ao menos uma das funções* $L_i(x)$ *mod* p.

DEMONSTRAÇÃO. Suponhamos que $f(x)$ e $g(x)$ não tenham factores comuns mod p. Então é possível determinar polinómios $\Phi(x)$ e $\psi(x)$ tais que $g(x) \cdot \Phi(x) - \psi(x) \cdot f(x) \equiv 1 \pmod p$. Então $g(x) \cdot \Phi(x) - \psi(x) \cdot f(x) = 1 + p \cdot \chi(x)$, com $\chi(x)$ com coeficientes racionais inteiros, e daí

$$g(\vartheta) \cdot \Phi(\vartheta) = 1 + p \cdot \chi(\vartheta), \ldots, g(\vartheta^{(n-1)}) \cdot \Phi(\vartheta^{(n-1)}) = 1 + p \cdot \chi(\vartheta^{(n-1)})$$

e multiplicando membro a membro $N(\alpha) \cdot N(\Phi(\vartheta)) = 1 + p \cdot m$ onde m é um número racional inteiro. Logo, $N(\alpha) \cdot N(\Phi(\vartheta)) \equiv 1 \pmod p$ isto é, $N(\alpha)$ não é divisível por p, e a condição é necessária.

(+) Isto decorre, também, do facto de ser $\mathfrak{P}_i = (L_i(\vartheta), p)$ e $N(\mathfrak{P}_i) = p^{f_i}$, pois $N(\mathfrak{P}_i) / N(L_i(\vartheta))$.

Seja agora $g(x) \equiv L_i(x) \cdot \Phi(x) \pmod p$. Então, sendo $\psi(x)$ polinómio com coeficientes em Z temos

$$g(x) = L_i(x) \cdot \Phi(x) + p \cdot \psi(x),$$

logo

$$g(\theta) = L_i(\theta) \cdot \Phi(\theta) + p \cdot \psi(\theta), \cdots, g(\theta^{(n-1)}) = \\ = L_i(\theta^{(n-1)}) \cdot \Phi(\theta^{(n-1)}) + p \cdot \psi(\theta^{(n-1)})$$

e multiplicando $N(\alpha) = N(L_i(\theta)) \cdot N(\Phi(\theta)) + \\ + p \cdot m$, $m \in Z$, e sendo $N(L_i(\theta)) \equiv 0 \pmod p$, temos $N(\alpha) \equiv 0 \pmod p$.

Teorema. *Condição necessária e suficiente para que* f(x) *admita factores múltiplos mod* p *é que* p/d.

Sabemos que uma base de $Q(\theta)$ é a base natural $1, \theta, \theta^2, \cdots, \theta^{n-1}$ e que seu discriminante é o quadrado do determinante de Vandermonde [1, pág. 17]

$$V(\theta, \theta^{(1)}, \cdots, \theta^{(n-1)}) = \\ = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^{(1)} & \cdots & \theta^{(n-1)} \\ \theta^2 & |\theta^{(1)}|^2 & \cdots & |\theta^{(n-1)}|^2 \\ \cdots & \cdots & \cdots & \cdots \\ \theta^{n-1} & |\theta^{(1)}|^{n-1} & \cdots & |\theta^{(n-1)}|^{n-1} \end{vmatrix}$$

Então

$$D(1, \theta, \cdots, \theta^{(n-1)}) = (\theta^{(1)} - \theta)^2 \cdot \\ \cdot (\theta^{(2)} - \theta)^2 \cdot \cdots \cdot (\theta^{(n-1)} - \theta)^2 \cdot \\ \cdot (\theta^{(2)} - \theta^{(1)})^2 \cdot \cdots \cdot (\theta^{(n-1)} - \theta^{(1)})^2 \cdot \\ \cdot (\theta^{(n-1)} - \theta^{(n-2)})^2$$

e $D = J^2 \cdot d$. Supondo que p seja de 1.ª espécie, temos que p/d é equivalente a p/D.

Suponhamos que $p \nmid D$ e que $f(x)$ admita $L_i(x)$ como factor múltiplo mod p, isto é, que $e_i \geq 1$; então $f(x) = \Phi(x) \cdot |L_i(x)|^{e_i} + \\ + p \cdot \psi(x)$ com $\Phi(x)$ e $\psi(x)$ polinómios com coeficientes em Z. Derivando temos

$$f'(x) = \Phi'(x) \cdot |L_i(x)|^{e_i} + e_i |L_i(x)|^{e_i - 1} \cdot \\ \cdot L_i'(x) \cdot \Phi(x) + p \cdot \psi'(x),$$

isto é

$$f'(x) \equiv \chi(x) \cdot L_i(x) \pmod p$$

onde

$$\chi(x) = \Phi'(x) \cdot |L_i(x)|^{e_i - 1} + \\ + e_i |L_i(x)|^{e_i - 2} \cdot L_i'(x) \cdot \Phi(x),$$

e pelo lema 2, temos $N(f'(\theta)) \equiv 0 \pmod p$. $f'(\theta)$ é denominado *diferente de* θ, e é um elemento de $Q(\theta)$ [7, pág. 11].

Sendo

$$f(x) = (x - \theta) \cdot (x - \theta^{(1)}) \cdot \cdots \cdot (x - \theta^{(n-1)})$$

temos

$$f'(x) = (x - \theta^{(1)}) \cdot \cdots \cdot (x - \theta^{(n-1)}) + (x - \theta) \cdot \\ \cdot (x - \theta^{(2)}) \cdot \cdots \cdot (x - \theta^{(n-1)}) + \cdots + (x - \theta) \cdot \\ \cdot (x - \theta^{(1)}) \cdot \cdots \cdot (x - \theta^{(n-2)}),$$

logo

$$f'(\theta) = (\theta - \theta^{(1)}) \cdot \cdots \cdot (\theta - \theta^{(n-1)}) \cdot \cdots \\ \cdot f'(\theta^{(n-1)}) = (\theta^{(n-1)} - \theta) \cdot \cdots \cdot (\theta^{(n-1)} - \theta^{(n-2)}),$$

e $N(f'(\theta)) = (-1)^{\frac{n(n-1)}{2}} \cdot D$. Mas, então, como $N(f'(\theta)) \equiv 0 \pmod p$, temos p/D, contra a hipótese inicial. Logo, se $p \nmid D$, temos $e_i = 1$, isto é, $f(x)$ não contém factores múltiplos mod p.

Seja agora p/D. Suponhamos que

$$e_i = 1, (i = 1, 2, \cdots, g),$$

isto é, que $f(x) \equiv L_1(x) \cdot L_2(x) \cdot \cdots \cdot L_g(x) \pmod p$. Eentão $f(x) = L_1(x) \cdot \cdots \cdot L_g(x) + \\ + p \cdot \Phi(x)$ e

$$f'(x) = L_1'(x) \cdot L_2(x) \cdot \cdots \cdot L_g(x) + \\ + \cdots + L_1(x) \cdot \cdots \cdot L_g'(x) + p \cdot \Phi'(x)$$

logo $f'(x)$ não contém como factor nenhum $L_i(x)$, e pelo lema 2, $p \nmid N(f'(\theta))$, e portanto $p \nmid D$, contra a hipótese. Então, se p/D, $f(x)$ deve conter factores múltiplos mod p, o que demonstra completamente o teorema.

Como a ordem de ramificação de $L_i(x)$ em $f(x)$ é a ordem de ramificação de $\mathfrak{P}_i$ em (p), temos demonstrado o teorema enunciado no início deste parágrafo, mas apenas para números primos racionais de 1.ª espécie em $Q(\theta)$.

Vamos agora completar a demonstração para números primos racionais quaisquer.

Se p/d, temos p/D, independentemente de ser p de 1.ª ou de 2.ª espécie, e a demonstração feita subsiste, logo a condição suficiente do teorema de DEDEKIND fica completamente demonstrada. No entanto, para demonstrar que a condição é necessária, este raciocínio falha se p é primo de 2.ª espécie.

Para demonstrar a condição necessária, isto é, se $\mathfrak{P}^2/(p)$, então p/d, utilizaremos o seguinte

LEMA. *Sendo* $Q(\theta)$ *extensão de grau* n *de* Q, *e* γ *um inteiro de* $Q(\theta)$, *temos* $|T(\gamma)|^p \equiv T(\gamma^p) \pmod{p}$ (+).

DEMONSTRAÇÃO. Sendo $T(\gamma) = \gamma^{(1)} + \cdots + \gamma^{(n)}$, temos $|T(\gamma)|^p = |\gamma^{(1)} + \cdots + \gamma^{(n)}|^p \pmod{p}$. Mas $T(\gamma^p) = |\gamma^{(1)}|^p + \cdots + |\gamma^{(n)}|^p$, logo $|T(\gamma)|^p \equiv T(\gamma^p) \pmod{p}$.

Seja $\mathfrak{P}^2/(p)$; então $(p) = \mathfrak{P}^2 \cdot \mathfrak{Q}$. Seja α um inteiro do corpo tal que $\mathfrak{P} \cdot \mathfrak{Q}/\alpha$ e $\mathfrak{P}^2 \cdot \mathfrak{Q} \nmid \alpha$; existem inteiros assim pois $\mathfrak{P} \cdot \mathfrak{Q}/\mathfrak{P}^2 \cdot \mathfrak{Q}$. Então temos $\alpha \not\equiv 0$ (senão $\alpha \in \mathfrak{P}^2 \cdot \mathfrak{Q}$) e $p \nmid \alpha$ (senão $\mathfrak{P}^2/\alpha$). Também p/α^2, pois $(p)/\mathfrak{P}^2 \cdot \mathfrak{Q}/\mathfrak{P}^2 \cdot \mathfrak{Q}^2/(\alpha)^2/(\alpha^2)$. Sendo $p \geqq 2$, e ω um inteiro do corpo, temos sempre $\alpha^2/(\alpha \cdot \omega)^p$, logo $p/(\alpha \cdot \omega)^p$, ou seja $(\alpha \cdot \omega)^p/p$ é inteiro do corpo. Então $T((\alpha \cdot \omega)^p/p) = T((\alpha \cdot \omega)^p)/p$ é racional inteiro, ou seja, $T((\alpha \cdot \omega)^p) \equiv 0 \pmod{p}$. Mas sendo $\alpha \cdot \omega$ inteiro do corpo, pelo lema temos $T((\alpha \cdot \omega)^p) \equiv |T(\alpha \cdot \omega)|^p \pmod{p}$ e daí $|T(\alpha \cdot \omega)|^p \equiv 0 \pmod{p}$. Mas como $T(\alpha \cdot \omega)$ é racional inteiro, é $T(\alpha \cdot \omega) \equiv 0 \pmod{p}$.

Seja agora $\Omega_1, \cdots, \Omega_n$ uma base inteira de $Q(\theta)$. Então $\alpha = h_1 \cdot \Omega_1 + \cdots + h_n \cdot \Omega_n$, com os h_i inteiros racionais, nem todos divisíveis por p, senão p/α. Logo

$$T(\alpha \cdot \Omega_l) = T\left(\sum_1^n{}_i h_i \cdot \Omega_i \cdot \Omega_l\right) = \sum_1^n{}_i h_i \cdot T(\Omega_i \cdot \Omega_l),$$

e então

$$\sum_1^n{}_i h_i \cdot T(\Omega_i \cdot \Omega_l) \equiv 0 \pmod{p}.$$

Sendo h_i e $T(\Omega_i \cdot \Omega_l)$ racionais inteiros, e pelo menos um $h_i \not\equiv 0 \pmod{p}$, temos

$$|T(\Omega_i \cdot \Omega_l)| \equiv 0 \pmod{p},$$

e como $|T(\Omega_i \cdot \Omega_l)| - d$ resulta $d \equiv 0 \pmod{p}$, o que demonstra o teorema.

(+) $T(\gamma)$ é o *traço* de γ, inteiro do corpo, definido como $T(\gamma) = \gamma^{(1)} + \cdots + \gamma^{(n)}$, onde $\gamma^{(i)}$ são os conjugados de γ. [1, pág. 4].

BIBLIOGRAFIA

[1] FURQUIM DE ALMEIDA, FERNANDO, *Teoria dos Números Algébricos*, Primeiro Colloq. Bras. de Matem., C. N. Pq., S. Paulo, 1957.

[2] LANDAU, EDMUND, *Vorlesungen über Zahlentheorie*, vol. III (1927), New York, 1955.

[3] FRICKE, ROBERT, *Lehrbuch der Algebra*, vol III, Braunschweig 1928.

[4] DEDEKIND, RICHARD, *Über den Zusammenhang zwischem der Theorie der Ideale und der Theorie der höherem Kongruenzen* (1878), Gesammelte Mathem. Werke, vol. I, Braunschweig, 1930.

[5] DEDEKIND, RICHARD, *Über die Diskriminanten endlicher Körper* (1882), Gesam. Mathem. Werke, vol. I, Braunschweig, 1930.

[6] ZOLOTAREFF, G., *Sur la théorie des Nombres Complexes*, I, Journal de Mathématiques Pures et Appliquées, tome VI, pág. 51, 1880.

[7] HILBERT, DAVID, *Théorie des Corps de Nombres Algébriques*, (1897), Paris, 1913.