

OS TRÊS PROBLEMAS GREGOS DA ANTIGUIDADE, AS CONSTRUÇÕES COM RÉGUA E COMPASSO E A TEORIA DE GALOIS

Arlete Cerqueira Lima*

RESUMO – *Este artigo foi pensado para alunos do Curso de Matemática. Os assuntos que constituem o título tripartido acima se reencontram ao longo da História, do século V antes de Cristo até o século XX. O texto mostra, utilizando a teoria de Galois, que é impossível resolver, com uso exclusivo de régua e compasso, os três problemas gregos da antiguidade: a quadratura do círculo, a duplicação do cubo e a triseção do ângulo.*

ABSTRACT – *This article was conceived for Mathematics students. The topics that form the tripartite title above are commonly found together in History, since the 5th century b.C. up to today. The text demonstrates with the Galois Theory that it is impossible to solve the three ancient Greek problems (quadrature of the circle, duplication of the cube, trisection of the angle) only by using ruler and drawing compass.*

O texto é apresentado sob a forma de um diálogo simulado com o objetivo de minimizar a monotonia ao recordar pré-requisitos importantes em álgebra linear, extensões de corpos, teoria das equações algébricas e teoria dos polinômios. O diálogo se passa numa sala de aula e o material didático é quadro de giz e apagador. A integração entre os três problemas, as construções com régua e compasso e a teoria de Galois é mostrada na fala do professor (P) e dos seus alunos (A). O tratamento é "você-você" entre professor e aluno, que se interrompem e se revezam na utilização do quadro de giz. O texto que fundamentou parte do diálogo foi: Introdução à teoria de Galois, de Kaplansky.

Ao colocar o título da aula no quadro e fazer uma pausa...

A – Quais foram os três grandes problemas gregos da antiguidade, professor?

P – A quadratura do círculo, a duplicação do cubo e a triseção do ângulo.

A – Você poderia dizer para nós em que consiste cada um desses problemas e, se possível, um pouco da história...

P – O estudo sobre os dois primeiros tornou conhecido Hipócrates, contemporâneo do seu ilustre homônimo, o médico Hipócrates de Cós (460–380 a.C.). O problema da quadratura do círculo tinha por objeto construir um quadrado cuja área fosse igual à área de um círculo conhecido e o da duplicação do cubo, construir um cubo cujo volume fosse o dobro do volume de um cubo de aresta dada. O terceiro

* Professor Adjunto do Departamento de Educação da UEFS. Professor Adjunto do Instituto de Matemática da UFBA. Mestre em Matemática pela UFBA.

tornou célebre o sofista Hípias, que viveu na segunda metade do século V a.C. e...

A – Mas, professor, se tomarmos como unidade de comprimento o raio “r” do círculo e a aresta “a” do cubo dados, teremos, indicando respectivamente por x e y o lado do quadrado e a aresta do cubo procurados:

$$x^2 = \pi r^2 \text{ e, portanto, } x = r \sqrt{\pi}$$

$$\text{e } y^3 = 2 a^3 \text{ e, conseqüentemente, } y = a \sqrt[3]{2}$$

Além disso, professor, trissectar um ângulo significa dividi-lo em três partes iguais. E isso é também simples...

P – Um momento! Ainda não tive oportunidade de dizer que tais problemas ficaram célebres pelo fato de ninguém ter conseguido resolvê-los utilizando apenas construções elementares derivadas do emprego exclusivo da régua e do compasso, únicos instrumentos admitidos por Platão em construções geométricas.

É conveniente observar que a régua e o compasso aludidos não podem ser utilizados nessas construções como instrumentos de medida.

A – E foram muitas as tentativas?

P – Para resumir, foram tantas que em 1755, a Academia de Ciências de Paris e mais tarde outros grandes centros matemáticos anunciaram que não examinariam mais papéis sobre a solução dos três problemas mencionados.

A – Mas, dizer que ninguém conseguiu resolver tais problemas equivale a afirmar que alguém demonstrou a impossibilidade de encontrar uma solução para os mesmos...

P – Com o uso exclusivo de régua e compasso.

A – Alguém demonstrou esta impossibilidade?

P – Foi através da teoria de Galois que os matemáticos mostraram que, escolhida uma unidade de comprimento para os segmentos do plano, não se podem construir com régua e compasso os segmentos de comprimento $\sqrt{\pi}$ e $\sqrt[3]{2}$ e que existe um ângulo α tal que $\cos \alpha$ pode ser construído com régua e compasso, mas $\cos(\alpha/3)$ não pode.

A – O título da aula começa agora a ter sentido e estou curioso para saber quem foi Galois!

P – Darei a vocês um esboço rápido da vida deste francês. Ele ficou famoso por sua contribuição à alta álgebra, dando o seu nome à teoria dos grupos de Galois. Apesar de ser um matemático genial, perdeu duas vezes os exames para a Escola Politécnica e, ao entrar para a Escola Normal, dela foi excluído no ano seguinte por suas opiniões políticas. Por uso ilegal de um uniforme e de porte de armas foi sentenciado a 6 meses de cadeia. Morreu em 1832, quando somente com 20 anos, recebeu ferimentos em um duelo, possivelmente com um agente provocador da polícia. Os seus principais trabalhos foram recusados pela academia francesa e sua obra, verdadeiramente genial, mais escondida que publicada em diversas comunicações, só foi reconhecida depois de sua morte. Na noite que precedeu o duelo

resumiu a traços largos na carta a Auguste Chevalier a teoria das equações algébricas, bem como suas conclusões sobre as integrais abelianas, sua classificação e seus períodos, resultados que Riemann estabeleceria 25 anos mais tarde. Naquela memorável noite, Galois deixou as bases para a construção da teoria dos grupos, ou seja, os conceitos fundamentais para o que posteriormente seria a matemática moderna.

A – Puxa, professor! Com 20 anos!

P – É, de fato, inacreditável!

A – Mas, de modo mais concreto, qual a relação dos trabalhos de Galois com os três problemas gregos?

P – Chegaremos lá! Porém, para satisfazer, de modo imediato, à curiosidade de vocês diria que os três problemas estão ligados a seus estudos sobre as equações algébricas e, portanto, à teoria dos polinômios. Desde já chamaria a atenção para os seguintes fatos: Linderman, no século XVIII, demonstrou que não existe uma equação com coeficientes racionais que tenha π como raiz e lembrem-se que $\sqrt{\pi}$ está ligado ao problema da quadratura do círculo; que $\sqrt[3]{2}$, número ligado à duplicação do cubo, é solução da equação $x^3 - 2 = 0$ e, como veremos mais adiante, o problema da triseção do ângulo de 60° , por exemplo, está ligado às propriedades da equação $x^3 - 3x - 1 = 0$, fatos estes já previstos por Viète. É interessante registrar aqui que o problema da duplicação do cubo foi também chamado problema de Delos, por causa do oráculo de Delfos que em 430 a.C. teria prescrito aos atenienses contaminados pela peste que dessem a um altar de forma cúbica da ilha de Delos um volume duplo sem lhe mudar a forma.

De modo mediato, diria que depois de trabalhada pelos matemáticos que sucederam a Galois, a sua teoria tem por objeto as relações existentes entre dois corpos K e M , quando $K \subseteq M$, ou o que é o mesmo, quando M é uma "extensão" de K . A resolução de equações que deu origem a essa teoria é hoje apenas uma de suas aplicações.

A – Estou pressentindo, professor, que aplicaremos agora tudo o que estudamos anteriormente sobre extensões de corpos e sobre o conjunto $K[x]$, anel dos polinômios na indeterminada x com coeficientes em K .

P – Nem tudo, apenas algumas coisas; além disso, em vez do anel $K[x]$ onde K é um corpo qualquer, utilizaremos o anel $Q[x]$, onde Q é o corpo dos racionais.

A – Como tais assuntos foram vistos há algum tempo, seria possível uma revisão da parte que vai nos interessar diretamente, utilizando em paralelo alguns exemplos?

P – Tudo bem! Vejamos até que ponto vocês se lembram de tais assuntos.

Já vimos que se K e M são corpos tais que $K \subseteq M$, diz-se que M é uma extensão de K . Alguém poderia dar um exemplo de uma extensão do corpo Q dos racionais? Por favor, não me dêem o exemplo do corpo R dos reais!

P – O conjunto $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$ é um corpo e contém Q .

P – Muito bem! Também vocês se recordam de que se K e M são corpos e $K \subseteq M$, então M é um espaço vetorial sobre K . Nestas condições faz sentido falar em

elementos de M linearmente independentes sobre K , em base de M sobre K , etc. Lembrem-se que a dimensão de M sobre K é indicada por $[M:K]$ e é chamada "grau de M sobre K ". Estaremos interessados nos casos em que $[M:K]$ é um número finito. Quem é capaz de indicar uma base de $Q(\sqrt{2})$ sobre Q ?

A – O conjunto $\{1, \sqrt{2}\}$, por exemplo, o que significa que $[Q(\sqrt{2}):Q] = 2$

P – Também será muito importante nesta revisão o teorema sobre a multiplicatividade dos graus: "Se K, L e M forem corpos satisfazendo às condições $K \subseteq L \subseteq M$, $[M:L]$ e $[L:K]$ finitos, então $[M:K] = [M:L] \cdot [L:K]$."

Alguém é capaz de lembrar do esboço da demonstração?

A – Se $\{u_1, \dots, u_n\}$ é uma base de M sobre L e $\{v_1, \dots, v_m\}$ uma base de L sobre K , basta mostrar que $\{u_1 v_1, \dots, u_1 v_m, u_2 v_1, \dots, u_2 v_m, \dots, u_n v_1, \dots, u_n v_m\}$ é uma base de M sobre K . Uma vez provado isto, vemos que $[M:K] = n \cdot m = [M:L] \cdot [L:K]$.

P – Alguém poderia dar um exemplo do teorema sobre a multiplicatividade dos graus?

A – Supondo $K = Q$, $L = Q(\sqrt{2})$ e $M = [Q(\sqrt{2})](\sqrt{3})$ onde

$$[Q(\sqrt{2})](\sqrt{3}) = \{a + b\sqrt{3}, a, b \in Q(\sqrt{2})\},$$

é fácil ver que $[Q(\sqrt{2})](\sqrt{3})$ é um corpo que contém $Q(\sqrt{2})$ e, portanto, um espaço vetorial sobre $Q(\sqrt{2})$. Uma base deste espaço é o conjunto $\{1, \sqrt{3}\}$. Dessa maneira,

$$[[Q(\sqrt{2})](\sqrt{3}) : Q(\sqrt{2})] = 2.$$

Como já esboçamos anteriormente, o conjunto $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2} \cdot \sqrt{3}\}$ é uma base de

$[Q(\sqrt{2})](\sqrt{3})$ sobre Q . Logo,

$$[[Q(\sqrt{2})](\sqrt{3}) : Q] = [[Q(\sqrt{2})](\sqrt{3}) : Q(\sqrt{2})] \cdot [Q(\sqrt{2}) : Q] = 2 \times 2 = 2^2.$$

P – Bravo! Vejo que vocês fixaram bem os assuntos anteriormente estudados. Agora eu pergunto: em que condições um elemento $u \in M$ diz-se "algébrico" – sobre K ?

A – Se existe um polinômio $f \in K[x]$, $f \neq 0$, tal que u é raiz desse polinômio, ou seja, $f(u) = 0$.

P – $\sqrt[3]{2} \in \mathbb{R}$ é algébrico sobre Q ?

A – É claro, porque $\sqrt[3]{2}$ é raiz de $f(x) = x^3 - 2$, onde $f \in Q[x]$; este número está ligado ao problema da duplicação do cubo.

P – A negação da definição de elemento algébrico nos conduz à definição de elemento "transcendente". Quem é capaz...

A – Se $K \subseteq M$ e $u \in M$, u diz-se "transcendente" sobre K quando qualquer que seja o polinômio $f \in K[x]$, $f \neq 0$, tem-se $f(u) \neq 0$, isto é, u não é raiz de f .

P – Alguém pode dar um exemplo de um número real transcendente sobre o conjunto dos racionais?

A – π e, conseqüentemente $\sqrt{\pi}$, número ligado ao problema da quadratura do círculo.

P – Muito bem, chegamos ao ponto de revermos a classificação de uma extensão M de K . Alguém se lembra? Não? Uma extensão M de K diz-se:

– “algébrica” se todo $u \in M$ é algébrico sobre K ;
– “transcendente” se existe pelo menos um $u \in M$ que é transcendente sobre K ;

– “simples” se existe $u \in M$ tal que $M = K(u)$, onde $K(u)$ indica o subconjunto de M gerado pelo conjunto $K \cup \{u\}$, isto é, o menor subcorpo de M que contém K e u .

– “finita” se $[M:K]$ é finita. Citando um exemplo já considerado aqui em classe, $Q(\sqrt{2})$ é uma extensão simples e finita de Q .

A – Lembro-me, professor, que existem algumas correlações entre estes tipos de extensões.

P – É verdade. “Toda extensão finita é algébrica” e este é um corolário de um teorema que afirma o seguinte: “Se $K \subseteq M$ e $u \in M$, $K(u)$ é uma extensão finita de K se e somente se u é algébrico sobre K ”.

A – É o caso do exemplo que nos está servindo de ilustração: Q está contido em $Q(\sqrt{2})$. Neste caso, $\sqrt{2}$ é algébrico sobre Q por ser raiz de $f(x) = x^2 - 2$.

P – Existe um outro resultado sobre extensões finitas que afirma: “Toda extensão finita pode ser obtida por meio de uma sucessão finita de extensões simples”. Em outras palavras, se K e M são corpos, com $K \subseteq M$, e $[M:K] = n$ é finito, existem corpos $K_0 = K, K_1, \dots, K_n = M$ tais que

$$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = M \text{ e } K_{i+1} = K_i(u_{i+1}), u_i \in K_i, i = 0, 1, \dots, n-1.$$

A – Só para exercitar, professor, evocando ilustrações anteriores, se considerarmos em particular $K_0 = Q$ e a cadeia

$Q = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = M$, onde $u_{i+1} = \sqrt{c_i}$ com $c_i \in K_i, i=0, 1, \dots, n-1$, teremos:

$$[K_1:Q] = [K_2:K_1] = \dots = [M:K_{n-1}] = 2.$$

e, portanto, $[M:Q] = 2^n$, pelo teorema da multiplicatividade dos graus.

P – Isso! Quero observar que precisaremos exatamente deste resultado, mais adiante, considerando $K_0 = Q =$ conjunto dos racionais.

É necessário rever, ainda, a seguinte notação:

Se u é algébrico sobre K , o símbolo $[u:K]$ e a expressão “grau de u sobre K ” serão usados para indicar o grau de $[K(u):K]$ = grau do polinômio minimal de u sobre K .

A – Confesso que não me lembro mais do conceito de polinômio minimal. É

um polinômio de grau mínimo?

P – Em parte é, mas vamos tornar as coisas mais completas e mais precisas: chama-se “polinômio minimal” de u sobre K ao polinômio $f \in K[x]$ de grau mínimo tal que $f(u) = 0$. Exige-se ainda que ele seja “mônico”, isto é, o coeficiente do seu termo de maior grau seja 1. O polinômio minimal de u sobre K pode ser ainda caracterizado pelas propriedades de ser mônico, irredutível e tal que $f(u) = 0$; isto se deve ao fato básico de que todo polinômio $g(x) \in K[x]$ tal que $g(u) = 0$ é um múltiplo do polinômio minimal de u .

A – Acho que o conceito de polinômio irredutível está fazendo falta!

P – $f \in K[x]$, diz-se “irredutível” sobre K se $f = g.h$, $g, h \in K[x]$ implica que $g = \text{constante}$ ou $h = \text{constante}$. Existe, inclusive, um “critério de irredutibilidade” que, apesar de elementar, é útil para os nossos objetivos: “um polinômio do 2º ou do 3º grau $f \in K[x]$ ou é irredutível ou possui uma raiz em K ; além disso, essa raiz é inteira e divide o termo constante”.

A – Eu me lembro da demonstração desse critério, professor: sendo $f \in K[x]$ um polinômio do 2º ou do 3º grau, $f = g.h$, $g, h \in K[x]$, $g \neq \text{constante}$ e $h \neq \text{constante}$, então g ou h será do 1º grau. Suponhamos que seja g . Nestas condições,

$$f = (ax + b)h, \text{ donde } f(-b/a) = 0, -b/a \in K.$$

P – Muito bem! Acho que essa revisão é suficiente para vocês entenderem as correlações existentes entre os três problemas gregos da antiguidade, as construções com régua e compasso e a teoria de Galois.

Recordem-se que o nosso objetivo agora é demonstrar a impossibilidade de construir com régua e compasso:

- um quadrado de área igual à de um círculo dado;
- um cubo de volume igual ao dobro do volume de outro cubo dado;
- um ângulo igual a um terço de um ângulo dado.

Como já dissemos anteriormente, a nossa tarefa consiste em mostrar que escolhida uma unidade de comprimento para os segmentos do plano, não se podem construir com régua e compasso os segmentos de comprimento π e $\sqrt[3]{2}$ e que existe um ângulo α tal que $\cos \alpha$ pode ser construído com régua e compasso, mas $\cos(\alpha/3)$ não pode.

Falarei agora sobre os “números construíveis” com régua e compasso.

Seja x um número real. Para nós, a expressão “construir um número x ” significará construir com régua e compasso, a partir do segmento tomado para unidade, um segmento de comprimento igual a x . Em termos numéricos, 1 é dado e procuraremos determinar que número se pode construir a partir de 1, usando-se a régua e o compasso um número finito de vezes.

A – Serão esses os números chamados “construíveis”?

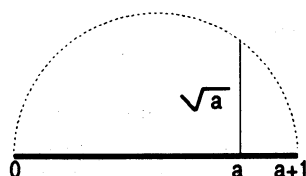
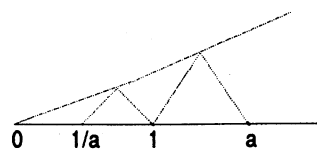
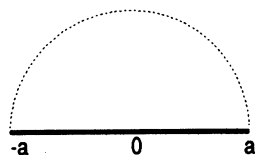
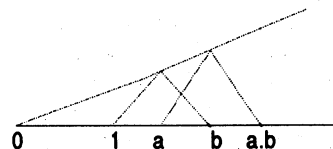
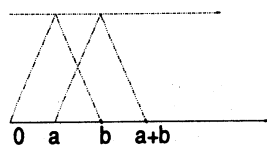
P – É verdade, e afirmo que se a e b são construíveis, $a + b$, $-a$, $a.b$, $1/a$ e $\sqrt{a}$ também o são.

A – O que você acaba de afirmar é que o conjunto dos números construíveis constitui um corpo K , com mais uma condição: se $x \in K$ então $\sqrt{x} \in K$.

P – Exatamente!

A – Quer dizer que todo número racional, em particular, é construível?

P – Perfeito! Utilizemos agora régua e compasso para provar a minha afirmação anterior. Temos, quaisquer que sejam os números construíveis a e b .



A – Semelhança de triângulos e teorema de Pitágoras tornam pacíficos os resultados acima que são menos triviais.

P – Sem dúvida alguma, e deixarei as demonstrações dos mesmos como exercícios. Examinemos mais detalhadamente a natureza dos elementos de K . Introduzindo coordenadas cartesianas no plano, os pontos passam a ser representados por pares (a,b) de números reais e é evidente que o ponto (a,b) pode ser construído se e somente se os números a e b são construíveis. Ora, construir com régua e compasso significa que somos autorizados a efetuar as seguintes construções;

- 1) Traçar a reta que une dois pontos dados.
- 2) Traçar o círculo com centro e raio dados.

A – Estou pressentindo que com este raciocínio você poderá passar das construções com régua e compasso para as equações da reta e do círculo, ou, em outras palavras, para a representação analítica. E a partir dessas equações você envolverá o conceito de extensão de um corpo e a teoria dos polinômios.

P – É mais ou menos esse o caminho. Seguindo esse roteiro, se P e Q são pontos dados, a equação da reta PQ envolve apenas expressões racionais em termos das coordenadas de P e Q . Portanto, as operações 1) e 2) acima significam,

analiticamente, que podemos considerar:

1') Retas $y = ax + b$, a, b números construíveis.

2') Círculos $(x - a)^2 + (y - b)^2 = r^2$, a, b e r números construíveis.

Um ponto, nas construções com régua e compasso só pode ser determinado por meio da repetição de um número finito das seguintes operações:

I) intersecção de duas retas construíveis;

II) intersecção de dois círculos construíveis;

III) intersecção de uma reta e um círculo, construíveis.

A – Isto significa, analiticamente, que um número construível u pode ser obtido a partir dos números racionais por meios de uma sequência finita dos seguintes processos:

I') resolução do sistema $ax - y = b$
 $a'x - y = b'$;

II') resolução do sistema $(x - a)^2 + (y - b)^2 = r^2$
 $(x - a')^2 + (y - b')^2 = r'^2$;

III') resolução do sistema $ax - y = b$
 $(x - a')^2 + (y - b')^2 = r'^2$

P – Parabéns pelo raciocínio. Finalmente deparamo-nos com as equações algébricas que vocês haviam previsto. Acrescento que os processos I') e II'), aplicados com coeficientes num corpo L produzem resultados em L . O processo III'), em geral, nos faz passar de L a $L(\sqrt{c})$, $c \in L$.

Repetindo estes processos um número finito de vezes, a partir do corpo Q dos racionais chegamos à conclusão de que todo número construível u pertence a um corpo M tal que existe uma cadeia $Q = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = M$, onde $K_{i+1} = K_i(\sqrt{c_i})$, $c_i \in K_i$, $i = 0, 1, \dots, n-1$.

Pelo teorema da multiplicatividade dos graus...

A – Temos que $[M:Q] = 2^n$, como já vimos.

P – Exato! E como $u \in M$, u é algébrico sobre Q e o grau de u sobre Q (ou seja, $[u:Q]$ que é o mesmo que $[Q(u):Q] = \text{grau do polinômio minimal de } u \text{ sobre } Q$), divide 2^n . Portanto, podemos enunciar o

Teorema

Todo número construível é algébrico sobre os racionais e seu grau é uma potência de 2.

Corolário 1

$\sqrt{\pi}$ não é construível...

A – Porque π é transcendente sobre os racionais. Logo a quadratura do círculo

não é possível!

P – Perfeitamente!

Corolário 2

$\sqrt[3]{2}$ não é construível pois satisfaz ao polinômio irredutível $x^3 - 2 \in \mathbb{Q}[x]$ e, portanto, tem grau 3 sobre $\mathbb{Q}$, não sendo possível a duplicação do cubo!

Corolário 3

Se $\alpha = 60^\circ$, $\cos \alpha = 1/2$ é construível, mas $\cos(\alpha/3)$ não é. Portanto, não é possível trissectar um ângulo de 60° .

A – Não entendi o Corolário 3, professor.

P – Você não entendeu porque não é imediato. Veja bem, sendo

$$\cos 3\beta = 4 \cos^3 \beta - 3 \cos \beta, \quad \beta = 20^\circ, \text{ temos:}$$

$$1/2 = 4 (\cos 20^\circ)^3 - 3 (\cos 20^\circ)$$

Fazendo $u = 2 (\cos 20^\circ)$ vem: $u^3 - 3u - 1 = 0$

A – O polinômio $f(x) = x^3 - 3x - 1$ é irredutível sobre $\mathbb{Q}$. De fato, sendo do 3º grau, ou é irredutível ou tem uma raiz racional...

P – E se tivesse uma raiz racional, esta seria inteira e dividiria -1, donde seria +1 ou -1, mas estes números não são raízes de f .

A – Portanto, $u = 2 \cos 20^\circ$ tem grau 3 sobre $\mathbb{Q}$, não sendo, conseqüentemente, construível. Então $u/2 = \cos 20^\circ$ também não é construível, daí a impossibilidade da trisecção do ângulo.

P – Ficou tudo claro? A missão foi cumprida e quero cumprimentá-los pelo empenho e pela participação!

A – Descobriremos juntos é muito mais gostoso, professor!

REFERÊNCIAS BIBLIOGRÁFICAS

- BOYER, Carl B. *História da Matemática*. São Paulo: Edgar Blücher, 1974.
 JACOBSON, N. *Lectures in Abstract Algebra*. N. York: D. Van Nostrand Company, Inc., 1955.
 KAPLANSKY, I. *Introdução à teoria de Galois*. Rio de Janeiro: Notas de Matemática, IMPA, 1955.
 WAERDEN, Van der. *Modern Algebra*. N. York: Frederick Ungar Publishing Co., 1950.