Teoria dos Números Algébricos

Textuniversitários 35

Alfredo R. Jones

Teoria dos Números *Algébricos*

Editora Livraria da Física
São Paulo — 2025

1a. Edição

Editor: Victor Pereira Marinho / José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

Texto em conformidade as regras ortográficas do Acordo da Língua Portuguesa (AO90).

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Jones, Alfredo R.
Teoria dos números algébricos / Alfredo R. Jones. –– São Paulo : LF Editorial, 2025. –– (Textuniversitários ; 35)

Bibliografia.
ISBN 978-65-5563-662-8

1. Teoria dos números I. Título. II. Série.

25-308981.0 CDD–512.7

Índices para catálogo sistemático:

1. Teoria dos números : Matemática 512.7

Eliete Marques da Silva – Bibliotecária – CRB-8/9380

Impresso no Brasil
Printed in Brazil

www.lfeditorial.com.br
Visite nossa livraria no Instituto de Física da USP
www.livrariadafisica.com.br
Telefones:
(11) 2648-6666 | Loja do Instituto de Física da USP
(11) 3936-3413 | Editora

Prefácio

O Instituto de Matemática e Estatística da Universidade de São Paulo, IME–USP (hoje Instituto de Matemática, Estatística e Ciência da Computação) foi criado pela reforma universitária de 1969 e começou a exercer suas funções no ano seguinte.

O Prof. Alfredo Jones, autor deste texto, chegou ao IME–USP, como professor visitante, justamente no segundo semestre desse mesmo ano, quando ministrou uma disciplina sobre Representações de Grupos Finitos, sua área de pesquisa. Em visitas subsequentes, ministrou outras disciplinas avançadas: Representações de Álgebras, Módulos sobre Ordens e Teoria dos Números Algébricos. A partir de 1973, ele se tornou professor permanente do IME–USP; em 1985, foi aprovado em concurso para professor titular e, no ano seguinte, finalmente se aposentou da USP e retornou ao Uruguai, seu país de origem, onde continuou por muitos anos suas atividades docentes. Sem sombra de dúvidas, sua presença em São Paulo foi determinante para a formação do grupo de pesquisa em Álgebra, que hoje atua em múltiplas direções e certamente é um dos mais ativos da América Latina.

O Prof. Jones obteve seu doutorado em 1962 na Universidade de Illinois, em Urbana-Champaign, orientado por Irving Reiner, um dos nomes mais expressivos na teoria de Representações de Grupos. Aliás, pode ser interessante observar que a referência mais importante da área, o livro *Representation Theory of Finite Groups and Associative Algebras*, de C. W. Curtis e I. Reiner, foi publicada no mesmo ano

em que o Prof. Jones obteve seu doutoramento e foi feito um esforço especial para incluir na obra, já em fase de impressão, o resultado principal de sua tese. Este é apresentado como o Teorema (81.18), a ele atribuído, e é classificado como um *"striking result"*.

Após um breve retorno ao Uruguai, voltou aos Estados Unidos como professor visitante da universidade de Cornell onde permaneceu por quase três anos e onde ministrou pela primeira vez um curso sobre a Teoria de Números Algébricos, que, anos depois, voltou a ministrar algumas vezes no IME–USP e cujas notas deram origem ao presente livro. O texto foi escrito para leitores que já têm uma boa maturidade em álgebra. Desde o início, os assuntos são tratados na maior generalidade e abstração possível, mas o estilo cuidadoso e elegante do autor torna a leitura acessível e muito agradável. Sua edição em forma de livro é certamente uma contribuição importante para a literatura matemática em português.

Os assinantes deste prefácio fizeram, em épocas distintas, o curso do professor Alfredo Jones, cujas notas deram origem a este livro.

César Polcino Milies
Eduardo do Nascimento Marcos
São Paulo, outubro de 2025

Sumário

I

Domínios de Dedekind

Para desenvolver uma aritmética nos corpos de números algébricos, começaremos introduzindo a noção de elemento inteiro de um corpo de números algébricos. Mostraremos que, com uma definição adequada de inteiro, em todo corpo de números algébricos, o conjunto de seus inteiros forma um anel. Neste anel, em geral, não vale a fatoração única em elementos primos, mas todo ideal do anel de inteiros admite uma fatoração única em produto de ideais primos. Este resultado fundamental, que demonstraremos na seção 3 deste capítulo, é o ponto de partida para o estudo da aritmética dos corpos de números algébricos.

1 Inteiros

Todos os anéis considerados serão comutativos e com identidade. Dados dois anéis R e S, escreveremos $R \subset S$ se R é um subanel de S com a mesma identidade que S. Se C é um conjunto qualquer de elementos de S, indicaremos com $R[C]$ o subanel de S gerado por R e o conjunto C.

Definição. Um elemento $\alpha \in S$ diz-se *inteiro* sobre um subanel R de S se é raiz de um polinômio com coeficientes em R e coeficiente inicial 1, ou seja,

$$x^m + a_1 x^{m-1} + \cdots + a_m \in R[x].$$

Lema 1. *As seguintes afirmações são equivalentes:*

1. *O elemento $\alpha \in S$ é inteiro sobre R.*

2. *Existe um inteiro $m > 0$ para o qual*

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{m-1}.$$

3. *Existe um módulo fiel M sobre $R[\alpha]$ que é finitamente gerado como módulo sobre R.*

PROVA. $1 \to 2$. Se $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$, com $a_i \in R$, então $\alpha^m \in R + \cdots + R\alpha^{m-1}$. Logo,

$$\alpha^{m+1} \in R\alpha + \cdots + R\alpha^m \subset R + \cdots + R\alpha^{m-1}.$$

Assim, mostra-se que $\alpha^j \in R + \cdots + R\alpha^{m-1}$ para todo j, portanto $R[\alpha] \subset R + \cdots + R\alpha^{m-1}$.

$2 \to 3$. É claro que, se vale 2, o próprio $R[\alpha]$ é um módulo fiel sobre $R[\alpha]$ que é finitamente gerado sobre R.

$3 \to 1$. Sejam $x_1, \ldots, x_t$ geradores de M sobre R, isto é, $M = Rx_1 + \cdots + Rx_t$. Como para todo x_i se tem $\alpha x_i \in M$, existem $a_{ij} \in R$ tais que

$$\alpha x_i - (a_{i1}x_1 + \cdots + a_{it}x_t) = 0 \quad \text{para} \quad i = 1, \ldots, t. \qquad (*)$$

Seja agora I a matriz identidade de dimensões $t \times t$ e T a matriz $t \times t$ sobre $R[\alpha]$ definida por:

$$T = \alpha I - (a_{ij}).$$

Sabe-se que, se T^* é a transposta da matriz dos cofatores de T, então $T^*T = (\det T)I$. Escrevendo o sistema de igualdades $(*)$ com notação matricial e multiplicando pela matriz T^*, resulta:

$$(\det T)x_i = 0 \quad \text{para} \quad i = 1, \ldots, t.$$

Como $x_1, \ldots, x_t$ geram M, deduz-se que $(\det T)M = 0$. Logo, $\det T = 0$, pois M é fiel sobre $R[\alpha]$. Portanto, α é raiz do polinômio com coeficientes em R e coeficiente inicial 1:

$$\det(XI - (a_{ij})).$$

□

Definição. Um *anel* S diz-se *inteiro* sobre um subanel R se todo elemento de S é inteiro sobre R.

Lema 2. *Se C é um conjunto de elementos inteiros sobre R, então o anel $R[C]$ é inteiro sobre R.*

Prova. Para cada $\alpha \in R[C]$, existe um conjunto finito $c_1, \ldots, c_t$ de elementos de C tal que

$$\alpha \in R[c_1, \ldots, c_t].$$

Como c_j é inteiro sobre R, pelo Lema 1, $R[c_j]$ é gerado por um conjunto finito de potências de c_j como módulo sobre R. Consequentemente, $R[c_1, \ldots, c_t]$ é gerado por um conjunto finito de produtos da forma $c_1^{i_1} \cdots c_t^{i_t}$ como módulo sobre R. Como $R[c_1, \ldots, c_t]$ é um módulo fiel sobre $R[\alpha]$, o mesmo lema mostra que α é inteiro sobre R. □

Proposição 1. *Se $R \subset S$, o conjunto C dos elementos de S que são inteiros sobre R é um subanel de S.*

Prova. Do último lema segue que $R[C] \subset C$, logo $C = R[C]$. □

Proposição 2. *Dados três anéis $A \subset R \subset S$, se S é inteiro sobre R e R é inteiro sobre A, então S é inteiro sobre A.*

Prova. Dado $\alpha \in S$, existem $c_1, \ldots, c_m$ em R tais que

$$\alpha^m + c_1\alpha^{m-1} + \cdots + c_m = 0.$$

Logo,

$$A[c_1, \ldots, c_m, \alpha] = \sum_{i=0}^{m-1} A[c_1, \ldots, c_m]\alpha^i.$$

Como vimos na demonstração do Lema 2, $A[c_1, \ldots, c_m]$ é finitamente gerado sobre A. Portanto, da igualdade acima segue que $A[c_1, \ldots, c_m, \alpha]$ é finitamente gerado sobre A. Daqui, pelo Lema 1, concluímos que α é inteiro sobre A. □

Definição. O anel C introduzido na Proposição 1 chama-se o *fecho integral* de R em S.

Diz-se que R é *integralmente fechado* em S quando o fecho integral de R em S coincide com R.

Um domínio de integridade diz-se *integralmente fechado* se é integralmente fechado em seu corpo de frações.

Consideremos três anéis $A \subset R \subset S$. Se R é inteiro sobre A, então, pela Proposição 2, o fecho integral de R em S coincide com o fecho integral de A em S.

Em particular, resulta que se R é o fecho integral de A em S, então R é integralmente fechado em S.

É fácil provar que *todo domínio fatorial é integralmente fechado*. Com efeito, seja $\frac{a}{b}$ um elemento do corpo de frações do domínio fatorial A, com $a, b \in A$ e $b \neq 0$. Se $\frac{a}{b}$ é inteiro sobre A, existem $a_1, \ldots, a_m$ em A de modo que

$$\frac{a^m}{b^m} + a_1\frac{a^{m-1}}{b^{m-1}} + \cdots + a_m = 0,$$

logo

$$a^m + a_1a^{m-1}b + \cdots + a_mb^m = 0.$$

Daqui segue que se p é um elemento irredutível de A que divide b, então p divide a e

$$\left(\frac{a}{p}\right)^m + a_1\left(\frac{a}{p}\right)^{m-1}\left(\frac{b}{p}\right) + \cdots + a_m\left(\frac{b}{p}\right)^m = 0.$$

Logo, o raciocínio feito para $\frac{a}{b}$ pode-se repetir para $\frac{a}{p}$ e para $\frac{b}{p}$. Assim, por indução sobre o número de fatores irredutíveis de b, prova-se que b divide a e portanto $\frac{a}{b} \in A$.

Proposição 3. *Se R é um domínio de integridade com corpo de frações K e E é uma extensão algébrica de K, todo elemento de E é da forma $\frac{\beta}{a}$, onde $\beta \in E$ é inteiro sobre R e $a \in R$.*

Prova. Todo $\alpha \in E$ é algébrico sobre K, logo, como K é um corpo de frações de R, existem $a, a_1, \ldots, a_m$ em R tais que

$$a\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0,$$

donde

$$(a\alpha)^m + a_1(a\alpha)^{m-1} + \cdots + a^{m-1}a_m = 0.$$

Logo, $\beta = a\alpha$ é inteiro sobre R. □

Esta proposição mostra que toda extensão algébrica de K é um corpo de frações do fecho integral de R em E.

Se E é uma extensão finita e separável de K, então E é uma extensão simples de K, isto é, $E = K(\alpha)$ para algum $\alpha \in E$. Escrevendo $\alpha = \frac{\beta}{a}$, com β inteiro sobre R e $a \in R$, obtém-se $E = K(\beta)$.

Definição. Um *número algébrico* é um número complexo que é algébrico sobre $\mathbb{Q}$. Um *inteiro algébrico* é um número complexo inteiro sobre $\mathbb{Z}$.

Chama-se *corpo de números algébricos* todo corpo que é uma extensão finita de $\mathbb{Q}$.

Vejamos como se aplicam os resultados anteriores aos corpos de números algébricos.

Consideremos um corpo de números algébricos K e uma extensão finita E de K. Seja R o anel dos inteiros algébricos de K e S o anel dos inteiros algébricos de E.

É imediato que $R = S \cap K$. Por outro lado, $\mathbb{Z} = R \cap \mathbb{Q}$, pois $\mathbb{Z}$ é integralmente fechado, já que é fatorial.

Pela Proposição 2, R é integralmente fechado em K e S é integralmente fechado em E. Aplicando a Proposição 2 aos anéis $\mathbb{Z} \subset R \subset E$, resulta que o fecho integral de R em E é S. A Proposição 3 mostra que K é um corpo de frações de R e E é um corpo de frações de S.

É usual chamar de *inteiro de um corpo de números algébricos* K a qualquer elemento do anel R dos inteiros algébricos de K. Nesse caso, os inteiros de $\mathbb{Z}$ chamam-se inteiros racionais. Esta denominação se justifica pela igualdade $\mathbb{Z} = \mathbb{R} \cap \mathbb{Q}$.

Dado um corpo F, notaremos com $F(X)$ o *corpo de frações do anel de polinômios* $F[X]$.

Definição. Chama-se *corpo de funções algébricas* em uma variável sobre o corpo F toda extensão finita K de $F(X)$.

Para os corpos de funções algébricas, valem observações análogas às feitas para os corpos de números algébricos, pois as demonstrações acima continuam válidas trocando $\mathbb{Z}$ por $F[X]$ e $\mathbb{Q}$ por $F(X)$, já que $F[X]$ também é um domínio fatorial. O anel dos inteiros do corpo de funções algébricas K é o fecho integral R de $F[X]$ em K, e $F[X] = R \cap F(X)$.

Se α é um elemento algébrico sobre um corpo K, indicamos com $\mathrm{Irr}(\alpha, K)$ o *polinômio irredutível em* $K[X]$ *com coeficiente inicial* 1 *que tem raiz* α. A última proposição desta seção mostra que, para saber se α é inteiro sobre um domínio R, integralmente fechado no seu corpo de frações K, é suficiente considerar o polinômio $\mathrm{Irr}(\alpha, K)$.

Proposição 4. *Seja R um domínio integralmente fechado e K seu corpo de frações. Um elemento α algébrico sobre K é inteiro sobre R se e somente se* $\mathrm{Irr}(\alpha, K) \in R[X]$.

Prova. Se α é inteiro sobre R, existe $f \in R[X]$ com coeficiente inicial 1 e com raiz α. Este polinômio é então um múltiplo de $\mathrm{Irr}(\alpha, K)$, logo as raízes de $\mathrm{Irr}(\alpha, K)$ são raízes de f, e, portanto, são inteiras sobre R. Em consequência, os coeficientes de $\mathrm{Irr}(\alpha, K)$, que são funções

simétricas elementares nas raízes, também são inteiros sobre R. Mas R é integralmente fechado em K, logo $\mathrm{Irr}(\alpha, K) \in R[X]$. □

Exercícios

1. Mostrar que $\frac{1}{2}(1+\sqrt{5})$ é um inteiro algébrico.
2. Mostrar que o fecho integral de $\mathbb{Z}$ em $\mathbb{Q}(\sqrt{-5})$ é $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.
3. Seja $\alpha \neq 0$ um inteiro algébrico e seja $f = \mathrm{Irr}(\alpha, \mathbb{Q})$. Provar que $\frac{1}{\alpha}$ é um inteiro algébrico se e só se $f(0) = \pm 1$.
4. Mostrar que da demonstração do lema 1 resulta que toda matriz é raiz do seu polinômio característico.
5. Considerar $\mathbb{Z} \subset M_2(\mathbb{Q})$ (anel das matrizes 2 por 2 sobre $\mathbb{Q}$) identificando cada inteiro m com a matriz mI. Mostrar que as matrizes:

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix}$$

são inteiras sobre $\mathbb{Z}$, mas $\alpha+\beta$ não é inteira sobre $\mathbb{Z}$.

2 Bases inteiras

Lembraremos as definições e as principais propriedades do discriminante e das funções norma e traço de uma álgebra sobre um corpo.

Seja A uma álgebra sobre um corpo K, de dimensão finita, $n = \dim_K A$. Para cada $\alpha \in A$, consideraremos a transformação linear $\overline{\alpha} : A \to A$ determinada pela multiplicação por α, isto é, $\overline{\alpha}(x) = \alpha x$.

Definição. Chama-se *polinômio característico* de α o seguinte polinômio de $K[X]$:

$$\chi_{A/K}(\alpha) = \det(XI - \overline{\alpha}) = X^n + c_1 X^{n-1} + \cdots + c_n.$$

Chama-se *norma* de α o determinante de $\overline{\alpha}$:

$$N_{A/K}(\alpha) = \det \overline{\alpha} = (-1)^n c_n,$$

e *traço* de α o traço de $\overline{\alpha}$:

$$\mathrm{Tr}_{A/K}(\alpha) = \mathrm{tr}\,\overline{\alpha} = -c_1.$$

1. Mostra-se facilmente que a função norma é um homomorfismo multiplicativo, $N_{A/K} : A \to K$, e que a função traço é um homomorfismo aditivo, $\mathrm{Tr}_{A/K} : A \to K$.

2. Se $\alpha \in K$, é imediato que

$$N_{A/K}(\alpha) = \alpha^{(\dim_K A)} \quad \text{e} \quad \mathrm{Tr}_{A/K}(\alpha) = (\dim_K A)\alpha.$$

3. Prova-se (ver [ZS], II.10) que se A é uma álgebra de dimensão finita sobre um corpo F e F é uma extensão finita de K, então

$$N_{A/K}(\alpha) = N_{F/K}\left(N_{A/F}(\alpha)\right) \quad \text{e} \quad \mathrm{Tr}_{A/K}(\alpha) = \mathrm{Tr}_{F/K}\left(\mathrm{Tr}_{A/F}(\alpha)\right).$$

4. De 2 e 3 segue que se E é um corpo que é uma extensão finita de K, então para todo $\alpha \in E$:

$$N_{E/K}(\alpha) = N_{K(\alpha)/K}\left(N_{E/K(\alpha)}(\alpha)\right) = N_{K(\alpha)/K}(\alpha)^{(\dim_{K(\alpha)})E}.$$

   Analogamente, obtém-se:

$$\mathrm{Tr}_{E/K}(\alpha) = \left(\dim_{K(\alpha)} E\right) \mathrm{Tr}_{K(\alpha)/K}(\alpha).$$

5. Se o corpo E é uma extensão simples de K, $E = K(\alpha)$, a matriz de $\overline{\alpha}$ em relação à base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ de E sobre K é a matriz companheira do polinômio minimal $\mathrm{Irr}(\alpha, K) = X^n + a_1 X^{n-1} + \cdots + a_n$, dada por:

$$U = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

A partir disso, calculando o determinante de $XI - U$, deduz-se que:

$$\begin{aligned}\chi_{K(\alpha)/K}(\alpha) &= \mathrm{Irr}(\alpha, K) = (X - \alpha_1)\cdots(X - \alpha_n),\\ N_{K(\alpha)/K}(\alpha) &= (-1)^n a_n = \alpha_1 \cdots \alpha_n,\\ \mathrm{Tr}_{K(\alpha)/K}(\alpha) &= -a_1 = \alpha_1 + \cdots + \alpha_n.\end{aligned}$$

Se α é separável sobre K, as raízes de $\mathrm{Irr}(\alpha, K)$ são todas distintas. Por outro lado, se α não é separável, a característica de K é um primo p, e todas as raízes têm a mesma multiplicidade $p^e > 1$. Portanto, nesse caso, pode-se escrever:

$$N_{K(\alpha)/K}(\alpha) = (\alpha_1 \cdots \alpha_s)^{p^e}$$

e

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = p^e(\alpha_1 + \cdots + \alpha_s) = 0.$$

6. Dado um corpo E, extensão finita de K, seja F a maior extensão separável de K contida em E, e seja $p^f = \dim_F E$. Usando os resultados 4 e 5, prova-se (ver [ZS]) que se $\sigma_1, \ldots, \sigma_s$ são os K-isomorfismos de E em uma extensão algebricamente fechada de E, então, para todo $\alpha \in E$:

$$N_{E/K}(\alpha) = (\sigma_1(\alpha) \cdots \sigma_s(\alpha))^{p^f}$$

e

$$\mathrm{Tr}_{E/K}(\alpha) = p^f\left(\sigma_1(\alpha) + \cdots + \sigma_s(\alpha)\right).$$

7. De 6 resulta imediatamente que, se E é uma extensão não separável de K, então $\mathrm{Tr}_{E/K}(\alpha) = 0$ para todo $\alpha \in E$.

Nosso próximo objetivo é estudar a função bilinear $\varphi : A \times A \to K$ definida por $\varphi(x, y) = \mathrm{Tr}_{A/K}(xy)$. Para isso, consideraremos primeiro uma função bilinear qualquer $\varphi : A \times A \to K$. Lembramos que φ é dita *degenerada* se existe $v \in A$, $v \neq 0$, tal que $\varphi(v, \alpha) = 0$ para todo $\alpha \in A$.

Definição. Dados $\alpha_1, \ldots, \alpha_n$ em A, com $n = \dim_K A$, chama-se *discriminante* de $\alpha_1, \ldots, \alpha_n$ com relação a uma função bilinear φ o determinante da matriz $(\varphi(\alpha_i, \alpha_j))$. Notação: $d_\varphi(\alpha_1, \ldots, \alpha_n)$.

É simples mostrar que se o conjunto $\alpha_1, \ldots, \alpha_n$ é linearmente dependente sobre K, então $d_\varphi(\alpha_1, \ldots, \alpha_n) = 0$ qualquer que seja a função bilinear φ (Exercício 1), de modo que só interessa considerar os discriminantes das bases de A sobre K.

Lema 1. *Se existe uma base $\alpha_1, \ldots, \alpha_n$ de A sobre K tal que*

$$d_\varphi(\alpha_1, \ldots, \alpha_n) = 0,$$

então φ é degenerada, e se φ é degenerada, o discriminante com relação a φ de toda base de A sobre K é zero.

Prova. Tem-se $\det(\varphi(\alpha_i, \alpha_j)) = 0$ se e só se existem $c_1, \ldots, c_n$ em K, não todos nulos, tais que $\sum_i c_i \varphi(\alpha_i, \alpha_j) = 0$ para todo j. Isto equivale a dizer que existe $\alpha = \sum_i c_i \alpha_i \neq 0$ que verifica $\varphi(\alpha, \alpha_j) = 0$ para todo j e, portanto, $\varphi(\alpha, x) = 0$ para todo $x \in A$. □

Enunciamos o lema que segue sem demonstração, pois se prova facilmente.

Lema 2. *Se $\beta_j = a_{1j}\alpha_1 + \cdots + a_{nj}\alpha_n$, com $a_{ij} \in K$, para $j = 1, \ldots, n$, então:*

$$d_\varphi(\beta_1, \ldots, \beta_n) = \det(a_{ij})^2 d_\varphi(\alpha_1, \ldots, \alpha_n).$$

Aplicaremos esta noção de discriminante a uma álgebra A, de dimensão n sobre um corpo K, e à função bilinear $\varphi : A \times A \to K$ definida por:

$$\varphi(x, y) = \mathrm{Tr}_{A/K}(xy).$$

Neste caso, omitiremos o φ na notação do discriminante e escreveremos $d_{A/K}(a_1, \ldots, a_n)$ ou $d(a_1, \ldots, a_n)$.

Se E é uma extensão separável de um corpo K e $\sigma_1, \ldots, \sigma_n$ são os K-isomorfismos de E em uma extensão algebricamente fechada de K, então verifica-se com um cálculo simples que

$$\big(\mathrm{Tr}_{E/K}(a_i a_j)\big) = \big(\sigma_i(a_j)\big)\,\big(\sigma_i(a_j)\big)^{\mathrm{tr}}.$$

Daqui se obtém a seguinte expressão do discriminante de $a_1, \ldots, a_n$:

$$d(a_1, \ldots, a_n) = \det\big(\sigma_i(a_j)\big)^2.$$

Se $E = K(\alpha)$, escrevendo $\alpha_i = \sigma_i(\alpha)$, resulta:

$$d(1, \alpha, \ldots, \alpha^{n-1}) = \begin{vmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Como $f = \mathrm{Irr}(\alpha, K) = \prod(X - \alpha_i)$, tem-se

$$\begin{aligned} d(1, \alpha, \ldots, \alpha^{n-1}) &= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \sigma_i(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} N_{E/K}(f'(\alpha)). \end{aligned}$$

Chama-se *discriminante do polinômio* f a $d(f) = d(1, \alpha, \ldots, \alpha^{n-1})$.

Os elementos da matriz $(\mathrm{Tr}_{E/K}(\alpha^{i+j}))$ são polinômios simétricos em $\alpha_1, \ldots, \alpha_n$, pois são da forma $\sum_k \alpha_k^{i+j}$. Portanto, podem-se escrever em função dos coeficientes de f. Em particular, é útil anotar os seguintes discriminantes:

- Se $f = X^2 + a_1 X + a_2$, então $d(f) = a_1^2 - 4a_2$.
- Se $f = X^3 + a_1 X^2 + a_2 X + a_3$, então

$$d(f) = a_1^2 a_2^2 - 4a_1^3 a_3 - 4a_2^3 - 27a_3^2 + 18a_1 a_2 a_3.$$

Lema 3. *Dadas duas extensões finitas e separáveis $E \supset F \supset K$, se $\alpha_1, \ldots, \alpha_n$ é uma base de E sobre F e $\beta_1, \ldots, \beta_m$ uma base de F sobre K, então:*

$$|d_{E/K}(\alpha_1\beta_1, \ldots, \alpha_n\beta_1, \ldots, \alpha_n\beta_m)| = \left|N_{F/K}\left(d_{E/F}(\alpha_1, \ldots, \alpha_n)\right)\ \left(d_{F/K}(\beta_1, \ldots, \beta_m)\right)^n\right|.$$

PROVA. Sejam $\sigma_1, \ldots, \sigma_m$ os K-isomorfismos de F em um fecho algébrico Ω de E. Esses isomorfismos podem-se prolongar a K-automorfismos de Ω, que indicaremos com a mesma notação $\sigma_i : \Omega \to \Omega$. Se $\tau_1, \ldots, \tau_n$ são os F-isomorfismos de E em Ω ($\tau_j : E \to \Omega$), então $\sigma_i\tau_j$ ($i = 1, \ldots, m$, $j = 1, \ldots, n$) são os K-isomorfismos de E em Ω. Logo, o discriminante a calcular é, a menos do sinal, o determinante da matriz $(\sigma_i\tau_j(\alpha_k\beta_t))$. Introduzindo os blocos de dimensão n por n,

$$S_i = (\sigma_i\tau_j(\alpha_k)), \quad i = 1, \ldots, m,$$

a matriz anterior pode-se escrever na forma

$$\begin{pmatrix} S_1\sigma_1(\beta_1) & \cdots & S_1\sigma_1(\beta_m) \\ \vdots & \ddots & \vdots \\ S_m\sigma_m(\beta_1) & \cdots & S_m\sigma_m(\beta_m) \end{pmatrix}.$$

Mas esta matriz é o produto

$$\begin{pmatrix} S_1 & & \\ & \ddots & \\ & & S_m \end{pmatrix} \begin{pmatrix} \sigma_1(\beta_1)I & \cdots & \sigma_1(\beta_m)I \\ \vdots & \ddots & \vdots \\ \sigma_m(\beta_1)I & \cdots & \sigma_m(\beta_m)I \end{pmatrix},$$

onde I é a matriz identidade de dimensão n por n, e basta calcular os determinantes destas duas matrizes para obter o resultado desejado. □

Proposição 1. *Seja E uma extensão finita de K. As seguintes propriedades são equivalentes.*

1. *A função bilinear $\mathrm{Tr}_{E/K}(x, y)$ é degenerada.*