**O trabalho de Leonard Eugene Dickson
em álgebras com divisão**

Regina Célia Nostre Marques

TESE APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO GRAU DE DOUTOR
EM
MATEMÁTICA

Concentração em História da Matemática
Orientador: Prof. Dr. Francisco César Polcino Milies

Durante a elaboração deste trabalho, a autora recebeu auxílio parcial da FAPESP

São Paulo, junho de 2004

Resumo

Neste trabalho, investigam-se as origens da teoria das álgebras com divisão, hoje de importância central na álgebra abstrata. Uma vez que as contribuições de alguns autores tais como W. R. Hamilton, B. Peirce e J. H. M. Wedderburn já foram estudadas por diversos pesquisadores, concentramos nossa atenção na figura e nos estudos de L. E. Dickson, que foi o responsável pelas primeiras construções de exemplos mais gerais e, como descobrimos, foi o introdutor de algumas das idéias fundamentais da área.

Abstract

In this work we study the origins of the theory of Division Algebras which is today of central importance in abstract algebra. Since the contributions of some authors like W. R. Hamilton, B. Peirce and J. H. M. Wedderburn were studied by several other authors, we concentrate our attention on the figure and work of L. E. Dickson, who was responsible for the construction of the first general examples and, as we discovered, he was the person who introduced some of the fundamental ideas in that area.

*Aos meus pais,
Adriano e Rodolphina.*

*Embora ninguém possa voltar atrás e fazer um novo começo,
qualquer um pode começar agora e fazer um novo fim.*

Chico Xavier.

Agradecimentos

Agradeço à minha família, em especial aos meus pais, que sempre me apoiaram em todos os momentos da minha vida.

Agradeço ao César, por ter acreditado neste projeto.

Agradeço aos amigos, em especial ao Raul, Mário e Fernando.

Agradeço aos professores deste instituto que me introduziram nas pesquisas matemáticas, em especial à Rosa, que me orientou no mestrado e ao Forger.

Conteúdo

Introdução	v
Lista de Notações	1
1 Os Primeiros Estudos	3
1.1 Introdução	3
1.2 A Descoberta dos Quatérnios por Hamilton	4
1.3 O Desenvolvimento dos Estudos em Álgebras	9
1.4 Joseph H. M. Wedderburn	14
2 A Matemática nos Estados Unidos	19
2.1 Introdução	19
2.2 A História da Matemática nos Estados Unidos	20
2.3 A Matemática na Universidade de Chicago	30
2.4 Leonard Eugene Dickson	35
2.5 A Influência dos Trabalhos de Dickson em Outros Autores	41
3 Fase Axiomática	45
3.1 Introdução	45
3.2 Primeiros Trabalhos	47
3.3 Definições de Corpo Através de Postulados	48
3.4 Sistemas de Números Hipercomplexos sobre um Corpo $\mathbb{F}$ Qualquer	52
3.5 Definição de Grupo Através de Postulados	56

4 Os Quatérnios e suas Generalizações	61
4.1 Introdução	61
4.2 O Teorema de Hurwitz	62
4.3 A Aritmética dos Quatérnios	67
4.4 Generalizações dos Quatérnios	69
5 Novos Exemplos de Álgebras com Divisão	73
5.1 Os Primeiros Exemplos	73
5.2 As Álgebras de Cayley-Dickson	75
5.3 As Álgebras Cíclicas	76
5.4 O Exemplo de Álgebra com Divisão de Dimensão Maior que Quatro	80
5.5 A Construção de Novos Exemplos de Álgebras com Divisão	90
Conclusão	101
A Um Pouco de Matemática	103
A.1 Definições	103
A.2 Álgebra Linear Associativa	104
A.3 Grupos	105
A.4 Álgebras	106
A.5 Teoremas de Estrutura	109
A.6 Exemplos de Álgebras	110
B Obras de Dickson	115
C O Livro <i>History of Theory of Numbers</i>	133
C.1 O Primeiro Volume	133
C.2 O Segundo Volume	137
C.3 O Terceiro Volume	148
Bibliografia	155

Lista de Figuras

1.1	Willian R. Hamilton	4
1.2	Joseph H. M. Wedderburn	14
2.1	Benjamin Peirce	24
2.2	Eliakim Hastings Moore	31
2.3	Leonard Eugene Dickson	36

Introdução

Este trabalho tem por objetivo estudar as contribuições de Leonard Eugene Dickson à teoria das álgebras com divisão.

A primeira álgebra com divisão (que não é corpo) descoberta foi a álgebra dos quatérnios reais, cuja tabela de multiplicação foi apresentada por William R. Hamilton. Apesar da existência, na literatura, de controvérsias a respeito do autor desta descoberta (pois Gauss a havia obtido implicitamente em 1819), é indiscutível que foi Hamilton quem percebeu a importância dos quatérnios, apresentando sua tabela de multiplicação com o claro objetivo de determinar uma álgebra com divisão. Na realidade, ele queria criar uma teoria análoga àquela dos complexos, que permitia trabalhar com vetores no plano, para trabalhar com vetores no espaço e criar uma linguagem matemática apropriada para o desenvolvimento da dinâmica. Entretanto, a motivação e as ferramentas necessárias para o desenvolvimento das álgebras finitas com divisão apareceram apenas algum tempo depois com a teoria de matrizes, de números hipercomplexos e de representações de grupos finitos. De acordo com Joseph H. M. Wedderburn, as matrizes também foram introduzidas por Hamilton, em 1853, embora o nome *matriz* tenha sido dado por Arthur Cayley, que foi quem desenvolveu seus cálculos.

No fim do século dezenove, Benjamin Peirce estendeu a teoria de números hipercomplexos à teoria geral de álgebras lineares. No seu trabalho *Linear Associative Algebras*, introduziu os importantes conceitos de elementos *idempotentes* e *nilpotentes* e investigou os possíveis tipos de álgebras que têm, no máximo, seis elementos na base. A partir deste momento, os estudos acerca do assunto tomaram rumos ascendentes, culminando com o teorema de estrutura apresentado por Wedderburn, em 1907, no trabalho [WE3]: as álgebras simples são, na realidade, matrizes sobre álgebras com divisão. Este resultado fez com que as álgebras com divisão se tornassem um tópico de relevante importância dentro da matemática.

Em 1906, Dickson introduziu as álgebras cíclicas, que, historicamente, foram de grande importância, pois permitiram a construção de novos exemplos. Elas foram tão fundamentais para o desenvolvimento desta teoria que mereceram a denominação de *álgebras de Dickson*, dada por Wedderburn em [WE4]. Usando o conceito de álgebras cíclicas, Dickson

construiu o primeiro exemplo de álgebra finita com divisão de dimensão diferente de quatro e o apresentou no seu livro *Algebras and their Arithmetics* ([229]), em 1923.

A primeira álgebra com divisão de dimensão dezesseis foi apresentada por Francesco Cecioni, em 1923, no seu trabalho *Sopra un tipo di Algebre prive di divisori dello zero* ([CE1]). Suas idéias foram estendidas por Dickson em [240], [257] e [267], que desenvolveu as ferramentas necessárias para a formulação do conceito de *produto cruzado*, introduzido por Emmy Noether, em 1929.

Na segunda metade da década de 1920, a teoria de álgebras lineares tornou-se tão importante que seus resultados passaram a ser apresentados em livros. O primeiro a surgir foi *Corpi Numerici e Algebre* ([SZA]) de Gaetano Scorza, em 1921, seguido por *Algebras and their Arithmetics* citado acima, onde Dickson dedicou um capítulo inteiro e dois apêndices ao estudo de álgebras com divisão. Este trabalho foi ampliado para o livro *Algebren und ihre Zahlentheorie* ([253]), que Dickson publicou em 1927, apenas no idioma alemão, com um grande impacto na ativa escola alemã de Göttingen (cujos membros foram grandes responsáveis pelo desenvolvimento desta teoria). Nesta época, Th. Skolem tomou conhecimento deste trabalho e publicou uma pequena monografia ([SK]) sobre álgebras associativas, onde apresentou uma primeira versão do hoje conhecido como teorema de Skolem-Noether (5.5).

A década de 1930 foi a mais ativa, no que diz respeito à pesquisa de álgebras com divisão, tanto nos Estados Unidos quanto na Alemanha, e, por isso, é até chamada, por alguns autores, de *período de ouro*. De um lado do Oceano Atlântico, tínhamos Dickson e também Abraham A. Albert, que desenvolveu a teoria geral de corpos de decomposição e relações numéricas entre as várias dimensões dos centralizadores das álgebras. Do outro lado, em especial em Göttingen, o interesse por este assunto dava-se por causa do desenvolvimento da teoria de representações de grupos, cujas idéias de similaridade e irredutibilidade eram bastante importantes. O grande salto em direção à teoria moderna de álgebra foi dado por Noether, quando estendeu o estudo de representações por matrizes ao de módulos e transformações lineares e cujos passos foram seguidos por jovens algebristas de Göttingen, incluindo R. Brauer, I. Schur e E. Artin.

Nos anos seguintes, as pesquisas sobre álgebras com divisão não pararam de crescer e, hoje, constituem um ramo muito promissor da matemática.

No presente estudo, inicialmente fazemos uma explanação sobre os primeiros trabalhos acerca deste assunto, incluindo o artigo *On Hypercomplex Numbers* de Joseph H. M. Wedderburn (baseado em [PA4]), que foi o primeiro a apresentar uma teoria mais geral sobre a estrutura das álgebras.

Em seguida, situamos Dickson na história da matemática dos Estados Unidos e da Universidade de Chicago, dando uma idéia de sua importância para a teoria da álgebra abstrata. A partir daí, estudamos detalhadamente seus trabalhos sobre álgebras com divisão, onde destacamos os seguintes tópicos:

- **Definições axiomáticas:** têm início em 1901 ([51]) e continua com publicações em 1903 ([82] e [83]) e 1905 ([105]), onde destacamos a definição de álgebra linear associativa apresentada em [83];
- **Teoremas de Wedderburn e Dickson sobre anéis finitos com divisão:** são publicados, em 1905, em [WE1] e [119], respectivamente;
- **Álgebras Cíclicas:** apresenta, pela primeira vez, a definição em 1905-1906, num *abstract* do volume doze do AMS *Bulletin*, e publica, em detalhes, seus estudos em 1914 ([184]). Em 1923 ([205]), Dickson mostra o primeiro exemplo de álgebra com divisão de dimensão maior que quatro (que é uma álgebra cíclica);
- **Álgebras de Cayley-Dickson:** primeiras idéias em 1906 ([122]) e primeiro exemplo em 1919 ([205]);
- **Quatérnios generalizados e a aritmética dos quatérnios:** primeiros estudos são apresentados em 1914 ([182]) e continuam com publicações em 1919 ([205]), em 1921 ([218] e [220]) e em 1924 ([235]);
- **Ordens maximais de uma álgebra:** apresenta o conceito em 1924 ([233]), embora não dê nenhum nome especial;
- **Produtos Cruzados:** primeiras idéias aparecem em 1926 ([240]) e os estudos prosseguem com a apresentação de trabalhos em 1927 ([253]), 1928 ([257]) e 1930 ([267]).

Nossa metodologia de trabalho consistiu em buscar, nas fontes primárias, a origem das idéias e explicitar, com precisão, quando, como e onde estas idéias apareceram. Neste sentido, seguimos a metodologia usual em história da matemática, como a empregada por pesquisadores tais como A. Amitsur em [AM1], A. Brigaglia em [BG1] e [BG2], A. Brigaglia e P. Mammone em [BM], T. Hawkins em [HAW], K. Parshal em [PA1], [PA2], [PA3], [PA4] e [PA5] e B.L. Van der Waerden em [WA1] e [WA2].

Lista de Notações para as Obras de Dickson

1. AJM: American Journal of Mathematics.
2. AM: Annals of Mathematics.
3. AMM: American Mathematical Monthly.
4. AMS: American Mathematical Society.
5. CMP: Circolo del Matematica di Palermo.
6. DJM: Duke Mathematical Journal.
7. DMV: Deutschen Math. Verein.
8. GN: Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen.
9. LMS: London Mathematical Society.
10. MA: Mathematical Annals.
11. MM: Messenger of Mathematics.
12. MMP: Monthly Mathematical and Physics.
13. NAS: National Academy of Science of USA.
14. NYMS: New York Mathematical Society.
15. QJM: Quarterly Journal of Pure and Applied Mathematics.
16. QJMO: Quarterly Journal of Mathematics of Oxford.

Capítulo 1

Os Primeiros Estudos

1.1 Introdução

A teoria de álgebras, que possui um caráter abstrato por estar distante das aplicações físicas imediatas ou das interpretações geométricas, é dotada de uma estrutura lógico-dedutiva, onde um grande número de teoremas é deduzido de um pequeno conjunto de axiomas. Como esta abstração se deu como consequência do estudo dos números complexos, vamos lembrar rapidamente a história do seu desenvolvimento.

Em sua *Ars Magna*, de 1545, Girolamo Cardan (1501-1576) considerou o problema de dividir um segmento de comprimento 10 em duas partes cujo produto é 40. Isto levou à equação $x^2 - 10x + 40$, cujas soluções são $x = 5 \pm \sqrt{-15}$. Para Cardan, assim como para seus contemporâneos, o símbolo $\sqrt{-15}$ não possuía significado. Entretanto, observou que

“deixando de lado as torturas mentais envolvidas e multiplicando $5 + \sqrt{-15}$ por $5 - \sqrt{-15}$ obtém-se $25 - (-15)$ que é 40.”

Problemas como este, eventualmente, resultam em equações do segundo grau que levam a raízes de números negativos. Porém, isto não causava preocupação: considerava-se, apenas, que o problema inicial não possuía solução.

Esta visão começou a mudar com o estudo das equações de terceiro grau: em sua *Algebra*, de 1572, Rafael Bombelli (1526-1572) aplicou a já conhecida fórmula para resolver equações do terceiro grau a $x^3 = 15x + 4$ e obteve como raiz $x = (2 + \sqrt{-121})^{\frac{1}{3}} + (2 - \sqrt{-121})^{\frac{1}{3}}$, onde aparecem raízes quadradas de números negativos. Entretanto, verifica-se diretamente que $x = 4$ é uma solução e um cálculo simples mostra que $-2 + \sqrt{3}$ e $-2 - \sqrt{3}$ são as outras raízes. Ou seja, todas as soluções desta equação são reais. Isto levou Bombelli a tentar *calcular* com raízes de números negativos, mesmo considerando-as sem sentido. Para isto,

Figura 1.1: William R. Hamilton

assumiu que as regras das operações (comutativa, associativa, etc) eram as mesmas que se tinham para números reais. Logo, expressões como $\sqrt{-1}$ eram impossíveis, mas não inúteis e valia a pena trabalhar com elas.

A partir deste momento, o estudo dos números complexos foi desenvolvendo-se gradativamente, embora houvesse muitas dúvidas quanto à sua legitimidade. O próprio Leonhard Euler (1707-1783), que obteve muitos resultados nesta teoria, escreveu a seu respeito na sua *Algebra*, de 1770:

“destes números só podemos afirmar que não são zero, nem maiores do que zero, nem menores do que zero, o que necessariamente os faz imaginários ou impossíveis.”

As muitas dúvidas ligadas à validade dos números complexos permaneceram até que aparecesse sua representação gráfica como vetores, ou pontos de um plano, dada por Caspar Wessel (1745-1818) em 1797, Jean Robert Argand (1768-1822) em 1813, e, finalmente, por Johann Carl Friedrich Gauss (1777-1855) em 1832.

Foi neste período de intensa atividade, na direção crescente da teoria de álgebras, que começaram a aparecer os trabalhos do notável matemático irlandês William Rowan Hamilton (1805-1871), cujas pesquisas culminaram com a descoberta dos quatérnios, em 1843.

1.2 A Descoberta dos Quatérnios por Hamilton

Para melhor compreender o processo histórico que levou à introdução da abstração na teoria de álgebras, daremos uma rápida visão da situação da matemática na Inglaterra,

no começo do século XIX, que será de fundamental importância para o surgimento desta teoria.

Na Inglaterra, esta ciência tinha-se isolado do resto do mundo, desde a época da controvérsia entre Isaac Newton (1642-1727) e Gottfried Wilhelm Leibniz (1646-1716) pela descoberta do cálculo. Entre outras coisas, os matemáticos ingleses continuavam a usar a notação de Newton, muito mais obscura do que a de Leibniz.

Em 1815, vários matemáticos da Universidade de Cambridge, como Charles Babbage (1792-1871), George Peacock (1791-1858) e John Herschel (1792-1878), fundaram a *Analytical Society*, cuja finalidade imediata era reformular o ensino e as notações do cálculo. Entretanto, sua contribuição fundamental foi repensar e discutir os fundamentos da álgebra. Em 1830, Peacock publicou seu *Treatise on Algebra*, quando tentou dar a esta disciplina uma estrutura lógica compatível àquela dada à geometria, nos *Elementos* de Euclides. Esta obra, ampliada para dois volumes em 1845, marcou o início do pensamento axiomático em álgebra. No primeiro volume, Peacock exibiu as leis fundamentais da aritmética trabalhando apenas com números e dando aos símbolos $+$ e $-$ seu significado ordinário. Já no segundo volume, desenvolveu uma *álgebra simbólica* e as mesmas regras foram aplicadas a símbolos sem conteúdo específico.

Os estudos que consideram a teoria de álgebras como uma ciência de símbolos, com suas leis de combinações, também foram considerados por Augusto de Morgan (1806-1871), que escreveu vários artigos sobre a estrutura de álgebra. Em seu *Trigonometry and Double Algebra*, de 1849, os símbolos não têm significado preestabelecido¹.

Foi neste período que Hamilton deu a fundamentação definitiva dos números complexos como pares ordenados de números reais, tal como é apresentada atualmente: afirmou, em seu *Conjugate Functions and on Algebra as the Science of Pure Time*, de 1837, que um número complexo $a + bi$ não é uma soma genuína no mesmo sentido que $2 + 3$. O uso do sinal de “mais” é um acidente histórico e bi não pode ser somado a a . O número complexo $a + bi$ nada mais é que um par ordenado (a, b) de números reais. A peculiaridade que i ou $\sqrt{-1}$ introduz nas operações, com números complexos, é incorporada por Hamilton, nas definições das operações com os pares ordenados. Daí, se $a + bi$ e $c + di$ são dois números complexos, então

$$(a, b) \pm (c, d) = (a \pm c, b \pm d),$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc),$$

$$\frac{(a, b)}{(c, d)} = \left(\frac{ac + bd}{c^2 + d^2}, \frac{bc - ad}{c^2 + d^2} \right).$$

¹A expressão *álgebra dupla* significa álgebra dos números complexos, enquanto que *álgebra simples* significa números negativos.

As propriedades usuais associativa, comutativa e distributiva podem agora ser deduzidas. Com esta visão dos números complexos, não apenas eles estão fundamentados nos números reais, mas o mistério que a expressão $\sqrt{-1}$ representava até este momento tinha, então, desaparecido. Incidentalmente em 1837, numa carta, Gauss observou a Wolfgang Bolyai que, em 1831, já havia tido esta noção de pares ordenados. Mas foi a publicação de Hamilton que deu, ao mundo matemático, o conceito de números complexos como pares ordenados de números reais.

A noção de um vetor, isto é, um segmento de reta direcionado que pode representar a magnitude e direção de uma força, uma velocidade ou uma aceleração foi aparecendo, gradativamente, na matemática. O filósofo grego Aristóteles já sabia que as forças podem ser representadas por vetores e que a ação combinada de duas forças pode ser obtida pelo que é comumente conhecido como a lei do paralelogramo: a diagonal do paralelogramo formado pelos vetores $\mathbf{a}$ e $\mathbf{b}$ dá a magnitude e a direção da força resultante. Simon Stevin empregou a lei do paralelogramo em problemas de estática, enquanto que Galileo afirmou explicitamente a lei.

Após a representação geométrica dos números complexos, apresentada por Wessel, Argand e Gauss, ter-se tornado mais familiar para os matemáticos, eles perceberam que os números complexos podiam ser usados para representar forças no plano. Por exemplo, se dois vetores são representados por $3+2i$ e $2+4i$, então a soma deles, $5+6i$, representa a soma destes vetores pela lei do paralelogramo. Na realidade, o números complexos oferecem uma álgebra para representar vetores, no plano, que permite combiná-los entre si. Entretanto, a utilidade dos números complexos é limitada: se várias forças agem num corpo, estas forças podem não estar no mesmo plano. Para tratá-las algebricamente, é necessário obter uma álgebra tridimensional análoga à dos números complexos. Poder-se-iam usar as coordenadas cartesianas ordinárias (x, y, z) de um ponto para representar o vetor da origem até o ponto; entretanto, não existiriam operações entre as triplas de números que representassem as operações com os vetores, que, assim como no caso dos números complexos, deveriam incluir a adição, a subtração, a multiplicação e a divisão, assim como deveriam obedecer às leis usuais — associativa, comutativa e distributiva. Os matemáticos passaram então a procurar pelos *números complexos tridimensionais* e sua álgebra.

Wessel, Gauss, Servois, Möbius e outros trabalharam neste problema. Gauss escreveu, em 1819, uma pequena nota, não publicada, sobre transformações de espaços. Ele pensou nos números complexos como deslocamentos: $a+bi$ era o deslocamento de a unidades, ao longo de uma direção fixada, seguido por um deslocamento de b unidades, na direção perpendicular. Então tentou construir uma álgebra tridimensional, na qual a terceira componente representaria um deslocamento, numa direção perpendicular ao plano de $a+bi$. Gauss obteve uma álgebra não comutativa, o que não era a álgebra efetivamente procurada pelos físicos. Ainda, pelo fato de que não publicou este trabalho, seus resultados tiveram pouca influência nesta teoria.

A criação de um espaço análogo ao dos números complexos deve-se a William R. Hamilton que, assim como Newton, era tão bom matemático quanto físico. Hamilton foi uma criança prodígio: aos três anos de idade lia perfeitamente inglês e já havia aprendido os fundamentos da aritmética; aos quatro, aprendeu geografia; aos cinco, sabia latim e hebraico; até os dez anos de idade aprendeu italiano, francês, árabe, sânscrito, persa, caldeu e várias línguas orientais. Aos doze, interessou-se por matemática. Nesta época, estudou a *Algebra Universalis* de Newton e, antes dos dezessete, estudou o monumental *Mecanique Céleste* de Laplace, onde encontrou um erro em 1822. Entrou, em 1823, para o *Trinity College* em Dublin, cujo desempenho foi brilhante. Fez importantes contribuições à física e à astronomia. Seu maior trabalho matemático foi a descoberta dos quatérnios, cuja forma final foi apresentada em *Lectures on Quaternions*, em 1853 e nos dois volumes *Elements of Quaternions*, de 1866, publicados após sua morte.

A noção exata dos números complexos, tida por Hamilton, permitiu que ele pensasse mais claramente sobre o problema de encontrar uma álgebra tridimensional, análoga à dos complexos, para representar vetores no espaço. Como tudo sobre números, que era conhecido até aquele momento, passava pela propriedade comutativa da multiplicação, era natural que Hamilton acreditasse que a nova álgebra fosse comutativa e que também possuísse as outras propriedades dos números reais e dos complexos. Após vários anos de pesquisa, observou que a nova álgebra deveria ser quadridimensional e não poderia ser comutativa, obtendo então os quatérnios em 1843.

Numa carta escrita a seu filho, 22 anos após a descoberta, relatou a excitação daquele momento:

“Mas no dia 16 do mesmo mês [outubro de 1843] — que era uma segunda-feira e dia de reunião do Conselho da Real Sociedade da Irlanda — eu ia andando para participar e presidir, [a reunião] e sua mãe andava comigo, ao longo do Royal Canal, ... e embora ela falasse comigo ocasionalmente, uma corrente subjacente de pensamento estava acontecendo na minha mente, que finalmente teve um resultado, cuja importância senti imediatamente. Pareceu como se um circuito elétrico tivesse se fechado; e saltou uma faísca, o heraldo de muitos anos vindouros de pensamento dirigido e trabalho, da minha parte se poupado, e de qualquer forma por parte de outros, se eu vivesse o suficiente para contar minha descoberta. Neste instante, peguei uma libreta de anotações, que ainda existe, e fiz um registro naquela mesma hora. Não pude resistir ao impulso — que pode ser não tão filosófico assim — de gravar com um canivete numa pedra da ponte de Brougham², quando a cruzamos, a fórmula fundamental dos símbolos i, j, k

$$i^2 = j^2 = k^2 = ijk = -1 \quad (1.1)$$

²Nesta ponte, atualmente existe uma placa comemorativa a este fato, com a seguinte mensagem:

“Here as he walked on the 16th of October 1843, Sir William Rowan Hamilton in a flash of

que contém a solução do Problema.”

Este problema, ao qual Hamilton se referia, era o de determinar a tábua de multiplicação de uma álgebra quadridimensional sobre $\mathbb{R}$, no mesmo sentido dos números complexos.

Observemos que a relação estabelecida em (1.1) implica nas conhecidas fórmulas que definem a tábua de multiplicação dos quatérnios

$$\begin{cases} ij = -ji = k \\ jk = -kj = i \\ ki = -ik = j. \end{cases}$$

Com a multiplicação definida desta forma, pode-se mostrar que esta álgebra é com divisão e tem-se que o conjunto dos quatérnios constitui o primeiro exemplo de álgebra não comutativa com divisão.

Hamilton reconheceu imediatamente a importância de sua descoberta, principalmente para o desenvolvimento da física. Ele mesmo realizou aplicações dos quatérnios à geometria, à mecânica e à física. Neste período, introduziu termos como *vetor*, *versor*, *tensor*, *escalar*, que nos são tão familiares, hoje em dia.

Os quatérnios não ocuparam o lugar que Hamilton sonhava na física — comparável ao papel desempenhado pelo cálculo na mecânica — mas, mesmo assim, tiveram importância decisiva, em pelo menos, dois sentidos: por um lado, deram origem ao cálculo vetorial, por outro lado, a descoberta dos quatérnios teve um papel decisivo no desenvolvimento da álgebra.

Com efeito, Josiah Willard Gibbs (1839-1903) era professor de física-matemática no *Yale College* e, numa tentativa de simplificar os métodos dos quatérnios, escreveu, para o uso de seus estudantes, um conjunto de notas intitulado *Elements of Vector Analysis*, onde expõe o cálculo vetorial da forma hoje usual. Independentemente, Oliver Heaviside (1850-1925), engenheiro especializado em telegrafia, publicou, durante a década de 1880-1890, uma série de artigos no jornal *Electrician*, onde usava o cálculo vetorial que tinha desenvolvido, da mesma forma que Gibbs, simplificando os métodos dos quatérnios, para torná-los mais acessíveis para os engenheiros.

Em relação à descoberta dos quatérnios, a abstração crescente, que estava em alta, teve a virtude de assinalar que as *leis fundamentais*, sugeridas pelos sistemas até então conhecidos, não eram, *a priori*, dados que deviam ser sempre assumidos, uma vez que o

genius discovered the fundamental formula of quaternions $i^2 = j^2 = k^2 = ijk = -1$, and cut it on the stone in this bridge.”

conjunto dos quatérnios é o primeiro exemplo conhecido, onde a ordem dos fatores altera o produto, isto é, a primeira álgebra não comutativa. Mostrou também, claramente, a possibilidade de estender, ainda mais, o conjunto das álgebras conhecidas.

1.3 O Desenvolvimento dos Estudos em Álgebras

1.3.1 Os Octônios e os Números Hipercomplexos

A descoberta dos quatérnios por Hamilton lançou a semente para o desenvolvimento de novas álgebras. Em 26 de dezembro do mesmo ano, John T. Graves (1806-1870) escreveu a Hamilton contando sua construção de uma álgebra de dimensão oito, análoga aos quatérnios, que chamou de oitavos. Embora Graves não tivesse percebido, Hamilton mostrou-lhe que os oitavos, ou octônios, não só não satisfaziam a lei comutativa da multiplicação, como também não verificavam a associatividade. Se Graves não tivesse deixado a cargo de Hamilton o anúncio da descoberta dos octônios, talvez estes números hoje fossem conhecidos como *números de Graves* em vez de *números de Cayley*, pois antes que Hamilton anunciasse a construção obtida por Graves, Arthur Cayley (1821-1895) publicou, em março de 1845, um artigo sobre esta álgebra no qual apenas descrevia sua tabela de multiplicação e indicava sua não comutatividade.

O caminho para novas generalizações estava, então, aberto. O próprio Hamilton introduziu, em sua *Lectures on Quaternions*, os biquatérnios, que nada mais são do que os quatérnios com coeficientes complexos, constituindo uma álgebra de dimensão oito sobre os reais. Também mostrou que esta álgebra contém divisores do zero (ou seja, elementos não nulos a e b tais que $ab = 0$) e, conseqüentemente, não é uma álgebra com divisão. Neste mesmo texto, desenvolveu uma nova generalização que já havia iniciado, num artigo publicado nos *Transactions of the Royal Irish Academy*, em 1848: os números hipercomplexos, que definiu como o conjunto de todos os símbolos da forma

$$x_1 e_1 + \cdots + x_n e_n,$$

onde $x_1, \dots, x_n$ são números reais ou complexos e $e_1, \dots, e_n$ são símbolos, chamados *unidades* do sistema. Tal como no caso dos quatérnios, a soma de dois números hipercomplexos é definida somando-se os coeficientes correspondentes e, assumindo a propriedade distributiva e definindo como multiplicar as unidades entre si, obtém-se a multiplicação de tais números.

Como o produto de duas destas unidades deve ser outro elemento do sistema, é possível escrevê-lo na forma

$$e_i e_j = \sum_{k=1}^n a_k(i, j) e_k.$$

A estrutura multiplicativa do sistema é determinada dando-se os valores dos coeficientes $a_k(i, j)$ que, por causa disto, são chamados *constantes estruturais* do sistema.

1.3.2 A Álgebra de Matrizes de Cayley

Arthur Cayley nasceu na Inglaterra, em 1821 e demonstrou talento matemático desde a juventude. Estudou no *Trinity College* em Cambridge, onde foi eleito membro e tutor assistente. Entretanto, abandonou a posição três anos depois para dedicar-se à advocacia, pelos quinze anos seguintes. Porém, neste período, não deixou suas pesquisas matemáticas, publicando mais de 200 artigos. Foi nesta época, também, que começou sua longa amizade e colaboração com James Joseph Sylvester (1814-1897). Em 1863 Cayley voltou para Cambridge e, exceto pelo ano de 1882, em que passou na Universidade Johns Hopkins, a convite de Sylvester, permaneceu lá até sua morte em 1895.

Cayley tinha uma notável habilidade para as formulações abstratas: sabia ver a generalidade por trás dos exemplos particulares, o que lhe permitiu formular o conceito de grupo abstrato no artigo *On the Theory of Groups as Depending on the Symbolical Equation $\theta^n = 1$* , de 1854. Ao definir grupo abstrato, Cayley usou uma notação multiplicativa e, para frisar o fato de que num grupo está definida uma única operação, observou que, no seu conjunto, os símbolos $+$ e 0 não têm nenhum significado. No fim do artigo, porém, colocou-se a questão de como introduzir a adição. Para isto, denotou os elementos do grupo por letras gregas $\alpha, \beta, \dots$ e considerou combinações lineares formais do tipo $a\alpha + b\beta + \dots$ e definiu a soma de dois destes elementos somando coeficiente a coeficiente e a multiplicação distributivamente, a partir de elementos do grupo. Ilustrou sua definição, mostrando como multiplicar dois elementos da forma $w + a\alpha + b\beta + c\gamma + d\delta + e\epsilon$, onde $1, \alpha, \beta, \gamma, \delta, \epsilon$ denotam os elementos do grupo não comutativo de ordem seis, cuja tabela de multiplicação já havia introduzido no artigo. Desta forma, construiu, explicitamente, pela primeira vez, o anel de grupo que hoje denotamos por $C[S_3]$. É interessante notar que ainda observou que o sistema acabado de construir é semelhante ao dos quatérnios.

Pouco tempo depois, Cayley introduziu um novo conceito, cuja importância no desenvolvimento da matemática, seria difícil de enxergar-se à época: a álgebra de matrizes. É verdade que, como Cayley observou, logicamente, a idéia de matriz precede à de determinante³, mas historicamente a ordem é inversa (o que justifica o fato de as propriedades básicas das matrizes já estarem suficientemente claras por ocasião de sua definição). Chegou a este conceito através de seus estudos de invariantes sob transformações lineares, conforme ele mesmo diz:

³Os determinantes e suas propriedades já eram estudados desde a primeira metade do século dezoito, introduzidos em conexão com a resolução de sistemas lineares. Foram utilizados, pela primeira vez, por Colin Maclaurin (1698-1746), provavelmente em 1729 e publicados, postumamente, no seu *Treatise of Algebra* de 1748.

“Eu certamente não cheguei à noção de matriz de forma alguma através dos quatérnios; foi diretamente dos determinantes ou como uma forma conveniente de expressar as equações

$$\begin{aligned}x' &= ax + by \\ y' &= cx + dy.”\end{aligned}$$

Cayley também introduziu a matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

que representa a informação essencial sobre a transformação. Pelo fato de que Cayley foi o primeiro a trabalhar com as matrizes propriamente ditas e o primeiro a publicar uma série de artigos sobre o assunto, é creditada a ele a criação da teoria de matrizes.

Em 1858, publicou *A Memoir on the Theory of Matrices*, onde introduziu a soma de matrizes e o produto por escalares. Neste trabalho, apresentou um novo sistema algébrico semelhante aos que vinham sendo desenvolvidos:

“Se verá que as matrizes (considerando apenas as de mesma ordem) se comportam como quantidades; elas podem ser somadas, multiplicadas ou compostas: a lei de adição das matrizes é precisamente semelhante àquela da adição de quantidades algébricas; no que diz respeito à sua multiplicação, existe uma peculiaridade de que matrizes não são, em geral, comutativas.”

Observemos que, na época, ainda não existia uma definição abstrata axiomática de anel; logo, o fato de que o conjunto das matrizes de um dado tamanho constituía um sistema hipercomplexo não era evidente.

Cayley observou, explicitamente, uma relação com os quatérnios: notou que se M e N são duas matrizes do tipo 2×2 que verificam $M^2 = N^2 = -1$ e $MN = -NM$, então, escrevendo $L = MN$, as matrizes L , M e N satisfazem

“um sistema de relações similar aquele da teoria dos quatérnios.”

Esta observação despertou o interesse de Sylvester que, no artigo *Lectures on the Principles of Universal Algebra*, de 1884, afirmou que um trabalho de Charles S. Peirce lhe sugeriu

“o método pelo qual uma matriz é despojada de suas dimensões como área e representada como uma soma linear.”

Ele se referia, naturalmente, ao fato bastante conhecido de que o conjunto de todas as matrizes do tipo $n \times n$ pode ser considerado como um espaço vetorial de dimensão n^2 . Denotando por e_{ij} a matriz que tem 1 na posição ij e 0 nas demais, uma matriz $A = (a_{ij})$ pode ser escrita na forma

$$A = \sum_{i,j} a_{ij} e_{ij}.$$

Isto torna evidente que as matrizes também são sistemas hipercomplexos. Vale ressaltar que esta notação não foi usada por Sylvester. Ela foi introduzida por Eduard Study (1862-1922), em 1889.

1.3.3 Peirce e as Primeiras Tentativas de Classificação de Álgebras

O primeiro trabalho a tentar estabelecer uma classificação sistemática dos vários exemplos que foram publicados a partir da descoberta dos quatérnios é devido a Benjamin Peirce (1808-1880), considerado o *pai fundador* da matemática americana. Era professor em Harvard e, na época em que Hamilton descobriu os quatérnios, dedicava-se, principalmente, à astronomia e a escrever livros. Porém, após a publicação dos primeiros trabalhos de Hamilton, interessou-se pelo assunto e passou a incluí-lo nas suas aulas.

Em 1870, publicou seu *Linear Associative Algebras*, em forma de litografia, e distribuiu entre seus amigos e conhecidos, arcando com todas as despesas de publicação. Numa carta, enviada, juntamente com uma cópia deste artigo, ao amigo George Bancroft (1800-1891), explicou o principal propósito deste trabalho:

“Este trabalho se responsabiliza pela investigação de todas as possíveis simples, duplas, triplas, quádruplas, e quádruplas álgebras as quais são objeto para certas simples e quase indispensáveis condições. As condições são aquelas bem conhecidas pelos algebristas como distributiva e associativa, as quais estão definidas na p. 21. Também contém a investigação de todas as álgebras sêxtuplas de uma certa classe, i.e., daquelas que contêm o que é chamado neste trabalho de um elemento idempotente.”

Peirce provou vários teoremas em relação a elementos nilpotentes e idempotentes. Depois investigou os possíveis tipos de álgebras que têm, no máximo, seis elementos na base.

1.3.4 Gauss, Weierstrass e Dedekind

Em 1831, quando falava dos números complexos e seu uso na teoria de números, Johann Carl Friedrich Gauss (1777-1855) levantou a seguinte questão: por que as relações

entre as coisas que representam uma multiplicidade de mais que duas dimensões não podem produzir outros tipos de quantidades permissíveis na aritmética geral?

Em 1883, numa carta a Hermann Amandus Schwarz (1843-1921), Karl Theodor Weiertrass (1815-1897) considerou este problema, dando uma concreta formulação algébrica. A carta foi publicada em 1884, no *Nacrichten der Ges. der Wiss. Göttingen* (pp. 395-414), com o título *Zur Theorie der aus n Haupteinheiten gebildeten complexen Größen*. Neste trabalho, Weiertrass provou o seguinte resultado: *uma álgebra comutativa sobre $\mathbb{R}$, de dimensão $n > 2$, sempre tem divisores do zero*.

No ano seguinte, Richard Dedekind (1831-1916) publicou um artigo, com o mesmo título, no mesmo *Göttingen Nachrichten* (1885, pp. 141-159), onde considerou o problema de um ponto de vista mais geral, provando que *este tipo de álgebra é uma soma direta de cópias do corpo dos números complexos $\mathbb{C}$* .

1.3.5 Theodor Molien

Theodor Molien (1861-1941) nasceu em Riga e estudou na Universidade de Dorpat (atual Tartu) na Estônia. Passou um breve período (1884-85) em Leipzig. No mesmo ano, tornou-se *Dozent* na Universidade de Dorpat e, em agosto de 1891, terminou sua tese *Über Systeme höherer komplexer Zahlen*. Em 1897, publicou dois artigos sobre representações de grupos finitos e, em 1901, tornou-se professor de matemática na Universidade de Tomsk, na Sibéria.

Em sua tese, Molien provou um resultado extremamente importante que, em linguagem moderna, diz: *toda álgebra simples sobre $\mathbb{C}$ é uma álgebra de matrizes completa*. Este teorema é um caso especial de um dos teoremas fundamentais de Wedderburn.

1.3.6 Élie Cartan

Vários resultados obtidos por Molien, em 1891, e publicados em 1893 foram redescobertos por Élie Cartan (1869-1951) e publicados, em 1898, num artigo intitulado *Les Groupes Bilinéaires et les Systèmes de Nombres Complexes*. Parece que Cartan não conhecia o trabalho de Molien, pois a primeira menção feita a ele foi em *Nombres Complexes* de 1908. Neste artigo, Cartan admitiu totalmente as realizações de Molien.

No trabalho de 1898, citado acima, Cartan investigou a estrutura das álgebras simples e semi-simples (soma direta de álgebras simples). A álgebra é suposta ter elemento unidade e é sobre o corpo dos números complexos $\mathbb{C}$. Seu principal teorema, em terminologia moderna, afirma que *toda álgebra sobre $\mathbb{C}$ é uma soma direta de uma subálgebra simples ou semi-simples*

Figura 1.2: Joseph H. M. Wedderburn

e uma subálgebra nilpotente invariante (i.e., ideal bilateral nilpotente). Este resultado pode ser obtido como um caso particular do principal teorema de Wedderburn.

Depois disso, Cartan passou a estudar álgebras simples e semi-simples sobre o corpo dos números reais $\mathbb{R}$.

1.4 Joseph H. M. Wedderburn

Wedderburn nasceu em 26 de fevereiro de 1882, em Forfar, Escócia, e morreu em 9 de outubro de 1948 em Princeton, Nova Jersey. Foi o décimo de catorze filhos. Seu pai, Alexander Wedderburn, era físico numa família de clérigos (pelo lado do pai) e advogados (pelo lado da mãe). Em 1898, matriculou-se na Universidade de Edinburgh; em 1903, recebeu seu grau de mestre em matemática como o primeiro aluno da classe. Influenciado pelos estudos de Friedrich Engel (1861-1941) e Georg Frobenius (1849-1917), seguiu para Leipzig, onde passou o inverno de 1903-1904, e para Berlim no verão seguinte. Durante este período, conheceu o trabalho de William Burnside (1852-1927), que o introduziu à teoria de grupos de Lie e aos sistemas de números hipercomplexos. Após deixar Berlim, passou um breve período na Escócia e depois, no ano acadêmico 1904-1905, foi para a recém-inaugurada Universidade de Chicago (onde estavam E. H. Moore e L. E. Dickson). As pesquisas desenvolvidas durante sua estada, em Chicago, direcionaram sua carreira matemática e ajudaram a projetá-lo internacionalmente.

De 1905 a 1909, Wedderburn deu conferências na Universidade de Edinburgh. Nesta época, editou o *Proceedings of the Edinburgh Mathematical Society* e, em 1908, obteve seu grau de doutor. Quando explodiu a Primeira Guerra Mundial, alistou-se na Armada Britânica e lutou na França. Após a guerra, retornou para a Universidade de Princeton,

onde permaneceu até se aposentar, em 1945. Quando o departamento de matemática de Princeton assumiu a responsabilidade de publicar os *Annals of Mathematics*, Wedderburn foi seu editor, de 1912 a 1928. Perto do fim da década de 1920, sofreu o que parece ter sido um acidente nervoso, o que o levou a se aposentar precocemente. Wedderburn publicou trinta e oito artigos e um livro, *Lectures on Matrices*, em 1934, cujo último capítulo contém um excelente resumo de seus teoremas, assim como algumas contribuições originais ao assunto.

Quando Wedderburn passou a estudar a teoria dos números hipercomplexos, em 1904, havia três enfoques distintos do assunto: o primeiro era originado pela descoberta dos quatérnios, por Hamilton e pela ênfase dada por ele às propriedades algébricas que esta nova álgebra possuía. Pesquisadores subseqüentes, como Arthur Cayley, James Joseph Sylvester (1814-1897) e Benjamin (1809-1880) e Charles S. Peirce (1839-1914), insistiram em considerar suas álgebras como objetos que satisfaziam certas propriedades algébricas, embora seu enfoque fosse diferente do de Hamilton: este partiu das propriedades desejadas para a álgebra para, então, encontrá-la; já os outros, possuíam a álgebra e, daí, obtiveram suas propriedades. Em contraste com esta abordagem, a teoria de Sophus Lie (1842-1899) considerava que sistemas de números hipercomplexos eram a melhor maneira de entender grupos de transformações e, portanto, não mereciam ser estudados independentemente. Esta situação mudou gradativamente, quando Theodor Molien e Élie Cartan começaram a interessar-se pelo assunto e fizeram significantes contribuições para a estrutura desta teoria. No fim da década de 1890, sistemas de números hipercomplexos tornaram-se uma área diferenciada de pesquisa matemática.

No fim de 1904, quando estava na Universidade de Chicago, Wedderburn apresentou à seção de Chicago da *American Mathematical Society*, juntamente com Saul Epstein (1878-19??), o artigo *On the Structure of Hypercomplex Number Systems* ([EW]), no qual provavam o teorema de Jordan-Hölder⁴. Este trabalho mostrou que Wedderburn já conhecia os estudos de Molien e Cartan sobre os números hipercomplexos. As realizações destes matemáticos, em especial de Cartan, serviram de base para uma nova abordagem para a teoria de álgebras, chamada *método racional*. Tal abordagem foi apresentada, inicialmente, no trabalho em conjunto com Epstein. Eles diziam que

“os métodos usados por toda parte são racionais e, então, os resultados aplicam-se aos sistemas de números hipercomplexos, nos quais os coeficientes são restringidos a serem escalares de um dado corpo, finito ou infinito.”

A esta abordagem deve-se todo o sucesso do artigo de Wedderburn *On Hypercomplex Numbers* ([WE3]), publicado em 1907.

⁴O teorema de Jordan-Hölder é um resultado da teoria de grupos finitos para sistemas de números hipercomplexos.

Neste trabalho, Wedderburn retoma os conceitos de elementos idempotentes e nilpotentes, introduzidos, anteriormente, por Benjamin Peirce e utiliza-os para fundamentar seus estudos sobre a classificação de álgebras. Como seus antecessores, concede especial importância ao conceito de *subálgebra invariante*, que corresponde à atual definição de ideal bilateral. Também introduz a noção de *álgebra diferença*, que corresponde à idéia de álgebra quociente e aponta o paralelismo com o quociente de um grupo finito.

Outro conceito fundamental que Wedderburn introduz é o de *álgebra nilpotente*. Ele prova que toda álgebra⁵ contém uma subálgebra invariante nilpotente maximal (eventualmente nula) e que toda outra subálgebra invariante nilpotente está contida nela. Wedderburn não lhe dá nome especial; o termo *radical*, que hoje é usado para designá-la, foi introduzido por Frobenius em 1903. Também apresenta a noção de *álgebra semi-simples*, que é uma álgebra que não contém subálgebras invariantes nilpotentes não nulas. Com isto, prova o seu mais importante resultado sobre a estrutura de álgebras:

Teorema de Wedderburn

1. *Qualquer álgebra é a soma de seu radical N e uma álgebra semi-simples.*
2. *Uma álgebra semi-simples pode ser unicamente expressa como soma direta de álgebras simples.*
3. *Uma álgebra simples é uma álgebra de matrizes sobre uma álgebra com divisão.*

A importância deste teorema é reconhecida pelo próprio autor, que afirma que este resultado

“é muito importante, pois ele nos permite concentrar nossa atenção nas álgebras que não contêm subálgebras invariantes nilpotentes.”

Com *On Hypercomplex Numbers*, a teoria de álgebras ganhou mais força. Como vimos anteriormente, Molien estudou sistemas de números hipercomplexos do ponto de vista das álgebras de Lie e dependia da estrutura destas para provar seus teoremas. Frobenius trabalhou em sistemas de números hipercomplexos como uma maneira de dar aplicações à sua teoria de determinantes. Apenas Cartan, em seu *Sur les Groupes Bilinéaires et les Systèmes de Nombres Complexes*, desenvolveu a teoria das álgebras por ela mesma. Mas todos eles trabalharam com álgebras sobre o corpo dos números reais ou dos números complexos e, na maioria dos casos, suas demonstrações dos teoremas dependiam de algum modo das propriedades destes corpos. Wedderburn viu além de seus predecessores, trabalhou com álgebras de dimensão finita sobre corpos arbitrários e revolucionou a teoria de álgebras, com

⁵Vale ressaltar que, naquela época, as álgebras consideradas eram de dimensão finita.

suas noções elegantes de ideais, sua fatoração em radicais e concentrando-se na parte semi-simples das álgebras. Com seus *métodos racionais*, atacou o *coração* da teoria de álgebras, cujos efeitos são sentidos até hoje.

Também devemos citar as contribuições de Wedderburn à teoria das álgebras com divisão (que serão mais detalhadas ao longo dos próximos capítulos, por estarem bastante relacionadas às descobertas de Dickson). Em 1905 ([WE1]), mostrou que toda álgebra comutativa finita é um corpo de Galois e deu uma classificação completa de todas as álgebras finitas semi-simples⁶, pois estas são álgebras de matrizes sobre álgebras finitas com divisão, que são corpos. Com isto, reduziu a estrutura de grupos semi-simples a de corpos não comutativos, abrindo uma nova linha de pesquisa.

⁶Este teorema também permitiu apresentar, de uma única vez, a estrutura de todas as geometrias projetivas e mostrou que, nestas geometrias, o teorema de Pascal é uma consequência do teorema de Desargues.

Capítulo 2

A Matemática nos Estados Unidos

2.1 Introdução

Neste capítulo, estudamos a trajetória da pesquisa matemática nos Estados Unidos e o papel desempenhado por Leonard E. Dickson no seu desenvolvimento.

Nossos estudos têm início no século XVIII, quando surgiu o revolucionário pensamento iluminista que criticava a sociedade, o governo, a economia, a educação e a religião. Este movimento pregava o conhecimento racional e científico da natureza, acreditava que as ciências deveriam ser desenvolvidas através da aplicação de métodos experimentais e que a sociedade deveria ser mais justa, sendo todos iguais perante à lei. Estas idéias liberais vieram ao encontro dos anseios por liberdade, existentes nas colônias européias na América e culminaram com a independência destas. O primeiro grupo a declarar-se independente foi aquele que depois formaria os Estados Unidos da América.

Os primeiros sinais de desenvolvimento científico no país começaram a aparecer com a fundação de escolas especializadas, na primeira metade do século dezanove, e o surgimento daquele que é considerado o grande fundador da matemática americana: Benjamin Peirce. A pesquisa, nesta área, não parou de crescer, depois da fundação da Universidade Johns Hopkins, em 1876, e da Universidade de Chicago, em 1892. Em Chicago, as presenças de Eliakin H. Moore e, posteriormente, de L. E. Dickson fizeram, desta universidade, o grande centro em pesquisa matemática da época. A partir deste momento, novos centros científicos surgiram e a pesquisa no país tornou-se referência mundial.

2.2 A História da Matemática nos Estados Unidos

Os estudos aqui apresentados seguem a mesma linha adotada por Karen H. Parshal em [PA1]. Dividimos a abordagem da história da matemática, nos Estados Unidos, em três partes: a primeira é dedicada aos cem anos, entre 1776 e 1876, quando o estudo matemático acontecia dentro do contexto de uma comunidade científica emergente; já a segunda parte é dedicada ao quarto de século, de 1876 até 1900, quando emergiu uma comunidade genuinamente americana de pesquisa em matemática propriamente dita e, na terceira parte, estudamos o período após 1900, em que ocorre uma consolidação desta comunidade científica.

2.2.1 O Período entre 1776 e 1876

O século XVIII, especialmente seu último quarto, é marcado por fortes mudanças, no comportamento sócio-cultural, decorrentes de uma nova corrente de pensamento.

Entre os séculos XVII e XVIII, a sociedade européia é dominada pelo absolutismo, que é um sistema de governo no qual o poder está concentrado nas mãos do monarca. Os reis controlam a administração do Estado, formam exércitos permanentes, dominam a padronização monetária e fiscal, estabelecem as fronteiras de seus países e intervêm na economia nacional, por meio de políticas mercantilistas e coloniais. Também criam uma organização judiciária nacional, a justiça real, que se sobrepõe ao fragmentado sistema feudal. Esta centralização do poder desenvolve-se a partir da crise do feudalismo. Com o crescimento comercial, a burguesia tem interesse em disputar o domínio político com os nobres e apóia a concentração do poder. A Reforma Protestante do século XVI também colabora para o fortalecimento da autoridade monárquica, pois enfraquece o poder papal e coloca as igrejas nacionais sob o controle do soberano. Com a evolução das leis, com base no estudo do direito romano, surgem teorias que justificam o absolutismo, como as de Nicolau Maquiavel (1469-1527), Jean Bodin (1530-1595), Jacques Bossuet (1627-1704) e Thomas Hobbes (1588-1679).

O Estado absolutista típico é a França de Luís XIV (1638-1715). Conhecido como o Rei Sol, a ele é atribuída a frase que se tornou o emblema do poder absoluto: *O Estado sou eu*. Na Inglaterra, no início do século XVI, Henrique VIII, segundo rei da dinastia Tudor, consegue impor sua autoridade aos nobres com o apoio da burguesia e assume também o poder religioso. O processo de centralização completa-se no reinado de sua filha Elizabeth I.

No século XVIII, surge o iluminismo, que defende o predomínio da razão sobre a fé, estabelecendo o progresso como o destino da humanidade. Seus principais idealizadores são John Locke (1632-1704), Montesquieu (1689-1755), Voltaire (1694-1778) e Rousseau (1712-1778). Representa a visão de mundo da burguesia intelectual da época e tem suas primeiras manifestações na Inglaterra e na Holanda. Alcança especial repercussão na França, onde se opõe às injustiças sociais, à intolerância religiosa e aos privilégios do absolutismo em

decadência. Influencia também a Revolução Francesa, fornecendo-lhe, inclusive, o lema *Liberdade, Igualdade e Fraternidade*. O iluminismo tem origem no Renascimento, o primeiro grande momento de construção de uma cultura burguesa, na qual a razão e a ciência são as bases para o entendimento do mundo. Para o iluminismo, Deus está na natureza e no homem, que pode descobri-lo por meio da razão, dispensando a igreja. Afirmar que as leis naturais regulam as relações sociais e considera os homens naturalmente bons e iguais entre si: quem os corrompe é a sociedade. Cabe, portanto, transformá-la e garantir a todos liberdade de expressão e culto, igualdade perante à lei e defesa contra o arbítrio. Quanto à forma de governo para a realização da sociedade mais justa, uns defendem a monarquia constitucional (o monarca tem um papel conciliador nos conflitos políticos), outros a república. Em *Ensaio sobre o Entendimento Humano* (1689), o inglês John Locke trata a experiência como fonte do conhecimento, que é organizado depois pela razão. Locke defende também o individualismo liberal contra o absolutismo monárquico. O escritor francês Montesquieu propõe, na obra *Do Espírito das Leis* (1751), a independência dos poderes Executivo, Legislativo e Judiciário como garantia da liberdade. Voltaire critica a Igreja e defende a monarquia comandada por um soberano esclarecido. O suíço Jean-Jacques Rousseau é o iluminista mais radical, precursor do socialismo e do romantismo. No livro *O Contrato Social* (1762), posiciona-se a favor do Estado democrático, voltado para o bem comum e a vontade geral, que inspiram os ideais da Revolução Francesa. Outra obra tipicamente iluminista é *Enciclopédia*, elaborada pelos franceses Denis Diderot (1713-1784) e D'Alembert (1717-1783), com o objetivo de organizar o conhecimento existente na época sobre artes, ciência, filosofia e religião. Na economia, o iluminismo é representado pela fisiocracia, que considera a terra como a única fonte de riqueza de uma nação, e pelo liberalismo econômico, que defende a não intervenção do Estado na economia.

Visto pelos intelectuais como um movimento que ilustrava a capacidade humana de criticar e de almejar um mundo melhor, o iluminismo transformou o século XVIII no chamado *Século das Luzes*.

As idéias iluministas, aliadas à repressão política exercida pelos ingleses, nas suas colônias na América, têm papel importante no processo revolucionário americano. As treze colônias americanas formam-se a partir do século XVII e apresentam um nível de desenvolvimento desigual entre as regiões. O sul é dependente da metrópole, para onde exporta tabaco, anil e algodão e importa produtos manufaturados. Com este tipo de economia, no sul prevalece a grande propriedade escravagista, com reduzido trabalho livre e monocultura voltada à exportação. Já no centro-norte, predominam a pequena e média propriedades, administradas por europeus exilados por motivos políticos ou religiosos. Seus produtos são semelhantes aos europeus, desestimulando o comércio da Inglaterra com a região, pois não havendo carga de volta, o frete torna-se caro. Assim, apesar da proibição de manufaturas nas colônias, os colonos do centro-norte possuem uma certa autonomia industrial: ultrapassam as fronteiras e criam parceiros comerciais. O crescimento do comércio colonial passa, então, a

concorrer com a metrópole. Isto faz com que o Parlamento inglês aumente as taxas sobre os produtos que não vêm da metrópole e são comercializados pelas colônias e acrescente vários itens à lista de produtos que só podem ser exportados para a Inglaterra (criando as chamadas *Leis Intoleráveis*). Os direitos da Coroa sobre as colônias, na América, também são estendidos. Com o descontentamento do proprietário sulista que está sempre endividado com o exportador inglês, os colonos do sul e do norte unem-se para lutar pela sua independência.

Em 1774, dá-se o Primeiro Congresso Continental da Filadélfia, de caráter não-separatista, que envia petição ao rei e ao Parlamento, pedindo a revogação das Leis Intoleráveis, em nome da igualdade de direitos dos colonos. Em 1775, com a morte de alguns colonos num conflito em Lexington, os americanos começam a organizar-se militarmente. O rei declara-os em rebelião e eles passam à revolta aberta. Em 1776, a Virgínia toma a iniciativa e declara-se independente, com uma explícita Declaração dos Direitos dos Homens. O Segundo Congresso da Filadélfia, reunido desde 1775, manifesta desejo separatista e nomeia George Washington, da Virgínia, comandante das tropas americanas. Este encarrega Thomas Jefferson (1743-1826) de redigir a **Declaração da Independência**. Em 4 de julho de 1776, reunidos na Filadélfia, delegados de todos os territórios promulgam o documento com mudanças introduzidas por Samuel Adams e Benjamin Franklin¹.

A guerra pela independência, que havia começado em março de 1775, com a tomada de Boston, num episódio conhecido como a Festa do Chá de Boston², conta com o apoio dos franceses que, estimulados pela propaganda feita por Franklin e imbuídos pelo pensamento iluminista, estão afinados com os ideais de liberdade do movimento e motivados pela intenção de golpear a Inglaterra, que lhes havia proporcionado grandes perdas em 1763 (Guerra dos Sete Anos). Com a ajuda francesa, os americanos conseguem vencer o exército inglês e, em 1783, o Tratado de Versalhes reconhece a independência dos Estados Unidos da América.

Foi neste período de construção de novas idéias e cultura e uma nova economia, que começaram a aparecer os primeiros sinais do desenvolvimento de uma comunidade científica nos Estados Unidos³. Gradativamente, foram ocorrendo mudanças na educação superior e

¹ Diz-se que a única razão pela qual Franklin não escreveu totalmente a Declaração da Independência é porque incluiria muitas piadas, característica de sua personalidade.

² Comerciantes disfarçados de índios *mohawks* destruíram trezentas caixas de chá tiradas dos barcos ingleses, em reação à Lei do Chá, que dava o monopólio deste produto à Companhia das Índias Orientais.

³ Benjamin Franklin já havia dedicado-se à pesquisa científica, em que formulou uma teoria interessante sobre origem e direção das tempestades; fez observações sobre causas e estrutura dos ciclones; estudou a natureza das correntes marítimas; investigou o fenômeno da condução do calor; pesquisou sobre óptica, cuja aplicação resultou nas lentes bifocais. Contudo, suas mais importantes pesquisas deram-se em eletricidade, com o famoso experimento, em 1752, que possibilitou a construção dos pára-raios: enquanto cientistas do mundo inteiro discutiam se o raio era ou não um fenômeno elétrico, Franklin saiu em meio a uma tempestade e conseguiu atrair um raio para uma chave, presa na ponta de um papagaio que empinava. Também cabe a Franklin a idéia da primeira biblioteca pública da Filadélfia, e de toda a América, e a criação de uma escola que deu origem à primeira universidade dos Estados Unidos: a Universidade da Pensilvânia.

seus ideais, com a formação de sociedades científicas, a criação de jornais especializados e com o aumento do suporte financeiro, por parte do governo federal, para a pesquisa científica, para as faculdades e as universidades.

Durante a primeira metade do século XVIII, a matemática no país era ensinada de modo superficial e os estudantes tinham acesso apenas a traduções dos “Elementos” de Euclides, juntamente com alguns trabalhos rudimentares em aritmética, trigonometria e álgebra. Assim, era difícil aos estudantes americanos atingir o nível de sofisticação e desenvolvimento teórico necessários, para entender os trabalhos matemáticos desenvolvidos no continente europeu, naquela ocasião.

Entretanto, na segunda década do século XIX, alguns professores de matemática perceberam que o problema estava no modo como esta ciência era apresentada aos estudantes e encontraram, principalmente na França, uma abordagem pedagógica mais interessante que a inglesa (até então adotada) para a álgebra, a geometria, a trigonometria e o cálculo, desenvolvida em trabalhos datados do fim do século XVIII, por autores como Lacroix (1765-1843), Bezout (1739-1783) e Legendre (1752-1833). Estes educadores trouxeram tais materiais para dentro de suas salas de aula, através de traduções e adaptações.

As décadas seguintes, de 1830 até 1870, foram de grande desenvolvimento científico, com os americanos percebendo seu grande potencial intelectual ainda a ser explorado. Em busca do aprimoramento da atividade científica semelhante à européia, que recebia grande incentivo e se tornava cada vez mais diferenciada e especializada, algumas universidades americanas, como Yale em 1846 e Harvard em 1847, fundaram suas escolas científicas especializadas. Em Harvard, por exemplo, Benjamin Peirce (sobre quem estudaremos mais detalhadamente na sequência) ministrou, em 1848, um curso, em matemática e mecânica celeste, no qual incorporou alguns dos últimos trabalhos desenvolvidos acerca do assunto. Seus alunos estudaram não somente as pesquisas sobre quatérnios de Hamilton, mas também as publicações nas quais John Couch Adams (1819-1892) e Urbain Leverrier (1811-1877) deduziram, independentemente, e usando matemática, a existência do planeta Netuno. Isto marcou o início do “profissionalismo” para os cientistas americanos.

Entretanto, apesar do aumento dos cientistas profissionais nas universidades e no governo, nenhum grupo destes especialistas tinha número suficiente de membros para sustentar periódicos especializados ou sociedades. No início dos anos 40, geólogos americanos tentaram organizar-se numa sociedade especializada, mas tiveram que unir forças com os naturalistas, pois seus membros eram em número reduzido. Em 1847, eles fundaram a Associação Americana para o Desenvolvimento da Ciência, uma sociedade para cientistas de todas as especialidades. Este grupo, num esforço para atrair o maior público científico possível, realizava suas reuniões em regiões variadas e, a fim de disseminar a informação científica mais rapidamente, também publicava seus *Proceedings*.

Apesar de todos estes esforços para estimular o desenvolvimento científico, o país

Figura 2.1: Benjamin Peirce

ainda carecia de centros especializados em matemática de alto nível: os estudantes que desejavam aprofundar-se mais, em suas pesquisas, ainda tinham que viajar para o exterior. Entretanto, como veremos, o panorama mudou após a fundação da Universidade Johns Hopkins, no ano de 1876, em Baltimore.

2.2.2 Benjamin Peirce

No ano de 1836, a matemática, na Universidade de Harvard, passou por um período de transição, com a saída de John Farrar (1779-1853), que durante trinta anos foi responsável por introduzir os fundamentos da matemática, da física e da astronomia aos estudantes desta universidade. Este posto passou, então, para Benjamin Peirce (1808-1880) e Joseph Lovering (1813-1892) que contribuíram, ativamente, pelos quarenta e quatro anos seguintes.

Farrar assumiu o posto de *Hollis Professor* de matemática e filosofia natural, em 1806, após Nathaniel Bowditch (1773-1838) ter declinado do convite. Bowditch, um autodidata em latim e nos ensinamentos de Newton (estudou o *Principia*), tornou-se famoso após traduzir o *Mécanique Céleste* de Pierre-Simon Laplace (1749-1827), onde explicou, em detalhes, vários tópicos que originalmente estavam resumidos. Seu interesse científico era compartilhado pelo jovem Peirce, que havia sido companheiro de seu filho em Harvard, e que o ajudou na tarefa de editar e publicar (com recursos próprios) o *Mécanique Céleste*, em 1829.

Em 1831, Peirce tornou-se *tutor* em matemática, em Harvard e em 1833, foi nomeado *professor* de matemática e filosofia natural. Em 1835, Peirce já havia escrito sete livros-texto para os cursos de Harvard, cujos assuntos variavam de geometria plana à mecânica e astronomia. Em 1836, com a crescente fragilidade da saúde de seu mentor (Farrar), Peirce

assumiu a responsabilidade, junto com Lovering, de conduzir os ensinamentos de matemática, física e astronomia, tornando-se *professor sênior*.

Seu interesse por matemática, em detrimento das outras ciências, parece ter-se consolidado com a publicação dos primeiros trabalhos de Hamilton sobre os quatérnios, no fim da década de 1840. Seu interesse pelo assunto foi tanto que, em 1848, mesmo ano em que Hamilton deu suas primeiras conferências sobre os quatérnios, Peirce passou a incluir este tópico em suas aulas em Harvard. Como consequência dos estudos das idéias e exemplos de Hamilton, elaborou seu grande trabalho *Linear Associative Algebra*, publicado em 1871, em forma de litografia: Peirce fez apenas cem cópias do artigo e distribuiu a seus amigos e conhecidos, arcando com todas as despesas. Talvez pelo fato desta obra não ter sido conhecida na Europa⁴ ou talvez porque Peirce fez e distribuiu poucas cópias deste trabalho com suas idéias sobre álgebra, estas permaneceram desconhecidas até a publicação do artigo, em 1881, no *American Journal of Mathematics* ([PE]), com diversas notas e acréscimos de seu filho, também matemático, Charles Sanders Peirce. Entretanto, outro motivo para este artigo ter passado despercebido pela comunidade matemática européia pode ter sido seu caráter mais filosófico do que matemático, com Peirce definindo matemática como uma ciência lógica. Esta definição foi revolucionária e muito importante, para o desenvolvimento desta ciência. Nas páginas iniciais deste trabalho, Peirce define matemática como

“... a ciência que tira conclusões necessárias”

e defende seu ponto de vista dizendo:

“A definição de matemática é mais ampla que aquela dada ordinariamente e pela qual seu alcance é limitado à pesquisa quantitativa. A definição ordinária, como aquela de outras ciências, é objetiva, enquanto esta é subjetiva. Investigações recentes, das quais os quatérnios são a instância mais notável, tornam manifesto que a definição antiga é demasiado restrita. A esfera da matemática é aqui estendida, em acordo com a derivação de seu nome, a todas as pesquisas demonstrativas, assim como para incluir todos os conhecimentos capazes de ensinamentos dogmáticos ...”

Na mesma perspectiva, afirma:

“É importante, portanto, separar o trabalho intelectual da forma externa. Símbolos devem ser adotados, e a matemática tratada por estes símbolos é chamada álgebra. Álgebra, então, é matemática formal.”

⁴Peirce enviou, em 1870, trinta e três cópias de seu trabalho para seu amigo George Bancroft (1800-1890), que estava na Alemanha, para que este distribuisse o material para a comunidade matemática deste país. Entretanto, não se sabe se Bancroft não apresentou a obra de Peirce aos alemães ou se eles não se interessaram pelo assunto.

Antes de iniciar a discussão matemática, Peirce continua sua perspectiva filosófica dizendo que uma álgebra é constituída por um *alfabeto* formado pelos elementos da base; um *vocabulário* que consiste das operações da álgebra; e uma *gramática* que define as regras de composição dos elementos da álgebra (isto é, os axiomas de estrutura). Explicitamente, define:

“Uma álgebra na qual toda expressão pode se reduzir à forma de uma soma algébrica de termos, cada um dos quais consiste de uma única letra com um coeficiente quantitativo, é chamada uma álgebra linear.”

Baseado nestes conceitos preliminares, Peirce, então, tenta determinar as diversas álgebras possíveis, obtendo as tabelas de multiplicação dos elementos de uma dada base e, para isso, procura métodos para escolher adequadamente os elementos desta base. Nesta tentativa, consegue determinar 154 álgebras, não isomorfas, de dimensão menor ou igual a seis. A grande diversidade de possibilidades para dimensões tão baixas mostra claramente que o caminho escolhido não é adequado. Porém, este trabalho (*Linear Associative Algebras*) foi muito importante, pois na tentativa de escolher e classificar elementos, Peirce introduz algumas das notações mais importantes associadas à teoria de álgebras. Por exemplo, suas álgebras podem conter elementos que são divisores do zero, ou **nilfatores** como ele os chama; elementos **nilpotentes**, isto é, elementos a para os quais existe um inteiro positivo n tal que $a^n = 0$; e elementos **idempotentes**, isto é, elementos e tais que $e^2 = e$. Outra novidade apresentada neste trabalho é que Peirce considera, pela primeira vez, álgebras que podem não ter unidade. Com estes conceitos estabelecidos, Peirce encontra-se, então, em condições de desenvolver sua teoria e prova um resultado fundamental: *toda álgebra (de dimensão finita) possui, pelo menos, um elemento idempotente ou um elemento nilpotente*.

Uma contribuição importante a esta teoria, e que também merece destaque, é a decomposição de uma álgebra A em soma direta, associada a um elemento idempotente e dado (que ficou conhecida como *decomposição de Peirce*): definindo-se

$$B_1 = \{x \in A : xe = 0\},$$

$$B_2 = \{x \in A : ex = 0\},$$

$$B = B_1 \cap B_2,$$

tem-se que

$$A = eAe \oplus eB_1 \oplus B_2e \oplus B.$$

O trabalho de Peirce teve pouca repercussão, no princípio; entretanto, tornou-se fundamental para o desenvolvimento da teoria de álgebras e para que Joseph H. M. Wedderburn (1882-1948) provasse um dos resultados mais importantes sobre classificação de álgebras (mostrado em (1.4)).

2.2.3 O Período entre 1876 e 1900 e a Fundação da Universidade Johns Hopkins

Um dia antes do Natal de 1873, o milionário de Baltimore, Johns Hopkins (que era solteiro), faleceu e deixou toda sua fortuna de sete milhões de dólares para a fundação de uma universidade e de um hospital. Enquanto planejavam a fundação da universidade, os curadores receberam orientação de três presidentes de universidades (que também eram cientistas): Charles William Eliot, presidente de Harvard no período de 1869 a 1909; James Burril Angell, presidente de Michigan de 1871 a 1909; e Andrew Dixon White, presidente de Cornell de 1866 a 1885. Eles decidiram entrevistar Daniel Coit Gilman (1831-1908), que à época era presidente da Universidade da Califórnia. Gilman, que tinha viajado muito ao exterior, a fim de conhecer melhor os métodos educacionais, principalmente das instituições da Inglaterra, da França e da Alemanha, deixou claro que queria criar uma universidade de caráter nacional, com o objetivo de promover a pesquisa científica, num nível mais avançado. Como os curadores já estavam inclinados nesta direção, concordaram com ele e o convidaram para ser o primeiro presidente da Universidade Johns Hopkins, o que aceitou prontamente.

Gilman criou um novo modelo institucional no país, com base em suas análises dos pontos fortes e dos pontos fracos das universidades estrangeiras e nas necessidades dos Estados Unidos. Esta universidade adotou, como parte de sua missão, a produção de uma pesquisa original e o treinamento de futuros pesquisadores, em adição ao objetivo tradicional de prover uma educação de alta qualidade para universitários.

Para ensinar matemática, Gilman contratou James Joseph Sylvester (1814-1897), um algebrista britânico com reputação internacional conquistada, principalmente, com os estudos em teoria de grupos invariantes. Junto com William E. Story (1850-1930), recém-doutorado pela Universidade de Leipzig, supervisionou, durante o período de 1876 a 1883, um programa de pós-graduação em matemática, cujo nível era elevadíssimo: nem mesmo o currículo de Harvard possuía o mesmo nível.

Em 1883, Sylvester voltou para a Inglaterra, para assumir posição de professor, em Oxford e Gilman não conseguiu substituí-lo por um matemático americano de igual talento. Com isto, os estudantes americanos, que desejavam um treinamento mais sofisticado, voltaram a procurar os grandes centros europeus, em especial Göttingen na Alemanha, onde Felix Klein (1849-1925) oferecia um treinamento de alta qualidade.

Klein, que é mais conhecido por seu trabalho em geometria não-euclidiana e por desenvolver uma conexão entre a geometria e a teoria de grupos, recebeu seu doutorado em 1868, pela Universidade de Bonn, sob a orientação de Julius Plücker (1801-1868), com a dissertação *Über die Transformation der allgemeinen Gleichung des zweiten Grades zwischen Linien-Koordinaten auf eine kanonische Form*, que trata de geometria e suas aplicações à mecânica. No ano em que Klein recebeu seu doutorado, Plücker morreu, deixando incompleta

a maior parte de suas pesquisas sobre os fundamentos da geometria. Klein era, então, a pessoa mais indicada para completar a segunda parte do trabalho de Plücker *Neue Geometrie des Raumes*, o que lhe proporcionou reconhecimento no meio matemático. Após ter passado por Erlangen, Munich e Leipzig, Klien mudou-se para a Universidade de Göttingen, em 1886, onde permaneceu até se aposentar em 1913, formando um centro de pesquisas em matemática — que contou com a presença e as idéias de David Hilbert (1862-1943), a partir de 1895 — e que servia como modelo para o restante do mundo.

A primeira descoberta importante de Klien deu-se em 1870, com a colaboração de Sophus Lie (1842-1899): descobriram as propriedades fundamentais das linhas assintóticas numa superfície de Kummer. Ainda com Lie, trabalhou na investigação de W-curvas, isto é, curvas invariantes por um grupo de transformações projetivas. Em 1871, realizou importantes descobertas em geometria: publicou dois artigos *On the So-called Non-Euclidean Geometry*, nos quais mostrou que é possível considerar a geometria euclidiana e a geometria não-euclidiana como casos especiais de uma superfície projetiva com uma seção cônica específica adicionada. Este resultado teve o notável corolário que afirma que *a geometria não-euclidiana é consistente se, e só se, a geometria euclidiana é consistente*. Com isto, desapareceu a dúvida que ainda havia sobre a existência da geometria não-euclidiana, colocando-a no mesmo nível da geometria euclidiana.

Logo, os estudantes americanos que foram para a Alemanha, para aprimorar suas pesquisas, trouxeram para os Estados Unidos a influência dos ensinamentos e idéias de Klein. A partir daí, estabeleceram vários programas de pós-graduação pelo país, sendo que as universidades Clark, em 1889, e de Chicago, em 1892, já foram fundadas com estes programas. A Universidade de Chicago (cuja história como centro emergente de pesquisa matemática será estudada em detalhes mais adiante), com seu departamento de matemática sob o comando de Eliakin Hastings Moore (1862-1932) — estudante de Yale — junto com os estudantes de Klein — Oskar Bolza (1857-1942) e Heinrich Maschke (1853-1908) — quase que imediatamente se tornou líder em pesquisas matemáticas de alto nível e em organizar comunidades para o desenvolvimento científico.

O ativismo deles, e particularmente de Moore, ganhou repercussão nacional com a organização da *World's Columbian Exposition* em Chicago no ano de 1893, que contou com a presença de Felix Klein. Este apresentou, no Congresso, vários artigos de sua autoria e dos melhores autores de seu país, como Hilbert, Herman Minkowski (1864-1909), Max Noether (1844-1921) e Heinrich Weber (1842-1912).

Em 1888, foi fundada a *New York Mathematical Society*, com apenas seis membros na reunião inaugural. Entretanto, esta comunidade cresceu e, em 1891, contava com cerca de duzentos membros e já havia iniciado a publicação regular de seus *Bulletins* com suas atividades. Com a aproximação de Moore e outros organizadores do congresso de Colúmbia à *New York Mathematical Society*, esta sociedade teve seu nome mudado, em 1897, para

American Mathematical Society, a fim de refletir seu caráter nacional.

2.2.4 O Período após 1900 - O Crescimento da Matemática nos Estados Unidos

Antes da Primeira Guerra Mundial, o departamento de matemática da Universidade de Chicago continuou a exercer um papel de liderança no cenário nacional, apesar da morte de Maschke, em 1908 e do retorno de Bolza à Alemanha, em 1910. Moore permanecia à frente do departamento, junto com os estudantes formados na própria universidade, Dickson e Gilbert A. Bliss (1876-1961), e também Ernest J. Wilczynski (1876-1932), um geômetra que estudou em Berlim. Neste período, Moore já havia passado a dedicar-se à “análise geral” (na primeira década do século), que é uma abordagem axiomática e abstrata da análise funcional, e o trabalho de Dickson (que provavelmente é o mais importante algebrista do início do século vinte) começava a sobressair como o continuador natural das idéias de Peirce e Hamilton, em álgebra. Sua definição de 1923, presente em *Algebras and their Arithmetics* ([229]), de conjunto de *elementos inteiros* de uma álgebra linear associativa com unidade sobre o corpo dos números racionais, mostrou novos caminhos para o desenvolvimento da teoria de ideais por Emil Artin (1898-1962), Helmuth Hasse (1898-1979) e Emmy Noether (1882-1935), entre outros. Também podemos citar seus estudos acerca dos teoremas de estrutura de Wedderburn ([WE2]), que até então haviam passado despercebidos e possibilitaram observar que o estudo de álgebras simples se reduz ao das álgebras com divisão — fundamental no desenvolvimento da teoria de álgebras. Seus estudos, juntamente com os de Bliss e Wilczynski, ajudaram a solidificar a tradição de Chicago em álgebra abstrata e geometria. Entretanto, antes da Primeira Guerra, muitos estudantes ainda iam graduar-se ou fazer pós-graduação no exterior, principalmente em Göttingen. Porém, isto sofreu uma pausa durante o conflito, com muitos pesquisadores desenvolvendo pesquisas ligadas à guerra. Por exemplo, um dos estudantes de Hilbert, Max Mason (1877-1961) trabalhou em técnicas de detecção de submarinos no recém-formado *National Research Council*. Após a guerra, com a derrota da Alemanha e seu conseqüente declínio cultural e econômico, os matemáticos não tinham mais este país como centro de referência de idéias e desenvolvimento científico e, então, resolveram desenvolver suas pesquisas em seu próprio território, crescendo assim o número de “escolas”, cujas pesquisas eram de alto nível, como Berkeley, MIT (*Massachusetts Institute of Technology*), Harvard e Princeton.

Em 1930, foi fundado, com a colaboração de Oswald Veblen (1880-1960), um instituto de pesquisas, o *Institute for Advanced Study* (com a cooperação institucional de Princeton), que abrigou refugiados europeus do pós-guerra, como por exemplo Albert Einstein (1879-1955) e Hermann Weyl (1885-1955), vindos da Alemanha, e o húngaro John von Neumann (1903-1957).

Mais um conflito deu-se no mundo a partir de 1939 e os Estados Unidos entraram nele e, mais uma vez, seus matemáticos participaram de pesquisas ligadas à guerra. O líder da mobilização matemática era Warren Weaver (1894-1979), que foi professor e chefe do departamento de matemática da Universidade de Wisconsin e chefe do *Rockefeller Foundation's Natural Sciences Division*. Em 1942, o *Office of Scientific Research and Development*, sob Vannevar Bush (1890-1974), criou o *Applied Mathematics Panel*, para dar suporte matemático aos seus vários ramos. Os esforços de seus matemáticos, como Samuel Vilks e John von Neumann, resultaram na criação de várias áreas, como por exemplo a análise sequencial. Assim, no fim da segunda guerra, os contornos da pesquisa matemática americana tinham sido totalmente reconfigurados e os Estados Unidos, agora, possuíam centros de matemática pura e aplicada.

O surgimento destas novas frentes e aplicações matemáticas deram início à chamada matemática de otimização, com a introdução, por exemplo, da programação linear, da teoria dos jogos (desenvolvida por von Neumann e que tem grande aplicabilidade na teoria econômica) e do controle estocástico. Estas pesquisas passaram a ganhar apoio financeiro federal, sendo desenvolvidas principalmente no *Office of Naval Research* (agência federal de suporte à pesquisa acadêmica), fundado em agosto de 1946. Em 1950, a captação de recursos para a pesquisa científica ganhou novo ânimo, com a fundação da *National Science Foundation* (NSF). Embora não tenha apresentado nenhum resultado significativo até 1957, com o lançamento do Sputnik, a NSF tornou-se a principal fonte de captação de recursos para a comunidade matemática americana. Com a criação destas agências e outras que surgiram posteriormente, o desenvolvimento da pesquisa, no país, não parou de crescer e os Estados Unidos tornaram-se um dos maiores centros científicos do mundo: ao contrário do que ocorria no século XIX e no início do século XX, quando os estudantes interessados em desenvolver pesquisas matemáticas, de alto nível, tinham que ir para a Europa, hoje os estudantes de todo o mundo reconhecem as universidades americanas como grandes centros científicos.

2.3 A Matemática na Universidade de Chicago

A Universidade de Chicago foi fundada em 1892 e teve como primeiro presidente William Rainey Harper (1856-1906), que construiu estruturas acadêmica e administrativa inigualáveis na época, financiadas por John D. Rockefeller (1839-1937). Com políticas de incentivo à pesquisa e aulas de excelente nível⁵, ele conseguiu atrair gente da melhor qualidade

⁵Segundo citação em [PA3], e traduzido livremente por nós, Harper sugeriu (no *The President's Report: Administration - The Decennial Publications*, 1st series, v. 1, University of Chicago Press, (1903), pp. XXV):

“4. Devem ser fornecidas bolsas de pesquisa para os professores, com as quais possam, ou não, lecionar de acordo com o que seja mais interessante para o trabalho no qual estejam en-

Figura 2.2: Eliakim Hastings Moore

para sua universidade⁶. Harper perseguiu seus ideais e não abriu mão deles nem mesmo quando foi pressionado a estabelecer uma escola de Engenharia em Chicago: negou-se a sacrificar o progresso científico já alcançado com as pesquisas, e o que ainda estaria por vir, e tentou contornar o problema de outras maneiras, juntando forças com o *Chicago Manual Training School* e o *Armour Institute of Technology*. Embora estas soluções não tenham funcionado, Harper não mudou de idéia e continuou a privilegiar o desenvolvimento científico.

A fim de estruturar a universidade, criou o posto de chefe de departamento (*Head Professor*), cuja missão era construir seus vários departamentos. O *Head Professor* seria responsável, segundo Harper determinou, por supervisionar o trabalho do departamento, preparar todos os exames de admissão e aprovar todas as provas preparadas pelos demais professores, estabelecer os cursos oferecidos, examinar todas as teses apresentadas no departamento, determinar textos a serem usados, editar jornais e artigos apropriados, conduzir seminários, verificar a necessidade de livros e periódicos, definir com o presidente a contratação de outros professores e assinar os certificados dos cursos oferecidos no departamento.

volvidos. Esta é, praticamente, a característica das bolsas para os professores no Observatório [Yerkes]. Devem existir postos em outros departamentos, talvez um posto em cada departamento, para os quais devem ser feitas nomeações permanentes, ou que podem ser ocupados por um período longo ou curto, por vários membros do departamento, capazes de realizar trabalhos de pesquisa ...

6. Ajustes devem ser feitos para encorajar um grande número de homens a devotar seis dos doze meses à pesquisa e investigação e dedicar os outros seis meses ao trabalho de lecionar. Este plano já tem sido adotado em vários casos individuais ..."

⁶O maior êxodo ocorreu na Universidade Clark, onde quase metade de seus talentosos pesquisadores foi para Chicago.

Para comandar o departamento de matemática, Harper trouxe o jovem Eliakin Hastings Moore (1862-1932), cujo primeiro contato com a pesquisa científica, em matemática, deu-se quando trabalhou, pelo período de um verão, como assistente de pesquisa de Ormond Stone (1847-1933) — chefe do Observatório de Cincinnati — cuja pesquisa era mais voltada para a matemática do que para a astronomia. Quando Moore foi para Yale, como estudante de graduação, sofreu a influência de outro matemático e astrônomo, Hubert A. Newton (1830-1896), sobressaindo-se em astronomia, inglês e latim, além, é claro, de matemática. Em 1883, graduou-se e, dois anos mais tarde, doutorou-se em matemática sob a orientação de Newton, com a tese intitulada *Extensions of Certain Theorems of Clifford and Cayley in Geometry for n Dimensions*. Newton percebeu, então, que Moore havia progredido em suas pesquisas, tanto quanto o desenvolvimento científico americano lhe permitia, e o encorajou a continuar seus estudos na Alemanha. Parando inicialmente em Göttingen, no verão de 1885, onde também estudou alemão, seguiu para Berlim, no semestre seguinte, onde as pesquisas matemáticas eram dominadas por Karl Weierstrass (1815-1897) e Leopold Kronecker (1823-1891), cujas idéias nortearam as pesquisas de Moore durante toda sua carreira. Voltando aos Estados Unidos, foi professor na *Academy at Northwestern University* durante o ano de 1886 e, após este período, foi para Yale, onde foi promovido a professor associado, dois anos depois. Em 1892, transferiu-se para a Universidade de Chicago.

Quando Moore chegou a Chicago, imediatamente indicou um matemático alemão que havia estudado em Berlim e Göttingen e que estava na Universidade Clark: Oskar Bolza (1857-1936).

Bolza veio para os Estados Unidos em 1888, à época com trinta e cinco anos de idade, para tentar uma nova vida acadêmica, uma vez que não teve sucesso na Alemanha. Em 1875, foi para a universidade em Berlim e deixou seus estudos na escola técnica, após dois semestres, para estudar física. Entretanto, em 1878 percebeu que nunca conseguiria ser um físico e passou a dedicar-se à matemática pura. No período de 1878 a 1881, Bolza estudou matemática com Elwin Bruno Christoffel (1829-1900) e Theodor Reye (1838-1919), em Strasbourg, com Hermann Amandus Schwarz (1843-1921), em Göttingen e com Karl Theodor Wilhelm Weierstrass (1815-1897), em Berlim. O curso de cálculo das variações ministrado por Weierstrass, em 1879, despertou o interesse de Bolza pelo assunto e orientou suas pesquisas para o doutorado. Entretanto, após dois anos dedicados a estes estudos, Bolza descobriu que Edouard Jean-Baptiste Goursat (1858-1936) já havia obtido os mesmos resultados e de um modo mais elegante. Isto motivou Bolza a fazer uma pausa nas suas pesquisas e foi lecionar no *Gymnasium* em Freiburg. Em 1884, depois de se firmar como professor, retornou aos seus estudos e, em 1886, completou sua tese em funções hiperelípticas, sob a orientação de Klein, na Universidade de Göttingen, onde passou o ano acadêmico de 1886-1887. Lá participou de seminários, junto com Heinrich Maschke (1853-1908), dirigidos por Klein. O trabalho junto com Klein deixou-o com dúvidas a respeito de sua capacidade de almejar um posto na universidade e ele, então, resolveu deixar a Alemanha, em 1888, em

busca de oportunidades acadêmicas nos Estados Unidos. Com uma carta de recomendação de Klein, Bolza bateu às portas da Universidade Johns Hopkins, onde trabalhou durante o ano de 1889. Em seguida, foi para a Universidade Clark, onde permaneceu até 1892. A possibilidade de uma promissora carreira oferecida por Harper convenceu Bolza a mudar-se para Chicago e a indicar seu velho amigo alemão Maschke⁷.

Maschke entrou na Universidade de Heidelberg em 1872, onde estudou com Leo Königsberger (1837-1921). Continuou seus estudos na Universidade de Berlim com alguns dos nomes mais proeminentes da época, como Weierstrass, Ernest Eduard Kummer (1820-1893) e Kronecker. Seguindo com suas pesquisas, foi para Göttingen, onde obteve seu doutoramento em 1880, sob a orientação de Klein, seis anos antes que Bolza. Assim como ele, foi lecionar no *Gymnasium*, em Berlim, enquanto não conseguia um posto na universidade. Entretanto, como a competição era muito grande, Maschke seguiu os passos de seu amigo e foi para os Estados Unidos, em 1891. Com o objetivo de manter-se financeiramente, antes de deixar a Alemanha, Maschke estudou por conta própria e tornou-se um eletricitista. Isto lhe possibilitou um emprego na *Weston Electric Instrument Company*, em Newark, nos Estados Unidos. Embora isto bastasse para seu sustento, não satisfazia suas necessidades intelectuais como matemático. A oferta de Harper era tudo que almejava naquele momento e também mudou-se para Chicago.

Apesar das dúvidas iniciais de Bolza e de Maschke a respeito da associação com o jovem Moore, estes homens completavam-se perfeitamente⁸ e tiveram um grande sucesso na organização do departamento de matemática da Universidade de Chicago.

Logo no início, em 1892, fundaram o *Mathematical Club*, onde as pesquisas eram apresentadas e discutidas. Esta experiência proporcionou-lhes, junto com Henry S. White (1861-1943), de Northwestern, cujo doutoramento foi obtido sob orientação de Klein em Göttingen, a incumbência de organizar o *World's Columbian Exposition* que aconteceu em Chicago, em 1893, para comemorar o quarto centenário da descoberta dos Estados Unidos. Este congresso contou com a presença de matemáticos vindos da Áustria, Itália e Alemanha (com a presença marcante de Felix Klein) e de vários estados americanos. Seu caráter internacional deve-se não apenas à presença destes pesquisadores, mas, principalmente, aos artigos apresentados: dos trinta e nove trabalhos, apenas treze foram escritos por americanos; treze eram de alemães, três de italianos, um suíço, três franceses, dois austríacos e um russo.

⁷Durante as negociações com Harper, Bolza impôs a condição de que seu amigo também deveria ser contratado.

⁸Conforme citado em [LA], G. A. Bliss — que estudou em Chicago na época — escreveu:

“Moore was brilliant and aggressive in his scholarship, Bolza rapid and thorough, and Maschke more brilliant, sagacious and without doubt one of the most delightful lectures on geometry of all times.”

(“Moore era brilhante e agressivo em sua erudição, Bolza rápido e minucioso, e Maschke mais brilhante, sagaz e, sem dúvida, um dos mais deliciosos professores de geometria de todos os tempos”).

Dentre estes autores, destacam-se Hermite, Hilbert, Minkowski, Netto, Max Noether, Study e Weber.

Após o encerramento do congresso, Moore e outros matemáticos participaram por duas semanas de um curso ministrado por Klein, na Universidade Northwestern. Após o retorno de Klein à Alemanha, Moore e White perceberam a necessidade e a importância de organizar-se encontros mais frequentes, e de caráter nacional, para discutir matemática e apresentar trabalhos: em 1^o de julho de 1894, acontecia a primeira reunião desta *sociedade*. Entretanto, Moore percebeu que, para esta sociedade ter um caráter realmente nacional, deveria abranger todas as regiões do país e, numa conferência realizada em Chicago, nos dias 31 de dezembro de 1896 e 1^o de janeiro de 1897, propôs a criação de seções: nascia, assim, a *American Mathematical Society* (AMS), com sua primeira reunião oficial ocorrendo em 24 de abril de 1897⁹.

Nos anos seguintes, Moore e seus colegas tentaram estimular a atmosfera intelectual que prosperava na Universidade de Chicago: na qualidade de chefe do departamento de matemática, Moore proveu a biblioteca com um grande número de jornais de primeira linha que serviram de referência, para os estudantes e pesquisadores em matemática daquela universidade. O sucesso de seus esforços, para construir um departamento voltado para pesquisas de alto nível e uma comunidade matemática de caráter nacional, é verificado na qualidade das teses defendidas nesta universidade: entre seus autores, destacam-se alguns dos mais brilhantes matemáticos do século vinte, como o algebrista Leonard E. Dickson, o geômetra Oswald Veblen e o físico-matemático George D. Birkoff¹⁰.

Veblen doutorou-se sob a orientação de Moore, em 1903 e, após ter permanecido por dois anos como professor associado em Chicago, foi para Princeton. Em 1932, transferiu-se para o recém-criado *Institute for Advanced Study*, onde realizou pesquisas de alto nível.

Embora também tenha sido supervisionado por Moore em sua tese, Birkoff tinha interesse nos resultados de Henri Poincaré (1854-1912) e seguiu suas pesquisas na direção dos sistemas dinâmicos. Assim como Veblen, ele foi para Princeton e transferiu-se para Harvard, em 1912, onde supervisionou um grande número de teses. Seu maior reconhecimento internacional deu-se com a nomeação para presidente do *International Congress of Mathematicians* que aconteceu em 1941, em Cambridge.

Estes três homens (Dickson, Veblen e Birkoff) produziram cerca de seiscentos artigos, trinta livros e supervisionaram quase duzentas teses! Ainda mais: editaram jornais especializados e cada um deles foi presidente da AMS. Assim como Moore, também Veblen e Birkoff ajudaram a construir departamentos fortes em suas instituições. Já Dicksonaju-

⁹Moore foi eleito presidente da AMS, em dezembro de 1900, e permaneceu à frente da sociedade por dois anos.

¹⁰Também podemos citar o topólogo Robert L. Moore, que se tornou famoso pelo seu *método Moore* de ensinar.

dou a manter a tradição da excelência em matemática que Chicago representava no cenário nacional.

2.4 Leonard Eugene Dickson

Leonard Eugene Dickson nasceu em Independence, Iowa, em 22 de janeiro de 1874 e casou-se com Susan Davis, em 30 de dezembro de 1902, tendo dois filhos, Campbell e Eleanor. Morreu em 17 de janeiro de 1954 em Harlingen, no Texas. Frequentou a escola primária e secundária em sua cidade natal e, em seguida, ingressou na Universidade do Texas, onde foi encorajado por George B. Halsted (1853-1922) a estudar matemática. Graduou-se em 1893 como o melhor aluno de sua classe e prosseguiu lecionando nesta universidade. Em 1894, sob a supervisão de Halsted, recebeu o grau de mestre pela Universidade do Texas. Dickson, então, requereu ingressar no doutorado em Harvard e na recém-criada Universidade de Chicago. Foi aceito na primeira mas, após ser também aceito em Chicago, decidiu-se pela segunda, onde estudou sob a supervisão de Eliakim H. Moore, mas também foi influenciado pelos outros grandes nomes do departamento de matemática: Oskar Bolza e Heinrich Maschke. Em 1896, foi o primeiro aluno de matemática a receber o grau de doutor pela Universidade de Chicago, com a tese *The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion on the Linear Group*, [12].

Dickson passou o ano seguinte em Leipzig e em Paris, onde estudou com Marius Sophus Lie (1842-1899) e Camille Jordan (1838-1922), respectivamente. Quando retornou aos Estados Unidos em 1897, tornou-se instrutor na Universidade da Califórnia, em Berkeley. Em 1899, foi nomeado professor assistente, na Universidade do Texas. Entretanto, Moore e seus colegas do departamento de matemática de Chicago queriam que ele retornasse àquela universidade e lhe ofereceram um cargo permanente. Dickson aceitou imediatamente a oferta e lá permaneceu pelo período de 1900 a 1939, quando se aposentou, ocupando os seguintes cargos: professor assistente entre 1900 e 1907; professor associado entre 1907 e 1910; e *professor*, em 1910. Em 1928, Moore nomeou-o *professor emérito*.

Dickson é um dos mais brilhantes matemáticos que os Estados Unidos produziram¹¹, publicando mais de 280 artigos e 18 livros¹², dos quais dois destes artigos foram produzidos num momento bastante incomum: conforme citado em [DU], Dickson declarou que sua lua-de-mel com sua esposa foi um sucesso, exceto pelo fato de ter escrito apenas dois artigos! Seus

¹¹Em 1903, Dickson era considerado o nono matemático mais importante dos Estados Unidos. Os oito primeiros eram: Moore, Hill, Osgood, Bôcher, Bolza, Morley, Brown e White — onde se nota que, excluindo Moore que à época já se dedicava à geometria, Dickson era o único algebrista entre os nove primeiros.

¹²Dois deles foram traduzidos para o alemão — *Modern Algebraic Theory (Höhere Algebra)* e *Introduction to the Theory of Numbers (Einführung in die Zahlentheorie)* — e um foi apenas publicado neste idioma — *Algebren und ihre Zahlentheorie*.

Leonard E. Dickson.

1932

Figura 2.3: Leonard Eugene Dickson

livros apresentam material de grande importância, como *Linear Groups with an Exposition of the Galois Field Theory* (discutido mais adiante), [49], e o seu monumental *History of Theory of Numbers* em três volumes, [204], onde ele realiza um estudo minucioso do assunto (que estudaremos no apêndice C).

Dickson teve grande reconhecimento pela sua importante contribuição à matemática, visto que ganhou um prêmio de mil dólares, em 1924, pelo seu livro *Algebras and their Arithmetics*, [229], junto com os dois artigos *The Theory of Numbers and Generalized Quaternions*, [235], e *Quadratic Fields in which Factorization is Always Unique*, [234]. Em 1928, ganhou o Prêmio Cole (duzentos dólares) pelo seu livro *Algebren und ihre Zahlentheorie*. Foi editor do *Monthly* em 1902-1908 e do *Transactions* da AMS em 1911-1916. Foi presidente da *American Mathematical Society*, no período 1916-1918 e sócio da *National Academy of Sciences* (eleito em 1913), da *American Philosophical Society*, da *American Academy of Arts and Sciences* e da *London Mathematical Society*. Também foi condecorado por Harvard, em 1936 e por Princeton, em 1941.

Suas pesquisas foram basicamente dedicadas a:

1. **Grupos Lineares:** Dickson realizou uma extensa pesquisa acerca do assunto, porquanto sua tese, para obtenção do grau de doutor, foi sobre este tema. Na próxima subseção, daremos alguns detalhes sobre seus estudos em grupos lineares.
2. **Corpos Finitos:** Em 1901 ([49]), Dickson deu a primeira grande exposição da teoria de corpos finitos, aplicando seu conhecimento do assunto, não apenas a grupos lineares mas a outros problemas: estudou questões de irredutibilidade sobre um corpo finito, a teoria de Galois e formas quadráticas. Em 1909 ([153]), afirmou:

*“For a finite field it seems to be true that every form of degree m in $m+1$ variables vanishes for values not all zero in the field”*¹³

e provou o teorema para os casos $m = 2$ e $m = 3$ ¹⁴.

3. **Álgebras:** Esta foi sua grande área de atuação, onde obteve seus principais resultados. Num *abstract* do volume doze do AMS *Bulletin* (1905-1906), Dickson definiu as álgebras cíclicas. Elas foram tão importantes para o desenvolvimento da teoria de álgebras com divisão que foram chamadas de **Álgebras de Dickson** por Wedderburn, em 1907 ([WE3]). A primeira vez que estudou a aritmética de uma álgebra foi em 1921 ([218]), quando fez um estudo detalhado da aritmética dos quatérnios. Entretanto, sua maior

¹³“Para um corpo finito parece ser verdade que toda forma de grau m em $m+1$ variáveis se anula para valores não todos nulos no corpo.”

¹⁴O resultado mais geral foi provado por C. Chevalley em *Démonstration d’une hypothèse de M. Artin*, Hamb. Abh., v. 11, (1935), pp. 73-75.

contribuição ao assunto deu-se no seu importante livro *Algebras and their Arithmetics* ([229]), de 1923, onde também expôs a teoria de Wedderburn. Já no período de 1926-1930 ([240], [253], [257] e [267]), apresentou importantes resultados sobre produto cruzado de álgebras. No capítulo 5, daremos mais detalhes sobre as pesquisas de Dickson na teoria de álgebras, em especial, as álgebras com divisão.

4. Teoria de Números: Dickson sempre citou a frase de Gauss que afirma:

“... a matemática é a rainha das ciências, e que a teoria de números é a rainha da matemática e, por isso, sempre quis estudá-la.”

No volume dois de seu monumental *History of Theory of Numbers*, confidencia:

“Conventional histories take for granted that each fact has been discovered by a natural series of deductions from earlier facts and devote considerable space in the attempt to trace the sequence. But men experienced in research know that at least the germ of many important results are discovered by sudden and mysterious intuition, perhaps the result of subconscious mental effort, even though such intuitions have to be subjected later to the sorting process of critical faculties. What is generally wanted is a full and correct statement of the facts, not an historian’s personal explanation of those facts. The more completely the historian remains in the background or the less conscious the reader is the historian’s personality, the better the history. ... With such a view of the ideal self-effacement of the historian, what induced the author to interrupt his own investigations for the greater part of the past nine years to write the history? Because it fitted in with his convictions that every person should aim to perform at some time in his life some serious, useful work for which it is highly improbable that there will be any reward whatever other than his satisfaction therefrom”¹⁵.

¹⁵ “Histórias convencionais aceitam como verdadeiro que cada fato é descoberto por uma série de deduções naturais de fatos preliminares e devotam considerável espaço à tentativa de traçar a seqüência. Mas homens experientes em pesquisas sabem que pelo menos o germe de muitos resultados importantes é descoberto por uma repentina e misteriosa intuição, talvez o resultado de esforços mentais subconscientes, mesmo que tais intuições tenham que ser submetidas, depois, ao processo de julgamento de capacidades críticas. O que geralmente é desejado é uma completa e correta exposição dos fatos, não uma explicação pessoal da história destes fatos. Quanto mais completamente o historiador permaneça no pano de fundo ou o menos consciente esteja o leitor da personalidade do historiador, melhor é a história. ... Com tal visão do historiador, o que induziu o autor a interromper suas investigações por grande parte dos nove anos passados para escrever a história? Porque está de acordo com suas convicções de que toda pessoa deveria ansiar executar, em algum tempo de sua vida, algum trabalho sério e útil para o qual é altamente improvável que existirá qualquer recompensa, que não seja sua satisfação.”

Em seu primeiro trabalho sobre teoria de números ([29]), de 1899, apresentou uma generalização do teorema elementar de Fermat surgido em conexão com a teoria de corpos finitos. Seu interesse, no trabalho de Fermat, continuou e seus estudos acerca do último teorema apareceram entre 1908 e 1917, em [147], [148], [149], [161] e [203]. Grande parte dos seus estudos, durante o período 1926-1930, foram dedicados à teoria aritmética de formas quadráticas, em particular a formas universais.

5. **Outros:** Dickson também manifestou interesse na teoria de matrizes, em geometria e em equações Diophantinas.

Muitos matemáticos continuaram as pesquisas de Dickson, em particular seus 64 alunos de doutorado¹⁶ pela Universidade de Chicago entre 1901 e 1937, que são os seguintes:

T. M. Putnam, W. H. Bussey, H. E. Jordan, A. Ranum, R. L. Börger, A. H. Wilson, W. C. Krathwohl, Mildred L. Sanderson, F. B. Wiley, Olive C. Hazlett, A. Henderson, J. E. McAtee, G. H. Cresse, W. L. G. Williams, Mayme I. Logsdon, C. C. MacDuffee, H. S. Everett, J. S. Turner, Constance R. Ballantine, M. M. Feldstein, G. E. F. Sherwood, B. F. Yanney, Marguerite D. Darkow, C. Gouwens, Mildred Hunt, C. G. Latimer, F. S. Nowlan, Echo D. Pepper, A. E. Cooper, R. J. Garver, J. S. Georges, R. G. Archibald, Lois W. Griffiths, J. Williamson, A. A. Albert, B. W. Jones, D. C. Morrow, E. L. Thompson, K. C. Yang, O. E. Brown, R. H. Marquis, G. Pall, S. Silberfarb, A. Oppenheim, R. S. Underwood, Mina S. Rees, Emily E. Chandler, A. E. Ross, F. W. Sparks, Ruth G. Mason, R. D. James, R. Hull, R. E. Huston, Frances E. Baker, R. C. Shook, G. C. Webber, Marie Litzinger, K. S. Ghent, Mable G. Humphreys, J. C. Brixey, Mae R. Anderson, Dora McFarland, S. B. Townes e H. Chatland.

Nos próximos capítulos deste trabalho, dividiremos os estudos de Dickson numa fase de redefinições de alguns conceitos, pelo método axiomático, e seus estudos em álgebras com divisão (que começa com a publicação de *On Finite Algebras*) e quatérnios.

2.4.1 Os Estudos de Dickson em Grupos Lineares

Como Dickson desenvolveu seu doutorado sob a supervisão de Moore, é natural que tenha seguido a mesma linha de pesquisa de seu mentor: quando ele chegou a Chicago, Moore investigava as propriedades dos corpos de Galois e tinha acabado de provar (em [MO1]) que todo corpo finito é um corpo de Galois. Dickson, então, procurou estender a teoria de corpos finitos e explorar sua conexão com a teoria de grupos. Inicia sua tese ([12]) examinando o seguinte problema: dado um polinômio numa única variável $\phi(\xi)$ de grau $k < p^n$ e com

¹⁶Conforme [LA], comenta-se que Dickson tinha duas classes de estudantes de doutorado: uma de alunos regulares e a outra com aqueles que ele considerava promissores (como, por exemplo, C. C. MacDuffee, C. G. Latimer, Burton W. Jones e A. A. Albert).

coeficientes num corpo de Galois $\text{GF}[p^n]$, onde p é primo e n é um inteiro positivo, considere uma aplicação de $\text{GF}[p^n]$ em $\text{GF}[p^n]$ que substitui sucessivamente a variável ξ por elementos do corpo. Dickson então estuda quando esta aplicação é uma bijeção. Na primeira parte da tese, ele determina completamente as aplicações de grau $k < 7$ e obtém resultados parciais nos graus 7 e 11.

Na segunda parte deste trabalho, discute grupos lineares finitos, originalmente definidos como sendo subgrupos do grupo de matrizes não-singulares de ordem n , com entradas em $\text{GF}[p^n]$, generalizando os estudos de Camille Jordan, o qual havia restringido suas pesquisas ao corpo $\text{GF}[p]$.

Nos três anos seguintes ao seu doutorado, Dickson continuou dedicando-se ao assunto de sua tese, publicando quase trinta artigos relacionados a grupos lineares. Em 1901, publicou o livro *Linear Groups with an Exposition of the Galois Field Theory* ([49]), com o qual passou a ser considerado o maior especialista em grupos lineares da época.

Os primeiros capítulos deste trabalho são dedicados a uma exposição linear da teoria de corpos de Galois, na sua forma abstrata. O conceito abstrato de corpo é introduzido através de exemplos simples, como as classes de resíduos módulo p , onde p é um primo. Do fato de que para todo primo p e todo inteiro positivo n existe um único corpo de Galois de ordem p^n e pelo teorema de Moore que afirma que todo corpo finito pode ser representado por um corpo de Galois, sua investigação atinge uma completa generalidade, quando toma como base o corpo $\text{GF}[p^n]$.

A segunda parte do livro apresenta uma exposição elementar dos resultados mais importantes sobre grupos lineares em corpos de Galois, com Dickson generalizando os resultados obtidos por Galois, Jordan e Serret em grupos lineares sobre o corpo dos inteiros módulo p para um corpo finito arbitrário.

Dickson finaliza este trabalho apresentando um resumo dos sistemas de grupos simples finitos conhecidos até o momento.

O significado desta obra para o desenvolvimento da álgebra moderna é que ela contém uma extensa e completa apresentação da teoria de Galois, com uma riqueza inacreditável de detalhes, representando o primeiro tratamento sistemático de corpos finitos na literatura matemática, conforme K. Prashal cita em [PA5]:

“... his book represented the first systematic treatment of finite fields in the mathematical literature.”

Suas pesquisas, acerca de grupos lineares, continuaram até 1908, e escreveu em torno de 44 artigos sobre o assunto. Nos seus últimos trabalhos, estudou isomorfismos de alguns grupos simples e questões envolvendo a existência de certos tipos de subgrupos. Também obteve muitos resultados sobre grupos lineares infinitos.

2.5 A Influência dos Trabalhos de Dickson em Outros Autores

A obra de Dickson, pela sua magnitude, influenciou o trabalho de muitos matemáticos do século vinte — dentre eles, podemos citar o grande algebrista escocês Joseph H. M. Wedderburn, o geômetra Oswald Veblen, os italianos Gaetano Scorza (1876-1939) e Francesco Cecioni (1884-1968), além, é claro, de seus alunos por Chicago, onde destacamos Abraham Adrian Albert (1905-1972).

Como observamos em (1.4), Wedderburn passou um período (o ano acadêmico 1904-1905), como visitante, na Universidade de Chicago. Nesta época, esta universidade era dominada pelos estudos em geometria: das catorze pessoas¹⁷ associadas ao departamento de matemática, nada menos que seis se dedicavam à geometria, e a principal fonte de inspiração geométrica era E. H. Moore¹⁸. Mas, o que atraiu o jovem algebrista Wedderburn a Chicago? O brilhante trabalho de Dickson!

Na ocasião, a Universidade de Chicago era considerada o centro da pesquisa americana em álgebra: Moore havia publicado alguns artigos sobre grupos e teoria de corpos, cujo mais notável resultado foi a demonstração de que todo corpo finito é um corpo de Galois; mas, desde 1899, dedicava-se aos fundamentos da geometria. Em contrapartida, havia Dickson que, à época que Wedderburn chegou a Chicago, já tinha publicado cerca de cem artigos e três livros, o que fazia dele certamente um prodígio, dado o fato de que tinha apenas trinta anos!

Aparentemente, Wedderburn logo começou a trabalhar junto com Dickson na teoria de corpos finitos¹⁹: em janeiro de 1905, Wedderburn apresentou o trabalho *Proof of Commutativity of Addition and Multiplication in Finite Fields*, e Dickson obteve seu *Theorem on Non-Commutative Finite Systems*. Apenas três meses depois, em abril do mesmo ano, Wedderburn e Dickson apresentaram seus resultados finais no assunto: *toda álgebra com divisão finita é um corpo*, em *A Theorem on Finite Algebras*, [WE1] e *On Finite Algebras*, [119], respectivamente. Ao total, Wedderburn deu três demonstrações do referido teorema neste artigo, sendo duas após conhecer a demonstração dada por Dickson. Em [119], Dickson cita, numa nota de rodapé, que Wedderburn já havia provado o resultado:

¹⁷As catorze pessoas eram Moore, Bolza, Maschke, Dickson, Veblen, Wedderburn, Jacob W. A. Young, Herbert E. Slaughter, Robert L. Moore, Nels J. Lennes, Harris F. MacNeish, Forrest R. Moulton, Saul Epstein, Arthur C. Lunn e William R. Longley. Os que trabalhavam em geometria eram: Moore, Veblen, Moulton e os estudantes R. L. Moore, Lennes e MacNeish; nesta época Maschke também havia mudado suas pesquisas para a geometria.

¹⁸Imbuído desta atmosfera geométrica, Wedderburn também pesquisou um pouco em geometria.

¹⁹Parshal cita, em [PA2], que esta dedução se faz ao analisar os registros no *Logbook of the Mathematical Club of the University of Chicago*, Departamento de Matemática, 1903-1957, pp. 8.

*"First proved by Wedderburn ... ("A Theorem on Finite Algebras"). Following my simpler proof above, and using the same lemma, Wedderburn constructed two further simple proofs, loc. cit."*²⁰.

Os estudos de Dickson também influenciaram as pesquisas do geômetra Oswald Veblen: Wedderburn e ele usaram este teorema para estabelecer que geometrias dadas por álgebras com divisão finita são Pascalianas e Desarguianas. Usando outro resultado obtido por Dickson, as álgebras cíclicas (álgebras de Dickson, conforme denotação dada por Wedderburn), construíram exemplos de geometrias que não são nem Pascalianas e nem Desarguianas.

O trabalho de Dickson era tão importante que ultrapassou fronteiras e conseguiu influenciar as pesquisas na Itália, onde o cenário era dominado pelos estudos em geometria algébrica, em análise e em física-matemática. A exceção dava-se na Universidade de Pisa, onde a figura de Luigi Bianchi (1856-1928) predominava: embora fosse um especialista em geometria diferencial, também possuía um grande conhecimento de álgebra e teoria dos números, refletido nos estudos de seus alunos de doutorado Gaetano Scorza e Francesco Cecioni.

Scorza, que foi membro do *Rendiconti del Circolo Matematico di Palermo* e da *Accademia Nazionali dei Lincei*, desenvolveu suas pesquisas em teoria de variedades abelianas e foi o único a apreciar totalmente os métodos da álgebra abstrata moderna. Sua grande obra no assunto foi a publicação, em 1921, do livro *Corpi Numerici e Algebre*, [SZA], que foi certamente o primeiro livro a dar uma introdução completa e abstrata à teoria de álgebras e aos mais importantes resultados das escolas alemã (Frobenius) e americana. Na segunda parte deste livro, Scorza introduz, de modo mais claro, todos os resultados obtidos até aquele momento por Wedderburn e Dickson; em [BG1], Brigaglia atesta este fato, dizendo:

*"La seconda parte è la più importante e si riferisce alla Teoria Generale delle Algebre. Essa contiene praticamente tutto quanto sull'argomento era stato fino ad allora prodotto, tranne i recentissimi risultati de Wedderburn e Dickson sulla costruzione di algebre di divisione ..."*²¹

Como vimos, Dickson teve influência direta na obra de Scorza; entretanto, a recíproca também ocorreu: no prefácio de seu livro *Algebras and their Arithmetics*, Dickson afirma que o livro de Scorza foi material de apoio do seu trabalho, embora diferísse em importantes aspectos:

²⁰"Primeiro provado por Wedderburn ... ("A Theorem on Finite Algebras"). Seguindo minha prova mais simples acima, e usando o mesmo lema, Wedderburn construiu duas demonstrações mais simples, loc. cit."

²¹"A segunda parte é mais importante e refere-se à Teoria Geral da Álgebra. Ela contém, praticamente, tudo que foi feito até então, exceto o recentíssimo resultado de Wedderburn e Dickson sobre a construção de álgebras com divisão ..."

“Scorza’s book has been of material of assistance to the author although the present exposition of the algebraic parts differs in many important respects from that by Scorza and from that in the author’s [Dickson] earlier book [173].”

A publicação da obra de Scorza proporcionou a outro matemático italiano e também aluno de Bianchi, Francesco Cecioni, as ferramentas necessárias para dar a mais importante contribuição da escola italiana ao desenvolvimento da teoria de álgebras, contida em um único artigo publicado em 1923: *Sopra un tipo di Algebre prive di divisori dello zero*, [CE1]. No início do século vinte, Wedderburn e Dickson costumavam afirmar que o principal problema na teoria de álgebras associativas era o de determinar todas as álgebras com divisão sobre um corpo arbitrário $\mathbb{F}$ (de dimensão finita sobre seu centro). Em 1878, Frobenius já havia provado que as únicas álgebras com divisão sobre $\mathbb{R}$ são $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ (os quatérnios). Em 1905, Wedderburn mostrou em [WE1] que não existe álgebra com divisão comutativa sobre um corpo finito. O primeiro método para construir novas álgebras, com divisão, foi dado por Dickson, em 1914 ([184]), onde obteve novas álgebras com divisão sobre os racionais $\mathbb{Q}$. Em [WE3], de 1921, Wedderburn mostrou que toda álgebra central (ou seja, aquela cujo centro é o corpo base), com divisão e de dimensão nove, é do tipo de Dickson (álgebra cíclica). Evidentemente, Wedderburn estava convencido que existiam álgebras de dimensão maior e que não eram de Dickson, mas não obteve sucesso em obter exemplos. Entretanto, sugeriu caminhos para construí-las.

Estes caminhos foram seguidos por Cecioni, que apenas conseguiu obter condições necessárias e suficientes para construir novas álgebras, sem entretanto saber se eram ou não do tipo de Dickson. Este problema foi resolvido por Albert em [AL1], de 1929, onde provou que todas as álgebras construídas por Cecioni são cíclicas.

Após a publicação deste trabalho de Cecioni, a teoria de construção de álgebras com divisão desenvolveu-se numa importante parte do estudo de álgebras: a teoria de produtos cruzados, que tornou-se um importante componente da teoria de álgebras e representações de grupo de Emmy Noether.

Dentre todos os matemáticos citados nesta seção, aquele que mais foi influenciado por Dickson foi Abraham Adrian Albert (um dos mais importantes algebristas do mundo e presidente da AMS de 1965 a 1967), pois foi seu aluno de mestrado e doutorado, em Chicago. Seu trabalho também mostra influência de Wedderburn, cujos elegantes resultados e métodos lhe serviram de inspiração; Hermann Weyl, cujos trabalhos em grupos e álgebras de Lie despertaram seu interesse no assunto; e Salomon Lefschetz, que o introduziu em matrizes de Riemann, durante seu pós-doutorado (1928-1929), em Princeton.

Suas principais contribuições foram em álgebras associativas, álgebras não associativas e matrizes de Riemann. Trabalhando em construir novas álgebras com divisão, Albert obteve, em [AL2], o primeiro exemplo de álgebra com divisão que não é do tipo de Dickson.

Suas pesquisas acerca do assunto continuaram, com Albert produzindo grandes resultados em teoria de álgebras (cujos maiores detalhes não daremos, por não serem o objetivo deste estudo) e também influenciando os estudos de outros matemáticos.

Capítulo 3

Fase Axiomática

3.1 Introdução

Após a publicação de *Linear Groups with an Exposition of the Galois Field Theory* em 1901, Dickson inicia uma fase de redefinições de alguns conceitos, de forma precisa, através de postulados. Isto se dá como consequência da crescente abstração que ocorreu em álgebra, no fim do século dezenove e início do século vinte.

Em meados do século dezenove, percebeu-se que se poderia trabalhar com coleções de objetos que não eram necessariamente os números reais ou os números complexos, mas objetos estes que poderiam ser combinados através de operações e leis próprias de cada coleção. Assim, surgiram, ao longo do tempo, várias denotações, tais como grupo, anel, ideal e corpo, para identificar estas estruturas segundo suas propriedades. Entretanto, apenas nas últimas décadas do século é que os matemáticos perceberam que poderiam atuar num nível mais elevado de eficiência, integrando várias coleções através de suas propriedades comuns. Com isto, estas coleções poderiam ser tratadas, de um modo único, como um conjunto de elementos munido de regras de combinação entre eles, cuja natureza é especificada apenas por certas propriedades abstratas, e a mais importante delas é que este conjunto é fechado para esta regra.

O grupo foi a primeira estrutura introduzida e estudada de forma abstrata, embora Cayley já o houvesse feito em 1854¹ e isto não tivesse sido percebido na ocasião. Em 1858, Dedekind deu uma definição abstrata de grupos finitos derivada de grupos de permutações. Já em 1877², observou que o módulo de números algébricos pode ser generalizado e sugeriu,

¹Introduzido nos três trabalhos *Phil. Mag.*, (3), 34, 1849, 527-529 = *Coll. Math. Papers*, 1, 423-424 e (4), 7, 1854, 40-47 e 408-409 = *Papers*, 2, 123-130 e 131-132

²*Bull. des Sci. Math.*, v. 2, (1877), pp. 17-41.

então, um grupo abstrato comutativo finito. Dedekind viu, claramente, no seu trabalho em teoria algébrica dos números, o valor de algumas estruturas, tais como ideais e corpos.

Kronecker, lançando mão do trabalho de Kummer em números ideais, deu definições abstratas similares àquelas dadas por Cayley, em 1854, para um grupo abeliano finito. Cayley especificou elementos abstratos, uma operação abstrata, a propriedade do conjunto ser fechado para a operação, as propriedades associativa e distributiva e a existência do único inverso de cada elemento. Com isto, provou alguns teoremas. Em 1878, Cayley escreveu mais quatro artigos sobre grupos finitos abstratos, onde observou que o conceito de grupo não precisa estar limitado a grupos de substituições, embora todo grupo com número finito de elementos possa ser representado por um grupo de substituições. Já Frobenius e Ludwig Stickelberger (1850-1936), num artigo em conjunto³, avançaram nesta teoria, verificando que o conceito de grupo abstrato engloba congruências e a composição de formas de Gauss, assim como os grupos de substituições de Galois. Aqui eles mencionam grupos de ordem infinita.

Em torno de 1880, novas idéias sobre grupos surgiram: Klein, influenciado pelo trabalho de Jordan em grupos de permutações, mostrou que grupos de transformações infinitos, ou seja, aqueles que têm infinitos elementos, podem ser usados para classificar geometrias. Sophus Lie, que havia trabalhado com Klein, na década de 70 do século XIX, usou o conceito de grupos contínuos não para classificar geometrias, mas sim para mostrar que a maioria das equações diferenciais são invariantes por classes de grupos contínuos de transformações. Já em 1882-1883, Walther von Dyck (1856-1934) introduziu a idéia abstrata de um grupo definido por elementos geradores⁴ e as relações entre eles. Os estudos acerca da definição abstrata de grupo sucederam-se, e, no início do século vinte, E. V. Huntington (1874-1952) (em [HU2] e [HU5]), Moore (em [MO2] e [MO3]) e Dickson (em [105]) apresentaram conjuntos de postulados independentes para um grupo abstrato. Com a noção abstrata de um grupo, os matemáticos passaram, então, a provar teoremas acerca do assunto, sugeridos por resultados obtidos a partir de casos concretos.

Já a teoria abstrata para corpos surgiu com Galois, prosseguiu com Dedekind e continuou com Heinrich Weber (1842-1913), que já havia aderido à abstração para grupos⁵. Em 1893⁶, apresentou uma formulação abstrata da teoria de Galois, onde introduziu corpos comutativos a partir da noção de grupos. Weber define corpo como uma coleção de elementos, munida de duas operações, chamadas adição e multiplicação, em relação às quais a coleção é fechada e cujas operações satisfazem às leis associativa e comutativa, à lei distributiva e tal que todo elemento não nulo possui um único inverso. Algum tempo depois, Dickson (em [82] e [105]) e Huntington (em [HU4] e [HU5]) deram postulados independentes para um corpo.

³ *Jour. für Math.*, v. 86, (1879), pp. 217-262.

⁴ Os geradores consistem de um subconjunto fixado de elementos de um grupo, tal que todo elemento do grupo pode ser expresso como um produto de potências dos geradores e seus inversos.

⁵ *Math. Ann.*, v. 20, (1882), 301-329

⁶ *Math. Ann.*, v. 43, (1893), 521-549

A partir deste momento, novas idéias foram surgindo e a abstração na álgebra foi crescendo.

Aqui estudaremos, em detalhes, as contribuições de Dickson acerca do assunto.

3.2 Primeiros Trabalhos

Dickson inicia sua fase de redefinições de alguns conceitos, de forma precisa, de modo axiomático, com a apresentação de *Theory of Linear Groups in an Arbitrary Field* ([51]), em agosto de 1901 (recebido para publicação em junho do mesmo ano), à *American Mathematical Society* no Encontro de Ithaca. Este trabalho tem como principal objetivo exibir quatro sistemas infinitos de grupos de transformações, que são grupos simples sobre todo corpo.

Para desenvolver sua teoria, Dickson então define *grupo* como um conjunto cujo produto (que é associativo) de dois de seus elementos pertence ao conjunto (“fechado” para o produto) e que todo elemento deste conjunto é inversível. Em seguida, define *corpo*⁷ como um conjunto que é “fechado” para a adição, a subtração, a multiplicação e a divisão, onde vale a associatividade, e que todo elemento não nulo é inversível.

Como exemplo de corpos, cita os números racionais, os números reais, os números complexos e os corpos finitos⁸.

De posse destas definições, Dickson estuda grupos de transformações lineares, pois, devido à sua simplicidade e sua importância nas aplicações em teorias gerais, oferecem um ponto de partida natural na construção da teoria de grupos lineares sobre um corpo qualquer.

Em março do ano seguinte, Dickson apresenta à *American Mathematical Society* o trabalho *On the Group Defined for Any Given Field by the Multiplication Table of Any Given Finite Group* ([64]), cujo objetivo é desenvolver teoria análoga àquela estabelecida por Burnside em seus dois artigos, ambos sob título *On the Continuous Group that is Defined by Any Given Group of Finite Order*⁹, onde obtém, por um novo método, um dos mais importantes teoremas de Frobenius sobre caracteres, dando um novo enfoque a esta teoria. Nestes seus estudos, Dickson desenvolve esta teoria em corpos arbitrários, que ele chama de domínios de integridade, e quando o corpo é o de Galois de ordem p^n . Entretanto, ele não faz o estudo do corpo cuja característica divide a ordem do grupo finito dado¹⁰.

⁷Dickson também denota corpo por domínio de racionalidade.

⁸Aqui ele menciona que são necessariamente os corpos de Galois de ordem de uma potência de um primo e indica que este resultado se deve a Moore.

⁹Proceedings of the London Mathematical Society, vol. 29 (1898), pp. 207-224 e 546-565.

¹⁰Este caso é estudado em *On the Groups Defined for an Arbitrary Field by the Multiplication Tables of Certain Finite Groups* ([74]), pois, por apresentar dificuldades específicas, recebe estudo detalhado para várias classes de grupos. Neste trabalho também apresenta alguns exemplos adicionais para a teoria geral.

3.3 Definições de Corpo Através de Postulados

O trabalho *Definitions of a Field by Independent Postulates* ([82]), recebido para publicação em julho de 1902, foi apresentado à *American Mathematical Society* em setembro do mesmo ano e tem por objetivo dar duas novas definições de corpo através de postulados¹¹ independentes, ou seja, nenhum dos postulados é consequência dos outros, fato que ocorria na definição usual de corpo. Conforme mencionado na introdução deste capítulo, Huntington e Moore desenvolveram trabalho semelhante.

Dickson inicia este trabalho dizendo que o termo *corpo* tem o mesmo significado de *domínio de racionalidade*¹² e observa que é usualmente definido como um conjunto de elementos que

“podem ser combinados por operações chamadas adição e multiplicação, submetidas às leis associativa, comutativa e distributiva, assim como pelas operações inversas chamadas subtração e divisão, com o divisor não sendo o único elemento que possui as propriedades aditiva e multiplicativa do zero e se a soma, o produto, a diferença e o quociente resultantes forem unicamente determinados como um elemento do corpo.”

Conclui este parágrafo com a seguinte frase:

*“A field may therefore be defined by the property that the rational operations of algebra can be performed within the field.”*¹³

Vale ressaltar que esta frase já havia sido usada em [51]¹⁴. Assim como o próprio Dickson afirma, esta definição possui inúmeras redundâncias, pois alguns dos postulados são facilmente deduzidos de outros. Logo, torna-se interessante dar definições que não possuam redundâncias.

3.3.1 Primeira Definição de Corpo

Em linguagem moderna, dizemos que um conjunto $\mathbb{F}$ munido das operações de adição e de multiplicação é um corpo, conforme (A.1.1), se valem a associatividade e a comutatividade da adição e da multiplicação, se existem elementos neutros e opostos para ambas

¹¹Em [HU1], Huntington observa a diferença entre postulado e axioma: postulado significa uma suposição aceita como base para futuras deduções; já axioma significa uma proposição auto-evidente, não requerendo demonstração formal para provar sua veracidade, mas recebido e aceito assim que mencionado.

¹²Dickson observa que este conceito, em alemão, recebe a denominação de Körper.

¹³“Um corpo pode, portanto, ser caracterizado pela propriedade que as operações racionais de álgebra podem ser efetuadas dentro de um corpo.”

¹⁴Dickson utiliza bastante o expediente de repetir frases já usadas em outros trabalhos.

(chamado de *inverso* no caso da multiplicação e de *oposto*, na adição) e se vale a propriedade distributiva. Em seu trabalho, Dickson define corpo como um conjunto de elementos com duas regras de combinação (que hoje chamamos de operações), denotadas por $\circ$ e $\diamond$, para os quais valem os seguintes nove postulados:

1. *Se a e b pertencem ao conjunto, então $a \circ b$ pertence ao conjunto.* Atualmente, este e o postulado 5 são redundantes na definição de corpo, pois quando dizemos que um conjunto $\mathbb{F}$ é munido de uma operação $\circ$, está subentendido que ele é fechado em relação à $\circ$, isto é, $\circ$ é vista como uma função

$$\begin{aligned} \circ : \mathbb{F} \times \mathbb{F} &\rightarrow \mathbb{F} \\ (a, b) &\mapsto a \circ b. \end{aligned}$$

2. *$a \circ b = b \circ a$, sempre que $a \circ b$ e $b \circ a$ pertencerem ao conjunto.* As condições de que $a \circ b$ e $b \circ a$ devem pertencer ao conjunto (também presente nos postulados abaixo) vem do desejo de manter a independência destes postulados.
3. *$(a \circ b) \circ c = a \circ (b \circ c)$, sempre que $a \circ b$, $b \circ c$, $(a \circ b) \circ c$ e $a \circ (b \circ c)$ pertencerem ao conjunto.*
4. *Para quaisquer dois elementos a e b do conjunto, existe um elemento x no conjunto tal que $(a \circ x) \circ b = b$.*
5. *Se a e b pertencem ao conjunto, então $a \diamond b$ pertence ao conjunto.*
6. *$a \diamond b = b \diamond a$, sempre que $a \diamond b$ e $b \diamond a$ pertencerem ao conjunto.*
7. *$(a \diamond b) \diamond c = a \diamond (b \diamond c)$, sempre que $a \diamond b$, $b \diamond c$, $(a \diamond b) \diamond c$ e $a \diamond (b \diamond c)$ pertencerem ao conjunto.*
8. *Para quaisquer dois elementos a e b no conjunto, tais que $c \diamond a \neq a$ para, pelo menos, um elemento c no conjunto, existe um elemento x no conjunto tal que $(a \diamond x) \diamond b = b$.*
9. *$a \diamond (b \circ c) = (a \diamond b) \circ (a \diamond c)$, sempre que $b \circ c$, $a \diamond b$, $a \diamond c$, $a \diamond (b \circ c)$ e $(a \diamond b) \circ (a \diamond c)$ pertencerem ao conjunto¹⁵.*

¹⁵Dickson afirma que outra definição pode ser obtida substituindo 8 pelo postulado:

“Para quaisquer dois elementos a e b tais que $c \diamond a \neq a$ para, pelo menos, um elemento c , existe um elemento x tal que $(a \diamond x) \diamond b = b$.”

De posse desta definição, Dickson mostra a existência e unicidade da operação inversa de $\circ$ e prova que vale a “lei do cancelamento à esquerda para $\circ$ ”, isto é:

$$a \circ b = a \circ b' \implies b = b'.$$

Também mostra que estas propriedades valem para a operação $\diamond$.

Em seguida, obtém que o elemento neutro da adição tem a propriedade do zero da multiplicação, mostrando:

1. Se $c \circ b = c$, então $l \circ (a \diamond b) = l$ para todo elemento l e todo elemento a .
2. Se $c \circ b = c$, então $a \diamond b = b$ para todo elemento a .
3. Se $k \circ (a \diamond b) = k$ e $c \diamond a \neq a$ para pelo menos um elemento c , então $l \circ b = l$ para todo elemento l .

A fim de ilustrar que estes postulados definem um corpo, Dickson dá o exemplo dos números inteiros módulo p , onde p é um primo, na seção em que chama de *Consistência dos Nove Postulados*: considera o conjunto formado por $0, 1, \dots, p-1$ e toma $a \circ b = a + b$ e $a \diamond b = a \times b$ como o menor resíduo positivo módulo p de $a + b$ e $a \times b$, respectivamente¹⁶. Em seguida, na seção *Comparação com a Definição Ordinária de um Corpo*, compara sua definição com a usual de corpo, mostrando que os postulados, juntamente com as propriedades derivadas deles, incluem todas as propriedades necessárias para aquela definição.

Para provar a independência dos postulados, Dickson utiliza o método apresentado por Hilbert em [HI]¹⁷, exibindo conjuntos S_k , com $k = 1, \dots, 9$, munido das regras $\circ$ e $\diamond$, tal que, em cada caso, o k -ésimo postulado não é satisfeito, enquanto que todos os outros oito o são¹⁸.

S₁. O conjunto dos elementos $0, +1, -1$, com $a \circ b = a + b$ e $a \diamond b = a \times b$.

S₂. Todos os números racionais positivos, com $a \circ b = b$ e $a \diamond b = a \times b$.

S₃. Todos os números racionais, com $a \circ b = -a - b$ e $a \diamond b = a \times b$. Aqui o postulado 3 falha porque $-(a - b) - c \neq -a - (-b - c)$ em geral. O postulado 4 é satisfeito quando se toma $x = 2b - a$.

S₄. Todos os números racionais positivos, com $a \circ b = a + b$ e $a \diamond b = a \times b$.

¹⁶Ou seja, o resto da divisão de $a + b$ e $a \times b$ por p , respectivamente.

¹⁷Este método já havia sido apresentado por G. Peano em [PE].

¹⁸Dickson sempre utiliza este método para provar a independência dos postulados.

S₅. O conjunto de todos os números da forma $n\sqrt{2}$, onde n é racional, com $a \circ b = a + b$ e $a \diamond b = a \times b$, pois $(n\sqrt{2}) \diamond (m\sqrt{2}) = 2mn$ está no conjunto apenas quando $n = m = 0$. Já para o postulado 8,

$$(n\sqrt{2} \diamond x) \diamond m\sqrt{2} = m\sqrt{2}$$

é satisfeita para $x = \frac{1}{2n}\sqrt{2}$, se $n \neq 0$.

S₆. Todos os números racionais, com $a \circ b = a + b$ e $a \diamond b = b$. Aqui o postulado 8 vale, mas não tem sentido, pois $c \diamond a = a$ para todo c ¹⁹.

S₇. Todos os números da forma $a_1\epsilon_1 + a_2\epsilon_2$, onde $a_1, a_2 \in \mathbb{R}$, e

$$\epsilon_1^2 = \epsilon_1, \quad \epsilon_1\epsilon_2 = -\epsilon_2, \quad \epsilon_2\epsilon_1 = -\epsilon_2, \quad \epsilon_2^2 = -\epsilon_1,$$

enquanto que $a \circ b = a + b$ e $a \diamond b = a \times b$. Evidentemente os postulados 1, 2, 3 e 4 são satisfeitos. Entretanto, o postulado 7 não vale, pois

$$(\epsilon_2\epsilon_2)\epsilon_1 = \epsilon_1^2 = -\epsilon_1, \quad \epsilon_2(\epsilon_2\epsilon_1) = -\epsilon_2^2 = +\epsilon_1.$$

Para mostrar que 5, 6, 8 e 9 valem, Dickson considera o produto

$$(a_1\epsilon_1 + a_2\epsilon_2)(b_1\epsilon_1 + b_2\epsilon_2) = (a_1b_1 - a_2b_2)\epsilon_1 + (-a_1b_2 - a_2b_1)\epsilon_2.$$

Então, se $a = a_1\epsilon_1 + a_2\epsilon_2$ e $b = b_1\epsilon_1 + b_2\epsilon_2$, tem-se $ab = ba$. Dados a e c , onde a_1 e a_2 não são ambos nulos, pode-se encontrar b_1 e b_2 tais que $ab = c$:

$$b_1 = \frac{a_1c_1 - a_2c_2}{a_1^2 + a_2^2}, \quad b_2 = \frac{-a_2c_1 - a_1c_2}{a_1^2 + a_2^2}.$$

Isto imediatamente mostra que o postulado 8 vale. Claramente 9 é satisfeito.

S₈. Todos os números inteiros, com $a \circ b = a \diamond b = a + b$ ²⁰.

S₉. Todos os números racionais, com $a \circ b = a \diamond b = a + b$ ²¹.

¹⁹O conjunto dos quatérnios com $a \circ b = a + b$ e $a \diamond b = a \times b$ também poderia ser considerado para este caso.

²⁰Dickson observa que poderia ter considerado o conjunto dos resíduos módulo n , onde n é um número composto, com $a \circ b$ e $a \diamond b$ sendo os resíduos de $a + b$ e de $a \times b$, respectivamente.

²¹Do mesmo modo, podia-se considerar o conjunto dos racionais com $a \circ b = a \diamond b = a \times b$.

3.3.2 Segunda Definição de Corpo

Na introdução deste artigo, Dickson diz que esta outra definição de corpo tem duas vantagens em relação à primeira que são a facilidade em derivar as propriedades suplementares de corpo e a conveniência de testar propriedades e regras de combinação para o corpo:

“My second definition of a field has two advantages over my first, the greater ease in deriving the further proprieties of a field and the suitableness in testing for the field property a given set of elements and laws of combination.”

Aqui ele considera um conjunto munido das regras de combinação $\circ$ e $\diamond$ onde valem os postulados anteriores, exceto o quarto e oitavo. Estes são, então, substituídos por:

[4'] *Existe um elemento z no conjunto tal que $z \circ b = b$ para todo elemento b .*

[4''] *Se existe o elemento z do postulado [4'], então para este z e para todo elemento a , existe um elemento x no conjunto para o qual $a \circ x = z$.*

[8'] *Existe um elemento u no conjunto tal que $u \diamond b = b$ para todo elemento b .*

[8''] *Se existe o elemento u do postulado [8'], então para este u e para todo elemento a tal que $c \diamond a \neq a$ para pelo menos um elemento c , existe um elemento x para o qual $a \diamond x = u$.*

Assim como fez na primeira definição de corpo, Dickson deriva propriedades destes postulados. Para mostrar que são independentes, exhibe um conjunto Σ_k para o qual o k -ésimo postulado não vale, enquanto os outros dez são satisfeitos.

3.4 Sistemas de Números Hipercomplexos sobre um Corpo $\mathbb{F}$ Qualquer

O trabalho *Definitions of a Linear Associative Algebra by Independent Postulates* ([83]), recebido para publicação em setembro de 1902, foi apresentado à *American Mathematical Society* no mesmo mês e tem por objetivo definir um sistema de números hipercomplexos (ver A.2.1)²² com coordenadas num corpo arbitrário $\mathbb{F}$, a fim de permitir o desenvolvimento de uma teoria mais geral sobre este assunto²³.

²²Também chamado *álgebra linear associativa* por Benjamin Peirce.

²³Nas definições existentes e teorias desenvolvidas até este momento, as coordenadas do sistema de números hipercomplexos pertencem ao corpo dos números reais ou corpo dos números complexos.

Aqui, Dickson dá duas definições para sistema de números hipercomplexos essencialmente distintas, porém equivalentes, das quais a primeira é através da tabela de multiplicação das unidades do sistema e a segunda é dada de forma abstrata. Trata-se, na realidade, da primeira tentativa de definição abstrata daquela estrutura, a qual hoje chamamos de álgebra linear associativa. Aos olhos do leitor moderno, ambas têm o inconveniente de depender de um sistema de coordenadas não sendo, assim, totalmente intrínsecas.

3.4.1 Primeira Definição de Sistema de Números Hipercomplexos

Nesta definição, Dickson considera elementos $e_1, \dots, e_n$ linearmente independentes sobre um corpo $\mathbb{F}$ qualquer, com tabela de multiplicação dada por

$$e_i e_k = \sum_{s=1}^n \gamma_{iks} e_s, \quad (3.1)$$

para $i, k = 1, 2, \dots, n$, onde cada $\gamma_{iks} \in \mathbb{F}$. Se $a_1, \dots, a_n \in \mathbb{F}$, a expressão

$$a \equiv a_1 e_1 + \dots + a_n e_n$$

é chamada *número hipercomplexo*²⁴ com coordenadas $a_1, \dots, a_n$ e unidades $e_1, \dots, e_n$. Seja

$$b \equiv b_1 e_1 + \dots + b_n e_n$$

outro número hipercomplexo. A adição e a subtração de a e b são dadas por:

$$a \pm b = (a_1 \pm b_1) e_1 + \dots + (a_n \pm b_n) e_n.$$

De modo que valha a lei distributiva, a multiplicação é definida por:

$$ab = \sum_{i,k}^{1, \dots, n} a_i b_k e_i e_k.$$

De (3.1), obtém:

$$ab = \sum_{s=1}^n u_s e_s,$$

²⁴Nesta época, as vezes a expressão número complexo era usada para indicar número hipercomplexo. Dickson utiliza esta expressão ao longo do trabalho. Entretanto, para não haver confusão com um elemento do corpo $\mathbb{C}$, optamos por usar *número hipercomplexo* nos nossos estudos.

onde

$$u_s \equiv \sum_{i,k}^{1,\dots,n} \gamma_{iks} a_i b_k.$$

Dickson observa que, independentemente das n^3 constantes γ_{iks} de $\mathbb{F}$, definiram-se, sem ambigüidades, a adição, a subtração e a multiplicação, pois estas operações aplicadas a quaisquer números hipercomplexos com coordenadas em $\mathbb{F}$, resultam num único número hipercomplexo com coordenadas em $\mathbb{F}$ (o que hoje está implícito na palavra operação). Entretanto, para se obter um *sistema de números hipercomplexos*, é necessário impor certas condições às constantes γ_{iks} para que a associatividade da multiplicação seja satisfeita e para que a divisão definida abaixo seja única. Observando que a associatividade da multiplicação vale se, e só se,

$$(e_i e_k) e_l = e_i (e_k e_l), \quad (i, k = 1, 2, \dots, n),$$

obtém

$$\sum_{s=1}^n \gamma_{iks} \gamma_{slt} = \sum_{s=1}^n \gamma_{kls} \gamma_{ist}, \quad (i, k, l, t = 1, \dots, n). \quad (3.2)$$

Dados dois números hipercomplexos a e b , para que seja possível determinar unicamente outro número hipercomplexo x tal que $ax = b$, deve-se ter que

$$\Delta_a \equiv \left| \sum_{i=1}^n \gamma_{iks} a_i \right| \quad (3.3)$$

não se anula para todo $a_1, \dots, a_n$. Do mesmo modo, para que seja possível encontrar unicamente um número hipercomplexo y tal que $ya = b$, deve-se ter que

$$\Delta'_a \equiv \left| \sum_{k=1}^n \gamma_{iks} a_k \right| \quad (3.4)$$

não se anula para todo $a_1, \dots, a_n$. Com isto em mãos, Dickson afirma que todo sistema de números hipercomplexos sobre um corpo $\mathbb{F}$ define n^3 constantes γ_{iks} em $\mathbb{F}$, satisfazendo às condições (3.2), (3.3) e (3.4). Reciprocamente, um conjunto de constantes γ_{iks} define um sistema de números hipercomplexos sobre um corpo $\mathbb{F}$. Em seguida, assim como fez em [82], mostra que estas condições são independentes exibindo um conjunto S_j , para $j = 5, 6, 7$, de n^3 constantes de $\mathbb{F}$ onde a j -ésima condição falha enquanto que as outras duas são satisfeitas.

3.4.2 Segunda Definição de Sistema de Números Hipercomplexos

Nesta segunda definição, Dickson dá um passo a mais, determinando a multiplicação de forma abstrata (sem o uso das unidades). Aqui, considera um sistema de elementos $A = (a_1, \dots, a_n)$, onde $a_1, \dots, a_n \in \mathbb{F}$ são chamadas coordenadas de A e o elemento zero é denotado por $0 = (0, \dots, 0)$. Se $B = (b_1, \dots, b_n)$ é outro elemento deste sistema, então a adição de A e B é dada por:

$$A + B = (a_1 + b_1, \dots, a_n + b_n). \quad (3.5)$$

Daí, tem-se que existe um elemento $D = (a_1 - b_1, \dots, a_n - b_n)$ tal que $D + B = A$. Em seguida, considera uma segunda regra de combinação destes elementos que tem as seguintes propriedades:

1. Para quaisquer elementos A e B no sistema, $A \bullet B$ é um elemento do sistema cujas coordenadas são funções bilineares das coordenadas de A e de B , com coeficientes em $\mathbb{F}$ fixados.
2. $(A \bullet B) \bullet C = A \bullet (B \bullet C)$ se $A \bullet B$, $B \bullet C$, $(A \bullet B) \bullet C$ e $A \bullet (B \bullet C)$ pertencem ao sistema²⁵.
3. Existe um elemento I no sistema tal que $A \bullet I = A$ para todo elemento A do sistema²⁶.
4. Existe pelo menos um elemento A no sistema tal que $A \bullet Z \neq 0$ para qualquer elemento $Z \neq 0$ ²⁷.

Dickson prova, então, que esta definição de sistema de números hipercomplexos é equivalente à primeira. Para isto, inicialmente mostra que vale a distributividade de $\bullet$ em relação à soma:

$$A \bullet (B + C) = (A \bullet B) + (A \bullet C).$$

Em seguida, verifica que se $A \bullet I = A$ para todo A , então $I \bullet A = A$ e, portanto, $I \bullet A = A \bullet I = A$. A partir disto, e fazendo $A = (a_1, \dots, a_n)$ corresponder a $a \equiv a_1 e_1 + \dots + a_n e_n$, deduz que existem constantes $\gamma_{iks} \in \mathbb{F}$ satisfazendo (3.2); que existe uma única solução $X = I$ de $A \bullet X = A$ onde A satisfaz ao postulado 4 e, portanto, o determinante Δ_a não se anula para todos $a_1, \dots, a_n$; e que existe uma única solução $X = I$ de $X \bullet A = A$ onde

²⁵Do mesmo modo, como em [82], estas condições devem-se ao fato de Dickson querer obter a independência destes postulados.

²⁶Ou seja, existe identidade à direita no sistema.

²⁷Dickson observa que isto é mais fraco que a hipótese de existir uma identidade I' à esquerda. Entretanto, este postulado seguiria da existência de I' se tomássemos A como sendo I' .

A é tal que $Z \bullet A \neq 0$ se $Z \neq 0$ e, portanto, o determinante Δ'_a não se anula para todos $a_1, \dots, a_n$. Logo, as condições (3.2), (3.3) e (3.4) são satisfeitas e o conjunto destes elementos forma um sistema de números hipercomplexos. Dickson finaliza este artigo mostrando que estes postulados são independentes: para cada índice i entre 1 e 4, exibe um conjunto Σ_i de elementos onde o i -ésimo postulado falha, enquanto que os outros três são satisfeitos.

3.5 Definição de Grupo Através de Postulados

O trabalho *Definitions of a Group and a Field by Independent Postulates* ([105]), recebido para publicação em novembro de 1904, foi apresentado à *American Mathematical Society* em dezembro do mesmo ano sob o título *A Definition of a Group by Independent Postulates*. Entretanto, no mês seguinte, Dickson adicionou uma nova definição de corpo ao artigo e, portanto, ao título.

Na introdução deste trabalho, Dickson observa que a definição mais simples de grupo abstrato apresentada nestes estudos tem sua origem nas duas definições dadas por Moore em [MO2], pois alguns dias antes da publicação de seu artigo, Moore informou-o que o postulado $(3''_r)$ da segunda definição, que diz respeito ao inverso de um elemento, era redundante. Entretanto, Dickson pensou que ele se referia à primeira definição e passou a tentar construir uma prova para a redundância, que não existia. Para isto, alterou o postulado (4_1) e concluiu que (3_1) se tornava redundante no novo conjunto de postulados. Daí, surgiu a definição apresentada aqui:

“I thought the reference was to the first definition and attempted to reconstruct the proof of a redundancy, there absent. This attempt led me to alter his postulate (4_1) to read $aa'_r = i_r$ instead of $a'_r a = i_r$ and to note that postulate (3_1) becomes redundant in the altered set, thus obtaining the present definition.”

Dickson ainda comenta que, após ter obtido a sua definição, soube que Moore, em sua demonstração da redundância de $(3''_r)$ da segunda definição, obteve, em [MO3], relações suficientes para estabelecer a presente definição; entretanto, não o fez.

Neste artigo, Dickson define grupo (em linguagem moderna, é dado em A.3.1) como um conjunto munido de uma operação que satisfaz a uma lista de postulados independentes. Com isto em mãos, define corpo como um conjunto munido de duas operações que é um grupo em relação a ambas. Ainda observa que os postulados permanecem independentes quando o conjunto é finito, ou infinito mas enumerável, ou infinito mas não enumerável.

3.5.1 Definição de Grupo

Para definir grupo, Dickson considera uma operação $\circ$ e um conjunto munido desta operação. Então diz que este conjunto forma um grupo em relação a $\circ$ se verifica os seguintes postulados:

- [1₁] *Para quaisquer dois elementos a e b do conjunto, iguais ou distintos, existe $a \circ b$ ²⁸.*
- [1₂] *Para a e b no conjunto, existe no máximo um elemento $a \circ b$.*
- [1₃] *Se, para a e b no conjunto existe pelo menos um elemento $a \circ b$, este elemento pertence ao conjunto²⁹.*
- [2] *$(a \circ b) \circ c = a \circ (b \circ c)$ sempre que $a, b, c, a \circ b, b \circ c, (a \circ b) \circ c$ e $a \circ (b \circ c)$ estiverem no conjunto.*
- [3] *Existe um elemento i no conjunto tal que, para todo elemento a do conjunto, $a \circ i = a$.*
- [4] *Se tais elementos i existem, então para um particular i e para todo³⁰ a no conjunto, existe um elemento a' no conjunto tal que $a \circ a' = i$.*

Desta definição, Dickson conclui que existe um único elemento identidade e um único inverso para cada elemento do grupo e mostra que os postulados (1₁), (1₂), (1₃), (2), (3), (4) e (5_k), com $k = 1, 2$ ou 3 , são consistentes (no sentido que existe um grupo que os verifica) e independentes³¹, onde

- (5₁) *O número de elementos distintos é um inteiro fixado n , $n > 1$;*
- (5₂) *Os elementos distintos do conjunto formam um conjunto infinito enumerável;*
- (5₃) *Os elementos distintos formam um conjunto infinito não enumerável.*

Em seguida, passa a estudar o que ocorre quando se inclui um postulado para comutatividade:

- [6] *$a \circ b = b \circ a$ sempre que $a, b, a \circ b$ e $b \circ a$ estiverem no conjunto.*

Então prova que os postulados (1₁), (1₂), (1₃), (2), (3), (4), (5_k) e (6), com $k = 0, 2$ ou 3 são consistentes e independentes, onde

²⁸Dickson afirma que a suposição dos elementos serem iguais ou distintos não deve ser feita para $a \circ i$ ou $a \circ a'$, em vista dos postulados [3] e [4] seguintes.

²⁹Após a definição, afirma que os postulados [1₁], [1₂] e [1₃] podem ser combinados num único postulado:

[1] *Para quaisquer dois elementos do conjunto a e b , iguais ou distintos, $a \circ b$ é unicamente determinado como um elemento do conjunto.*

Assim como ocorre com as definições anteriores de corpo, este postulado torna-se redundante hoje em dia, pois esta condição é sempre assumida quando dizemos que o conjunto é munido de uma operação.

³⁰Neste ponto, Dickson observa que esta suposição não deve ser feita para $a = i$, tendo em vista o postulado [3].

³¹Usa o mesmo método de Hilbert, já citado nas seções anteriores.

(5₀) *O número de elementos distintos é finito, mas indeterminado.*

Daí, determina condições necessárias e suficientes para que todos os grupos de ordem n sejam comutativos (abelianos) no seguinte³²:

Teorema. *Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_v^{\alpha_v}$, onde $p_1, \dots, p_v$ são primos distintos e cada $\alpha_j > 0$. As condições necessárias e suficientes para que todos os grupos de ordem n existentes sejam abelianos são*

1. *cada $\alpha_j \leq 2$;*
2. *nenhum $p_j^{\alpha_j} - 1$ é divisível por algum dos primos $p_1, \dots, p_v$.*

3.5.2 Definição de Corpo

Aqui, Dickson considera um conjunto com as funções $\oplus$ e $\otimes$ e assume que, se $\circ = \oplus$, os postulados para grupo são denotados por 1^+ (combinação de $[1_1]$, $[1_2]$ e $[1_3]$ para $\oplus$), 2^+ , 3^+ , 4^+ e 6^+ (comutatividade de $\oplus$); se $\circ = \otimes$, os postulados são denotados por $j^\times$, onde $j \in \{1, 2, 3, 4, 6\}$ e $4^\times$ é assumido apenas para elementos diferentes de i_+ (elemento neutro de $\oplus$). Denota um elemento i que satisfaz a $3^\times$ por $i_\times$ e considera a distributividade dada por

[7] $a \otimes (b \otimes c) = (a \otimes b) \oplus (a \otimes c)$, sempre que a, b, c e todas as combinações aqui apresentadas estiverem no conjunto.

Com isto, obtém o

Teorema. *De 1^+ , 2^+ , 3^+ , 4^+ , $1^\times$, $3^\times$, $6^\times$ e 7, segue 6^{+33} .*

e o

Teorema. *Seja i_+ escolhido de modo que 3^+ e 4^+ são satisfeitos. Então $a \oplus i_+ = i_+ \oplus a$ para todo a . Se $a \oplus b = i_+$ e $b \neq i_+$, então $a = i_+$. Daí, i_+ tem as propriedades ordinárias do zero em relação a $\oplus$ e em relação a $\otimes$.*

³²Em nota de rodapé, Dickson observa que incluiu este teorema em fevereiro de 1905.

³³Dickson observa que alguns meses após ter apresentado a demonstração deste teorema, soube que uma prova similar havia sido obtida por Hilbert em *Jahresbericht der Deutschen Mathematiker-Vereinigung*, v. 8, (1899-1900), pp. 183, e que este havia percebido o ponto essencial da demonstração: que a unicidade da expansão de $(\beta + \gamma)(b + c)$ usada para mostrar o teorema depende da existência da comutatividade para a adição.

Tendo em vista os últimos teoremas acima, Dickson define corpo como um conjunto munido das regras $\oplus$ e $\otimes$ e que verifica os postulados 1^+ , 2^+ , 3^+ , 4^+ , $1^\times$, $2^\times$, $3^\times$, $4^\times$, $6^\times$ e 7. Em seguida, mostra que os postulados acima junto com (5_k) , com $k = 0, 2$ ou 3 , são independentes.

Com isto, finalizamos nossos estudos acerca da fase de redefinições de conceitos por parte de Dickson e passaremos a estudar suas contribuições em álgebras com divisão.

Capítulo 4

Os Quatérnios e suas Generalizações

4.1 Introdução

A construção dos quatérnios por Hamilton, em 1843, encorajou muitos algebristas da segunda metade do século dezenove a estudarem os sistemas de números hipercomplexos, a fim de encontrar outros exemplos de álgebras que, assim como os quatérnios, têm as propriedades dos números reais e dos números complexos, exceto para a comutatividade da multiplicação. Em 1845, Cayley construiu uma generalização de dimensão oito dos quatérnios reais, os octônios, onde a norma do produto de dois de seus elementos é o produto de suas normas (“lei do produto”). Em 1853, o próprio Hamilton introduziu os biquatérnios, ou seja, os quatérnios com coeficientes complexos e mostrou que a lei do produto não vale nesta álgebra. Já William K. Clifford (1845-1879), criou outro tipo de números hipercomplexos, também chamados biquatérnios, formados pelos elementos da forma $q + \omega Q$, onde q e Q são quatérnios e ω é tal que $\omega^2 = -1$ e comuta com todo quatérnio real. Os biquatérnios de Clifford satisfazem à lei do produto, mas a multiplicação não é associativa. Vários sistemas continuaram a aparecer e, num trabalho publicado em forma de litografia em 1871, B. Peirce definiu alguns novos números hipercomplexos, classificou todos os conhecidos até aquele momento e também denotou este conjunto por *álgebras lineares associativas*, nomenclatura que perdura até os dias de hoje.

A questão que surgia, então, era de quão livre poderia ser a variedade destas álgebras. Gauss estava convencido de que uma extensão de números hipercomplexos que preserva suas propriedades básicas era impossível; entretanto, mesmo após a construção dos quatérnios, não conseguiu provar que não existem álgebras comutativas tridimensionais. Já F. Georg Frobenius (1849-1917) provou, em 1878, que as únicas álgebras lineares associativas, de dimensão finita, com coeficientes reais e que obedecem à lei do produto são os números reais, os números complexos e os quatérnios reais. Este teorema foi provado independentemente

por Charles S. Peirce (1839-1914), num apêndice do trabalho de seu pai (B. Peirce). Outro resultado fundamental já tinha sido obtido por Karl Weierstrass (1815-1897), em 1861: *as únicas álgebras lineares associativas, de dimensão finita, com coeficientes reais ou complexos e que satisfazem à lei do produto, onde a multiplicação é comutativa, são os números reais ou complexos*. Dedekind obteve o mesmo resultado em 1870. Em 1898, Adolf Hurwitz (1859-1919) mostrou que os números reais, os números complexos, os quatérnios reais e os octônios são as únicas álgebras lineares associativas, ou não, que verificam a lei do produto. Os estudos acerca de generalizações de álgebras lineares associativas continuaram e Dickson foi um dos grandes nomes do século vinte que se dedicou ao assunto. Neste capítulo, realizamos um estudo detalhado de seus trabalhos em quatérnios.

4.2 O Teorema de Hurwitz

4.2.1 As Contribuições de Dickson em Quatérnios

Iniciamos nossos estudos sobre as contribuições de Dickson em quatérnios, destacando seu trabalho *On Quaternions and their Generalization and the History of the Eight Square Theorem*, de 1919 ([205]), onde aparece o primeiro exemplo das hoje chamadas **álgebras de Cayley-Dickson** (na construção dos octônios). Entretanto, as idéias para construção de tais álgebras surgiram no seu trabalho anterior *On Commutative Linear Algebras in which Division is Always Uniquely Possible*, de 1906 ([122]), que discutiremos com mais detalhes no capítulo 5, onde Dickson apresenta casos particulares de álgebras de Cayley-Dickson (a álgebra de partida é um corpo).

Em [205], Dickson declara que seu objetivo é apresentar a história das generalizações do teorema dos oito quadrados e dar uma demonstração mais simples do teorema de Hurwitz:

“Objects of the paper: We shall present the history of the generalizations to four and eight squares of the familiar formula

$$(a^2 + b^2)(\alpha^2 + \beta^2) = r^2 + s^2, \quad r = a\alpha - b\beta, \quad s = a\beta + b\alpha, \quad (4.1)$$

and a elementary exposition of Hurwitz’s proof that such a formula holds only for 2, 4 or 8 squares”¹.

Ainda observa que, para estes três casos (ou seja, para 2, 4 ou 8 quadrados), (4.1) admite uma interpretação simples como normas de elementos dos complexos, dos quatérnios e dos octônios (álgebra de Cayley), respectivamente:

¹Dickson afirma que seu interesse em dar uma nova demonstração deste teorema surgiu da sua observação que os estudantes tinham dificuldades em acompanhar os passos da prova resumida dada por Hurwitz. Logo, ele decidiu mostrar mais detalhadamente o referido teorema.

“For these three cases we shall show that the formula admits of a simple interpretation concerning the norms of numbers which are ordinary complex numbers, quaternions or numbers of Cayley’s algebra with 8 units.”

Apesar de o objetivo de Dickson, ao escrever este artigo, ter sido apresentar uma prova mais simples do teorema de Hurwitz (hoje existem demonstrações muito mais elementares do que a dada por ele), atualmente sua importância se deve à primeira parte do trabalho, onde constrói e apresenta as propriedades fundamentais dos complexos, dos quatérnios e dos octônios.

Inicialmente, define *norma* de um número complexo $a + bi$, onde $a, b \in \mathbb{R}$, como sendo $a^2 + b^2$ e observa que a fórmula (4.1) expressa a propriedade que o produto das normas de dois números complexos é a norma do seu produto (lei do produto, já citada na introdução deste capítulo).

A fim de estudar os quatérnios e a álgebra de Cayley, define brevemente números complexos como pares de números reais (conforme definição dada por Hamilton) e introduz algumas relações que devem ser válidas para estes pares:

1. *Dois pares (a, b) e (α, β) são iguais se, e só se, $a = \alpha$ e $b = \beta$.*
2. *Adição entre dois pares: $(a, b) + (\alpha, \beta) = (a + \alpha, b + \beta)$.*
3. *Multiplicação entre dois pares: $(a, b)(\alpha, \beta) = (r, s)$, onde r e s são dados em (4.1).*
4. *Multiplicação de um par por um número real: se $m \in \mathbb{R}$, então $m(a, b) = (a, b)m = (ma, mb)$.*

Identificando $1 = (1, 0)$ e $i = (0, 1)$, tem-se

$$(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1) = a + bi.$$

Logo, as definições dadas anteriormente tornam-se:

$$(a + bi) + (\alpha + \beta i) = (a + \alpha) + (b + \beta)i$$

e

$$(a + bi)(\alpha + \beta i) = r + si.$$

Analogamente, Dickson considera quádruplas (a, b, c, d) de números reais ou complexos e define adição e multiplicação entre estas quádruplas por:

$$(a, b, c, d) + (\alpha, \beta, \gamma, \delta) = (a + \alpha, b + \beta, c + \gamma, d + \delta)$$

e

$$(a, b, c, d)(\alpha, \beta, \gamma, \delta) = (A, B, C, D),$$

onde

$$\begin{cases} A = a\alpha - b\beta - c\gamma - d\delta, \\ B = a\beta + b\alpha + c\delta - d\gamma, \\ C = a\gamma - b\delta + c\alpha + d\beta, \\ D = a\delta + b\gamma - c\beta + d\alpha. \end{cases} \quad (4.2)$$

Assim como nos complexos, identifica $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ e $k = (0, 0, 0, 1)$ (chamadas *unidades*) e define $m(a, b, c, d) = (a, b, c, d)m = (ma, mb, mc, md)$, onde $m \in \mathbb{C}$. Então, passa a considerar os quatérnios como os elementos da forma

$$q = (a, b, c, d) = a + bi + cj + dk,$$

com tábua de multiplicação dada por

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k, ji = -k \\ jk = i, kj = -i \\ ki = j, ik = -j. \end{cases} \quad (4.3)$$

Claramente tem-se que a multiplicação não é comutativa, entretanto, é associativa.

Considerando o quatérnio q acima e definindo seu *conjugado* por $q' = a - bi - cj - dk$, tem-se que $N(q) = qq' = a^2 + b^2 + c^2 + d^2$, onde $N(q)$ é chamada *norma* de q . Se $q \neq 0$ é um quatérnio real (ou seja, se $a, b, c, d \in \mathbb{R}$), Dickson mostra que a álgebra dos quatérnios é uma álgebra com divisão e que vale a lei do produto, isto é:

$$(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = A^2 + B^2 + C^2 + D^2, \quad (4.4)$$

onde A, B, C, D são como em (4.2)².

Para definir a álgebra de Cayley (octônios), Dickson considera a álgebra com as unidades $1, i_1, \dots, i_7$, tais que $i_1^2 = \dots = i_7^2 = -1$ e verificam

²Dickson observa, neste momento, que Euler já havia descoberto a fórmula (4.4) quando investigava seu *elegante* (palavra usada por Dickson) teorema que afirma que todo inteiro positivo é a soma de quatro quadrados. Como todo inteiro positivo é um produto de números primos, a fórmula (4.4) mostra que todo número primo é a soma de quatro quadrados.

$$\left\{ \begin{array}{lll} i_1 i_2 = i_3 = -i_2 i_1, & i_2 i_3 = i_1 = -i_3 i_2, & i_3 i_1 = i_2 = -i_1 i_3 \\ i_1 i_4 = i_5 = -i_4 i_1, & i_4 i_5 = i_1 = -i_5 i_4, & i_5 i_1 = i_4 = -i_1 i_5 \\ i_6 i_2 = i_5 = -i_2 i_6, & i_2 i_4 = i_6 = -i_4 i_2, & i_4 i_6 = i_2 = -i_6 i_4 \\ i_6 i_5 = i_3 = -i_5 i_6, & i_5 i_3 = i_6 = -i_3 i_5, & i_3 i_6 = i_5 = -i_6 i_3 \\ i_7 i_2 = i_5 = -i_2 i_7, & i_2 i_5 = i_7 = -i_5 i_2, & i_5 i_7 = i_2 = -i_7 i_5 \\ i_7 i_3 = i_4 = -i_3 i_7, & i_3 i_4 = i_7 = -i_4 i_3, & i_4 i_7 = i_3 = -i_7 i_4 \\ i_1 i_7 = i_6 = -i_7 i_1, & i_7 i_6 = i_1 = -i_6 i_7, & i_6 i_1 = i_7 = -i_1 i_6. \end{array} \right. \quad (4.5)$$

Desde que $1, i_1, i_2$ e i_3 satisfazem as relações (4.3), ele substitui as quatro primeiras unidades por $1, i, j, k$. Escrivendo $e = i_4$, as unidades restantes são substituídas por $ie = i_5$, $je = i_6$ e $ke = i_7$. Daí, obtém que todo elemento da álgebra pode ser escrito na forma $q + Qe$, onde q e Q são funções lineares de $1, i, j, k$, ou seja, são quatérnios³.

Definindo a norma de $(q + Qe)$ por $(qq' + QQ')$, onde q' e Q' são os conjugados de q e Q , respectivamente, conclui que ela é o produto de $(q + Qe)$ pelo seu conjugado $(q' - Qe)$ e, então, Dickson mostra que vale a lei do produto nesta álgebra. Logo, a norma de todo elemento desta álgebra é a soma de oito quadrados. Ainda: se q e Q são quatérnios reais, a álgebra é com divisão.

Com isto, Dickson exhibe álgebras lineares com 2, 4 e 8 unidades onde vale a lei do produto, ou seja, a norma do produto de dois de seus elementos é igual ao produto de suas normas (obtendo então os teoremas dos 2, 4 e 8 quadrados, respectivamente), e tais que, se suas coordenadas são reais, então são álgebras com divisão⁴.

Em seguida, Dickson passa a estudar para quais valores de n a identidade

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2 \quad (4.6)$$

pode expressar o produto $(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2)$ como soma dos quadrados de n funções bilineares de $x_1, \dots, x_n$ e $y_1, \dots, y_n$.

Desenvolve este estudo em três etapas: na primeira, mostra que (4.6) vale apenas quando n é par; na segunda, obtém algumas condições necessárias para que (4.6) valha; e na

³Aqui, Dickson apresenta pela primeira vez a construção de uma álgebra de Cayley-Dickson. Para mais detalhes deste tipo de álgebra, veja a seção (5.2) onde explicamos essas idéias.

⁴Dickson observa que, embora estas três álgebras possuam estas duas propriedades fundamentais, elas diferem nas propriedades da multiplicação definida em cada uma delas:

“For complex numbers multiplication is both commutative and associative, for quaternions it is associative but not commutative, for Cayley’s algebra of 8 units it is neither commutative nor associative.”

(“Para os números complexos a multiplicação é comutativa e associativa, para os quatérnios é associativa mas não comutativa, para a álgebra de Cayley de 8 unidades não é comutativa nem associativa.”).

última etapa deduz que os valores possíveis para n na fórmula (4.6) são 1, 2, 4 ou 8. Com isto, Dickson prova o

Teorema de Hurwitz: *Exceto para $n = 1, 2, 4, 8$, não existe a identidade (4.6) expressando o produto $(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2)$ como soma de quadrados de $z_1, \cdots, z_n$ que sejam funções lineares de $x_1, \cdots, x_n$ e $y_1, \cdots, y_n$.*

4.2.2 A História do Teorema dos Oito Quadrados

Antes de Hurwitz provar seu teorema, muitos matemáticos sucederam-se na tentativa de descobrir para qual valor de n a expressão (4.6) é verdadeira. L. Euler (1707-1783) e C. F. Gauss (1777-1855) já haviam observado que (4.4) pode ser expressa, de modo mais simples, por:

$$(N(\alpha) + N(\beta))(N(\gamma) + N(\delta)) = N(\alpha\gamma + \beta\delta) + N(\alpha\delta' - \beta\gamma'),$$

onde α, β, γ e δ são números complexos, δ' representa o conjugado de δ e $N(\alpha)$ é a norma de α . Em 1818, C. P. Degen estendeu (4.4) a oito quadrados e afirmou, erroneamente, que esta fórmula vale para 2^n quadrados e tentou mostrar sua veracidade para 16 quadrados (no que, obviamente, não obteve sucesso). Já Graves, em 1844, e Cayley, em 1845, obtiveram o mesmo resultado, enquanto que o primeiro autor acreditava ser possível estender (4.4) a 2^n quadrados. Entretanto, J. R. Young observou que isto é impossível e exibiu um contra-exemplo para o caso de 16 quadrados: para $k = 2, 4, 8$, o produto de uma soma de km quadrados por uma soma de kn quadrados pode ser expresso como uma soma de kmn quadrados.

Em 1852, Cayley também tentou estender a fórmula para 2^n quadrados, mas apenas forneceu condições para que o teorema valha. Já A. Lebesgue deu uma fórmula para os oito quadrados em 1859 que, a menos de sinal, remete às condições dadas por Cayley. Posteriormente, em 1887, A. Puchta interpretou corretamente a fórmula para os oito quadrados, por meio de corpos regulares com nove vértices no espaço de dimensão oito. Ainda: E. Mathieu mostrou esta fórmula, em 1862, e afirmou que a expressão (4.4) não pode ser estendida para mais que oito quadrados. Já E. Sadun (em 1899) mostrou, de forma mais simples que seus antecessores, a impossibilidade de uma fórmula para $n = 16$. Entretanto, como vimos acima, o primeiro a provar realmente que o resultado só vale para 2, 4 ou 8 quadrados foi Hurwitz.

É interessante observar que Dickson é muito cuidadoso quanto ao registro histórico dos progressos nessa área. Os dados acima, bem como muitos outros detalhes, encontram-se no seu artigo [205].

4.3 A Aritmética dos Quatérnios

No trabalho *Arithmetic of Quaternions*, de 1921 ([218]), Dickson realiza um estudo detalhado da aritmética dos quatérnios, apresentando vários conceitos e teoremas análogos aos da Teoria de Números. Como não pressupõe nenhum conhecimento, inicia este artigo definindo a álgebra dos quatérnios sobre os números complexos, assim como a conjugação e a norma de um quatérnio. Em seguida, observa que valem a propriedade associativa e a propriedade da norma (ou seja, a norma do produto é o produto da norma). De posse disto, passa a desenvolver uma teoria da aritmética de quatérnios, que à época era importante ferramenta para resolver alguns problemas da teoria de números; entretanto, ressalta que para desenvolver quais quatérnios serão chamados inteiros (os **quatérnios inteiros**):

“Quaternions have recently been applied to the solution of several important problems in the theory of numbers. For this purpose it is necessary to make a choice of the quaternions which are to be called integral.”

Em seus estudos, Dickson segue a mesma definição dada por Lipschitz⁵ em 1886, mas desenvolve uma teoria mais direta e elementar:

“...the present theory is more direct and elementary than the earlier theories...”

Os trabalhos de Lipschitz eram baseados em soluções de congruências

$$\xi^2 + \eta^2 + \zeta^2 \equiv 0 \pmod{p^k}$$

e não faziam menção a máximo divisor comum (o que de fato não é aplicável em geral)⁶. Em alguns de seus estudos, Dickson ainda faz a suposição de que a norma do quatérnio seja ímpar (o **quatérnio ímpar**) e observa que isto não é inconveniente algum para sua aplicabilidade:

“The limitation that one of the quaternions is odd causes no inconvenience for the applications. Moreover, it is of theoretical interest to know exactly to what extent we can meet the difficulties which arise in the arithmetic of quaternions in which the integral quaternions are defined naturally to be those with integral coordinates exclusively.”

⁵Para Lipschitz, quatérnios inteiros são aqueles cujas coordenadas são inteiros, exclusivamente, e estes quatérnios não obedecem às leis essenciais de divisibilidades dos números inteiros.

⁶Hurwitz também estudou a aritmética dos quatérnios, em [HR], mas considerou como quatérnios inteiros aqueles cujas coordenadas são inteiros ou a metade de inteiros ímpares. Entretanto, a presença do fator 2 no denominador de alguns quatérnios mostrou-se inconveniente na aplicação da teoria de Hurwitz à completa solução em inteiros de equações quadráticas em diversas variáveis, conforme apresentado em [209].

Dickson também define unidade (quatérnio cuja norma é unitária) e observa que existem oito unidades: ± 1 , $\pm i$, $\pm j$ e $\pm k$.

Na teoria ordinária da divisibilidade em $\mathbb{Z}$, os inteiros a e $-a$ têm exatamente o mesmo conjunto de divisores e, por isso, dizem-se associados. Notemos que os associados de um inteiro a são obtidos multiplicando-o por 1 e -1, que são os elementos inversíveis de $\mathbb{Z}$. Dickson nota que um quatérnio inteiro tem oito associados que são obtidos multiplicando-o pelas oito unidades acima. Neste artigo define, também, divisores à direita e à esquerda de um quatérnio, o que se faz necessário por este ser um anel não comutativo. Com estes conceitos em mãos, passa a desenvolver a aritmética dos quatérnios inteiros.

Após dar algumas definições preliminares (como, por exemplo, divisor de um quatérnio inteiro) e mostrar alguns resultados, prova o “Algoritmo da Divisão” para os quatérnios inteiros:

Teorema: *Para qualquer quatérnio inteiro a , se b é um quatérnio ímpar, podemos encontrar quatérnios inteiros q , c , q_1 e c_1 tais que*

$$\begin{aligned} a &= qb + c, & N(c) < N(b), \\ a &= bq_1 + c_1, & N(c_1) < N(b). \end{aligned}$$

Em seguida, define máximo divisor comum (mdc) à esquerda e à direita de dois quatérnios inteiros. De posse disto, demonstra o equivalente ao “Teorema de Bézout” que afirma que o mdc (tanto à direita como à esquerda) de dois quatérnios inteiros, onde um deles é ímpar (condição que ele mostra ser essencial), pode ser expresso como combinação linear deles:

Teorema: *Para quaisquer dois quatérnios inteiros a e b , tais que pelo menos um deles é ímpar, existe um máximo divisor comum à direita D que é unicamente determinado a menos de um fator unitário. Ainda*

$$D = Aa + Bb,$$

onde A e B são quatérnios inteiros. Do mesmo modo, existe um máximo divisor comum à esquerda δ , único a menos de um fator unitário, para o qual

$$\delta = a\alpha + b\beta,$$

onde α e β são quatérnios inteiros.

Na seqüência, define quando dois quatérnios inteiros, onde pelo menos um deles é ímpar, são relativamente primos e quando um quatérnio inteiro é primo. Usando estes

conceitos, finaliza seus estudos mostrando o equivalente ao hoje conhecido como Teorema Fundamental da Aritmética, que afirma que todo quatérnio ímpar pode ser expresso de modo único (a menos de associações com fatores unitários) como produto de quatérnios primos, no seguinte

Teorema: *Se c é um quatérnio ímpar e $N(c) = pqr \cdots$, onde $p, q, r, \cdots$ são os fatores primos (iguais ou distintos) de $N(c)$ distribuídos em ordem arbitrária, mas definida, então $c = \pi\kappa\rho \cdots$, onde $\pi, \kappa, \rho, \cdots$ são quatérnios primos cujas normas são $p, q, r, \cdots$ respectivamente. Esta decomposição é única a menos de associações com fatores unitários.*

4.4 Generalizações dos Quatérnios

Como uma continuação natural de seus estudos em quatérnios, Dickson passou a estudar suas generalizações em *Quaternions and their Generalizations*, de 1921 ([220]), e em *On the Theory of Numbers and Generalized Quaternions*, de 1924 ([235]).

No primeiro destes trabalhos, Dickson deduz a álgebra dos quatérnios e as suas generalizações diretas, sem assumir a associatividade ou comutatividade da multiplicação. Antes, conforme a sua habitual preocupação em descrever a história das questões com apreço, destaca que Frobenius mostrou que as únicas álgebras lineares associativas com divisão são os números reais, os números complexos e a álgebra dos quatérnios sobre os reais e ressalta o importante papel que a descoberta da álgebra dos quatérnios, por Hamilton em 1843, teve no desenvolvimento da teoria de álgebras lineares. Dickson ainda observa que introduziu, no seu artigo *On the Relation Between Linear Algebras and Continuous Groups*⁷, de 1915 ([194]), os quatérnios de modo natural como um grupo contínuo a quatro parâmetros que preserva as retas numa superfície quadrática:

“Later, the writer was led to quaternions naturally by means of the four-parameter continuous group which leaves unaltered each line of a set of rulings

⁷Neste trabalho, Dickson apresenta uma relação bastante elementar entre uma álgebra associativa e um grupo contínuo a qual permite traduzir os conceitos e teoremas de uma teoria para a outra. Como ilustração, estabelece uma correspondência entre a álgebra dos números reais e o grupo contínuo a um parâmetro formado pelas transformações do tipo $T_c : \mathbb{R} \rightarrow \mathbb{R}$, dada por $T_c(z) = cz$. Em seguida, considera o grupo contínuo das transformações lineares que preservam a superfície quadrática S definida por

$$\begin{vmatrix} x_1 & x_2 \\ x_3 & x_4 \end{vmatrix} = 0,$$

onde $x_1, x_2, x_3, x_4 \in \mathbb{C}$ e os coeficientes da transformação também são complexos, e obtém uma correspondência entre este grupo e a álgebra dos quatérnios com coordenadas complexas, que tem, como subálgebra, os quatérnios reais. Através das propriedades destas transformações, obtém que a norma do produto de dois quatérnios é o produto de suas normas.

on the quadratic surface $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0$."

Seus estudos começam com a definição de uma álgebra linear sobre um corpo $\mathbb{F}$. Assumindo que a álgebra tem unidade⁸ e que todo elemento da álgebra satisfaz a uma equação quadrática com coeficientes em $\mathbb{F}$, Dickson passa a investigar as álgebras que verificam a propriedade que a norma do produto de dois de seus elementos é o produto de suas normas. Inicialmente, mostra que a dimensão deste tipo de álgebra é maior que três. Em seguida, tomando a dimensão igual a quatro, obtém que este tipo de álgebra é associativa e é a álgebra dos quatérnios generalizados (sobre $\mathbb{F}$). Dickson finaliza este trabalho dizendo que o estudo de álgebras de dimensão oito é desenvolvido de modo semelhante e tais investigações estão sendo realizadas por um de seus alunos. Não fica claro, entretanto, a qual de seus alunos estava se referindo, mas talvez fosse A. A. Albert, já que, em 1930, publicou um artigo intitulado *A Construction of all non-commutative rational division algebras of order eight* ([AL7]).

No segundo trabalho, Dickson inicia seus estudos apresentando uma demonstração mais simples do teorema de Euler, adaptando os métodos de Bachet, que afirma que todo inteiro positivo é a soma de quatro quadrados inteiros e generaliza este resultado mostrando que as raízes dos quatro quadrados podem ser escolhidas, convenientemente, para satisfazer quatro congruências lineares fixadas. Em seguida, usa quatérnios inteiros (já mencionados na seção 4.3), para obter uma prova simples de que todas as soluções inteiras de

$$x^2 + y^2 + z^2 + w^2 = uv$$

são dadas por

$$x + yi + zj + wk = fAB,$$

onde $u = fN(A)$, $v = fN(B)$, f é um inteiro e A e B são quatérnios cujas coordenadas são inteiros que não têm fator comum maior que um. A partir deste ponto, Dickson estabelece leis de fatoração para quatérnios inteiros e passa a desenvolver sua aritmética baseado nas definições de quatérnios inteiros dadas por Lipschitz e por Hurwitz. Entretanto, nestes estudos, Dickson não supõe o algoritmo da divisão para quatérnios inteiros e mostra a diferença essencial entre as duas teorias: na apresentada por Lipschitz, nem sempre existe máximo divisor comum entre dois quatérnios inteiros.

De modo análogo, Dickson passa a estudar a aritmética de uma nova álgebra, que chamou de **quatérnios generalizados**. Esta álgebra já havia aparecido nos seus estudos em *Linear Algebras*, de 1912 ([173]), embora não fosse dada nenhuma nomenclatura para ela. Em [173] retoma a definição de álgebra linear dada em [83], de 1903, como o conjunto

⁸Dickson usa a palavra *módulo* para indicar o que, hoje, chamamos de elemento unidade.

dos elementos da forma $\sum x_i e_i$, onde $x_i \in \mathbb{F}$ (com $\mathbb{F}$ corpo) e as unidades e_i verificam

$$e_i e_j = \sum_{k=1}^n \gamma_{ijk} e_k,$$

com $i, j = 1, \dots, n$ e $\gamma_{ijk} \in \mathbb{F}$, e passa a estudar álgebras sobre um corpo $\mathbb{F}$, com $\text{car}(\mathbb{F}) \neq 2$, cujos elementos (todos) satisfazem a uma equação quadrática. Para isto, introduz novas unidades $1, E_1, \dots, E_m$ para a álgebra, onde

$$\begin{aligned} E_k^2 &= c_k, & c_k &\in \mathbb{F} \\ E_k E_l + E_l E_k &= 0, & l, k &= 1, \dots, m, \quad l \neq k. \end{aligned}$$

Adicionando a hipótese da associatividade da multiplicação, Dickson mostra que esta álgebra é o próprio corpo $\mathbb{F}$ ou é uma extensão $\mathbb{F}(E_1)$ de $\mathbb{F}$ pelo elemento E_1 da álgebra (onde a ordem de E_1 é dois) ou é uma álgebra cujas unidades satisfazem

$$\begin{aligned} E_1^2 &= c_1, & E_2^2 &= c_2, & E_3^2 &= -c_1 c_2, \\ E_1 E_2 &= E_3 = -E_2 E_1, & E_1 E_3 &= c_1 E_2 = -E_3 E_1 & E_3 E_2 &= c_2 E_1 = -E_2 E_3, \end{aligned}$$

com $c_1, c_2 \in \mathbb{F}$, que hoje chamamos de álgebra dos quatérnios generalizados⁹. A partir disto, Dickson mostra que se particularizar $\mathbb{F} = \mathbb{R}$, obtém-se que as álgebras lineares associativas com divisão sobre $\mathbb{R}$ são o próprio $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$, onde observa que este resultado já havia sido obtido por Frobenius em 1878 e por Charles B. Peirce em 1881 (do mesmo modo que citou este fato no seu trabalho [220], conforme o início desta seção)¹⁰.

Vale ressaltar que, neste trabalho, Dickson também prova que a divisão à esquerda e à direita, por elementos não nulos, sempre é possível nos octônios, fato que passou despercebido por Cayley, quando da construção desta álgebra.

Em [235], Dickson define os inteiros dos quatérnios generalizados como elementos da forma $X = x + yi + zH + wL$, onde x, y, z e w são inteiros e as unidades i, H e L têm tábua de multiplicação dada por

$$\begin{aligned} i^2 &= -1, & iH &= L, & iL &= -H, & Hi &= i - L, & Li &= H - 1, \\ H^2 &= H - \epsilon, & HL &= \epsilon i, & LH &= L - \epsilon i, & L^2 &= -\epsilon, \end{aligned}$$

⁹No trabalho *Linear Associative Algebra and Abelian Equation* ([184]) (que será apresentado no capítulo 5), Dickson cita este resultado para mostrar que uma álgebra cíclica de dimensão quatro é a álgebra dos quatérnios generalizados.

¹⁰Neste artigo, Dickson ainda mostra que se uma álgebra linear comutativa (a associatividade não é assumida) é com divisão, então sua dimensão é pelo menos seis. Ainda exhibe uma álgebra comutativa com divisão de dimensão seis onde seus elementos satisfazem uma equação de grau quatro.

onde ϵ é um inteiro. Definindo conjugado e norma de um quatérnio generalizado inteiro, mostra que nesta álgebra a norma do produto de dois de seus elementos inteiros é o produto de suas normas. De posse destas ferramentas, Dickson estabelece leis de fatoração para quatérnios generalizados inteiros e observa que nenhum método havia sido sugerido, até o momento, devido à impossibilidade de encontrar-se o máximo divisor comum à esquerda de dois destes elementos por um algoritmo da divisão:

“... the laws of factorization in a arithmetic of generalized quaternions for which no previous method has been suggested since it is impossible to find the (existing) greatest common left divisor by an algorithm of divisions with remainders of decreasing norms.”

Vale ressaltar que as leis de divisibilidade, estabelecidas neste artigo para quatérnios generalizados inteiros, são totalmente similares àquelas desenvolvidas por Hurwitz para os quatérnios inteiros, conforme observado por Dickson:

“The laws of divisibility are entirely similar to those of Hurwitz’s integral quaternions.”

Com isto, encerramos nossos estudos acerca das contribuições de Dickson em quatérnios.

Capítulo 5

Novos Exemplos de Álgebras com Divisão

5.1 Os Primeiros Exemplos

Na época em que Frobenius mostrou que as únicas álgebras associativas com divisão são os números reais, os números complexos e a álgebra dos quatérnios sobre os reais, os estudos em álgebras eram desenvolvidos apenas sobre os reais ou sobre os números complexos e nenhuma técnica para trabalhar com álgebras sobre corpos quaisquer havia sido apresentada (o primeiro trabalho nesta direção deve-se a Wedderburn, conforme citado em (1.4)). Logo, a questão de encontrar-se todas as álgebras com divisão (de dimensão finita) parecia pertinente, embora os matemáticos daquele tempo não tivessem idéia de como resolver o problema. Em 1893, Moore provou (em [MO1]) que todo corpo finito é um corpo de Galois e, desde que todos os corpos finitos são álgebras comutativas com divisão, tornava-se natural a pergunta: “Quais são as álgebras com divisão finitas?”¹. A resposta a esta pergunta permaneceu em aberto até Wedderburn e Dickson² mostrarem, em 1905, que toda álgebra com divisão finita é um corpo em *A Theorem on Finite Algebras* ([WE1]) e em *On Finite Algebras* ([119]), respectivamente. Vale ressaltar que Wedderburn tentou mostrar este teorema diretamente, enquanto Dickson procurou um contra-exemplo para ele, ou seja, uma álgebra com divisão finita e não comutativa. Mas apesar de não atingirem seu objetivo, as

¹Vale ressaltar que o primeiro exemplo de álgebra com divisão de dimensão infinita foi apresentado por Hilbert, em 1898, para ilustrar o fato de que um corpo ordenado não-arquimediano não é necessariamente comutativo: o corpo de séries de potências em duas variáveis não comutativas. Entretanto, na época, não se reconhecia que este exemplo constituía uma álgebra com divisão.

²O interesse de Dickson pelo assunto é natural, pois havia se tornado um grande especialista em corpos de Galois com a publicação em 1897 de sua tese, [12], e do livro *Linear Groups with an Exposition of Galois Field Theory* em 1901, [49].

pesquisas de Dickson foram bastante produtivas: encontrou uma classe de álgebras finitas associativas cujos elementos são inversíveis e satisfazem à distributividade à esquerda, mas não necessariamente à direita³.

Em *On Finite Algebras*, Dickson declara seu objetivo de estudar a independência de um conjunto de postulados para um corpo finito com p^n elementos (o corpo de Galois $\text{GF}[p^n]$), devido à sua unicidade e sua conseqüente importância para a teoria de grupos:

*“Just as certain non-Euclidean geometries offer more interest than others, so the algebras which obey all the postulates for a field except commutativity or associativity of multiplication are of greatest interest”*⁴.

Para ilustrar suas palavras, apresenta exemplos de álgebras finitas cujos elementos não nulos formam um grupo aditivo comutativo em que vale a distributividade à esquerda, mas não à direita.

Neste artigo, retoma a definição de corpo dada em 1903 ([82], e apresentada em (A.1.1)) e acrescenta um postulado de finitude para o conjunto:

Postulado: *O número de elementos distintos é p^n , onde p é um primo fixado e n é um inteiro positivo fixado.*

Usando o método de Hilbert, mencionado no capítulo 3, demonstra a independência dos postulados. De posse destes, mostra que se uma álgebra com divisão é finita, então tem p^n elementos e prova que a multiplicação é comutativa. Em nota de rodapé, observa que deve esta demonstração a Wedderburn:

*“For this proof I am indebted to Mr. J.H. Maclagan-Wedderburn”*⁵.

Com isto, Dickson mostra, na seção seis, que toda álgebra com divisão finita é um corpo (de Galois) no seguinte:

³A julgar pelas atas das reuniões do Clube de Matemática da Universidade de Chicago de 1905, Wedderburn e Dickson estavam trabalhando juntos em corpos finitos no início daquele ano. Suas pesquisas renderam a apresentação ao Clube, em janeiro de 1905, de *Proof of Commutativity of Addition and Multiplication in Finite Fields*, por Wedderburn, e *Theorem on Non-Commutativity of Finite Systems*, por Dickson, e a publicação dos artigos citados acima três meses depois.

⁴*“Assim como certas geometrias não-Euclidianas oferecem mais interesse que outras, as álgebras que verificam todos os postulados para um corpo, exceto a comutatividade ou associatividade da multiplicação, são de maior interesse.”*

⁵*“Por esta prova estou em débito com o Sr. J.H. Maclagan-Wedderburn.”*

Teorema: *Se para uma conjunto finito de elementos submetidos aos postulados para as operações de adição e multiplicação $1^+ - 4^+$, $1^* - 4^*$ (postulados para corpo dados em 1903 no artigo [82]) e à distributividade à esquerda e à direita, então o conjunto é um corpo.*

Em outra nota de rodapé, Dickson afirma que este teorema já havia sido demonstrado por Wedderburn e que este, após tomar conhecimento deste trabalho, deu duas novas provas para o referido teorema:

“First proved by Wedderburn, Trans. Amer. Math. Soc., vol. 6, (1905), pp 349-352 (A Theorem on Finite Algebras). Following my simpler proofs above, and using the same lemma, Wedderburn constructed two further simple proofs, loc. cit”⁶.

É importante observar que, na demonstração deste teorema, Dickson utiliza um conhecido resultado da teoria de números apresentado em 1905 ([113]): *para $p = 2$ e $n = 6$ e para $p = 2^k - 1$ e $n = 2$ existe um primo q que divide $p^n - 1$ mas não divide $p^m - 1$ ($m < n$).* Na mesma nota de rodapé citada acima, Dickson observa que este resultado já tinha sido obtido anteriormente:

“I have since found that the theorem was proved earlier but differently by K. Zsigmondy, Monatshefte, 3 (1892) p. 283; and by Birkhoff and Vandiver, Annals of Math., vol. 5, (1904), p. 177”⁷.

Este resultado teve importância imediata para a geometria projetiva. No ano de 1907, em *Non-Desarguesian and Non-Pascalian Geometries*, [VW], Wedderburn e Veblen usaram este teorema e as álgebras cíclicas (apresentadas mais adiante, em 5.3) para mostrar que geometrias finitas não Pascalianas e não Desargueanas podem ser classificadas por álgebras finitas que não são comutativas e nem distributivas à direita.

5.2 As Álgebras de Cayley-Dickson

Dickson continuou seus estudos em álgebras com divisão publicando, em 1906, o artigo *On Commutative Linear Algebras in which Division is Always Uniquely Possible* ([122]),

⁶“Primeiro demonstrado por Wedderburn, Trans. Amer. Math. Soc., vol. 6, (1905), pp 349-352 (A Theorem on Finite Algebras). Seguindo minha demonstração mais simples acima, e usando o mesmo lema, Wedderburn construiu duas demonstrações mais simples, loc. cit.”

⁷“Descobri que o teorema já foi demonstrado anteriormente mas de modo diferente por K. Zsigmondy, Monatshefte, 3 (1892) p. 283; e por Birkhoff e Vandiver, Annals of Math., vol. 5, (1904), p. 177.”

cujas idéias deram origem às hoje chamadas **álgebras de Cayley-Dickson**. Entretanto, o primeiro exemplo deste tipo de álgebra aparece apenas em 1919, no trabalho *On Quaternions and their Generalization and the History of the Eight Square Theorem* ([205]).

Neste artigo, Dickson deduz a álgebra de Cayley (os octônios) a partir da álgebra dos quatérnios na seção quatro: considerando as unidades $1, i, j, k$ dos quatérnios, obtém que um octônio pode ser escrito na forma $q + Qe$, onde q e Q são funções lineares de $1, i, j, k$ (ou seja, são quatérnios), e observa que as 49 relações satisfeitas pelas unidades $i_1, \dots, i_7$ ($i_1^2 = \dots = i_7^2 = -1$ e (4.5)) são equivalentes à única fórmula

$$(q + Qe)(r + Re) = qr - R'Q + (Rq + Qr')e,$$

onde r' e R' são os quatérnios conjugados de r e R , respectivamente. Com isto, Dickson mostra, de modo bastante simples, que a norma do produto de dois octônios é o produto de suas normas, apresentando o primeiro exemplo de uma álgebra de Cayley-Dickson⁸.

Como foi citado acima, embora o primeiro exemplo tenha aparecido apenas em 1919, Dickson já havia apresentado as idéias que deram origem a este tipo de álgebra em 1906, no artigo *On Commutative Linear Algebras in which Division is Always Uniquely Possible* ([122]). Aqui, ele considera álgebras comutativas com $2n$ unidades $e_1, \dots, e_n, e_{n+1}, \dots, e_{2n}$ e coordenadas num corpo $\mathbb{F}$ qualquer (portanto, seus elementos são da forma $a_1e_1 + \dots + a_{2n}e_{2n}$, com $a_i \in \mathbb{F}$), assumindo que n destas unidades definem uma subálgebra, cujos elementos podem ser escritos na forma $A + BI$, onde I é um símbolo, com A e B pertencentes ao corpo $\mathbb{F}(I^2)$. É importante observar que, como a multiplicação não é em geral associativa, A e B não fazem o papel de coordenadas. De posse desta notação, Dickson caracteriza todas as álgebras com dimensão quatro e seis.

Vale ressaltar que a álgebra introduzida em [122] (cujos elementos são da forma $A + BI$, com A e B no corpo $\mathbb{F}(I^2)$) é um caso particular da álgebra de Cayley-Dickson: a álgebra de partida é um corpo.

5.3 As Álgebras Cíclicas

Seguindo com seus estudos, Dickson introduz um dos mais importantes tipos de álgebras com divisão, as **álgebras cíclicas**, tão fundamentais para o desenvolvimento desta teoria (pois permitiram a construção de novos exemplos) que até foram chamadas de **álgebras de Dickson** por Wedderburn. Foram apresentadas, pela primeira vez, num *Abstract* do *AMS Bull.*, v. 12, (1905-1906), pp. 442: Dickson afirma que obteve um exemplo interessante de álgebra associativa com divisão com n^2 unidades. Esta álgebra é aquela cujos

⁸Para maiores detalhes deste tipo de álgebra, veja sua definição e algumas de suas propriedades em (A.6.6.)

elementos são da forma $i_0 e^s$ ($r, s = 0, \dots, n-1$), onde $e^n = \tau$ é uma função racional de i_0 e $e^s i_0^r = i_s e^s$. Ainda: $i_0, i_1 = \theta(i_0), i_2 = \theta^2(i_0), \dots$, onde θ é um $\mathbb{F}$ -automorfismo de $\mathbb{F}(i_0)$ e $\text{Gal}(\mathbb{F}(i_0)/\mathbb{F}) = \langle \theta \rangle$, são as raízes de uma equação cíclica de grau n irredutível em $\mathbb{F}$ (corpo base) e os coeficientes de τ e de $\theta^{n-1}(i_0)$ devem satisfazer a certas condições que podem ser expressas em termos de formas homogêneas de grau n (trataremos este tipo de álgebra, com maiores detalhes, mais adiante). Como o próprio Dickson comenta, e conforme veremos na sequência, este exemplo aparece, em 1914, no trabalho *Linear Associative Algebras and Abelian Equations* ([184]).

Dickson inicia [184] mencionando que no estudo de álgebras associativas cujas coordenadas percorrem um corpo $\mathbb{K}$ qualquer, as álgebras simples (ou seja, as álgebras de matrizes com r^2 unidades) têm grande importância, onde observa (em linguagem moderna) que uma álgebra é simples se, e só se, é uma álgebra de matrizes sobre uma álgebra com divisão⁹. Logo, é de grande importância construir novos exemplos de álgebras com divisão, uma vez que,

“até o momento, a única álgebra associativa com divisão conhecida que não é um corpo é a álgebra dos quatérnios.”

Neste artigo, Dickson exhibe uma álgebra com divisão com uma base com r^2 elementos sobre $\mathbb{K}$ ¹⁰.

Para isto, considera a equação $\kappa(x) = 0$ de grau r , com coeficientes em $\mathbb{K}$ e irredutível em $\mathbb{K}$, cujas raízes são dadas por

$$i, \theta(i), \theta^2(i) = \theta[\theta(i)], \dots, \theta^{s+1}(i) = \theta^s[\theta(i)], \dots, \theta^{r-1}(i), \quad (5.1)$$

onde $\theta(x)$ é um polinômio com coeficientes em $\mathbb{K}$ e

$$\theta^r(i) = i. \quad (5.2)$$

Então mostra que uma álgebra A , sobre $\mathbb{K}$, com r^2 unidades da forma

$$i^s j^k \quad (s, k = 0, 1, \dots, r-1), \quad (5.3)$$

onde

$$ji = \theta(i)j \quad (5.4)$$

⁹Este resultado foi obtido por Wedderburn em 1907 ([WE3]), conforme observado por Dickson.

¹⁰Estudos detalhados são realizados para os casos $r = 2$ e $r = 4$. Já o caso $r = 3$ é analisado em *Algebras and their Arithmetics*, de 1923 ([229]), como veremos na próxima seção.

e

$$j^r = g, \quad g \in \mathbb{K}, \quad (5.5)$$

é associativa¹¹. Logo, a qualquer equação de grau r em $\mathbb{K}$ da forma acima corresponde uma álgebra associativa, sobre $\mathbb{K}$, com r^2 unidades, que ele chama *do tipo L*.

Considera, agora, uma álgebra associativa A sobre um corpo $\mathbb{F}$ que verifica as seguintes propriedades¹²:

1. Existe $i \in A$ tal que $\phi(i) = 0$, onde ϕ é um polinômio em $\mathbb{F}$ de grau n que é irredutível sobre este corpo.
2. Se $a \in A$ é tal que $ai = ia$, então $a \in \mathbb{F}(i)$.
3. Existe $j \in A$, com j não pertencendo a $\mathbb{F}(i)$, tal que $ji = \theta j + \sigma$, onde $\theta, \sigma \in \mathbb{F}(i)$ ¹³.

Dickson mostra, então, que uma álgebra do tipo L satisfaz às condições acima e obtém o

Teorema 1. *A álgebra A contém um elemento j que não está em $\mathbb{F}(i)$ e que verifica a relação (5.4). Entre as raízes de $\phi(x) = 0$ ocorrem os r ($r > 1$) elementos distintos (5.1); como vale a relação (5.2), estes elementos formam um ciclo fechado.*

A equação $\phi(x) = 0$ é chamada de cíclica¹⁴. Na sequência, obtém o Teorema 5 onde prova que toda álgebra associativa que verifica as propriedades 1, 2 e 3 e mais algumas relações, possui uma subálgebra do tipo L .

¹¹Neste ponto, Dickson faz uma ressalva, em nota de rodapé, para o caso especial da equação binomial $x^r - h = 0$: se ocorre uma raiz r -ésima ϵ da unidade em $\mathbb{K}$, com $h \neq a^r$ para todo $a \in \mathbb{K}$, e se r é primo, sabe-se que o polinômio é irredutível em $\mathbb{K}$. Então a álgebra é definida por

$$i^r = h, \quad j^r = g, \quad ji = \epsilon ij.$$

Se $h = g = 1$, então se perde a propriedade da irredutibilidade, mas se obtém a álgebra em que $i = e_2$ e $j = e_1$. Aqui ele observa que esta álgebra já foi considerada, em 1906, por Wedderburn, no artigo *A Theorem on Hypercomplex Numbers* ([WE2]).

¹²Dickson justifica a origem da exigência destas condições dizendo que (1) - (3) valem quando A é a álgebra dos quatérnios sobre $\mathbb{R}$ e as condições (1) e (2) são satisfeitas por qualquer álgebra associativa com divisão D sobre $\mathbb{F}$.

¹³Da associatividade de A segue que quaisquer duas potências de i são comutativas; então, quaisquer dois polinômios em i são comutativos. Do fato que o quociente de dois polinômios em i pode ser expresso como um polinômio em i (resultado da teoria de números algébricos), obtém-se que $\mathbb{F}(i)$ é composto de todos os polinômios em i com coeficientes em $\mathbb{F}$.

¹⁴Disto, segue o nome de *álgebras cíclicas* dado às álgebras obtidas pelo processo descrito no início desta seção.

Teorema 5. *Toda álgebra associativa A sobre o corpo $\mathbb{F}$ com as propriedades 1, 2 e 3 e tal que $g(i) \neq 0$ na equação $j^r = g(i)$ (onde g é um polinômio em $\mathbb{F}$) tem uma subálgebra S sobre $\mathbb{F}$ que pode ser expressa como a álgebra L (sobre um corpo $\mathbb{K}$) com as r^2 unidades (5.3) linearmente independentes em $\mathbb{K}$.*

Mas, observando que se N é um elemento de L que é comutativo com i então N é um polinômio em i com coeficientes em $\mathbb{K}$, obtém o

Teorema 6. *Toda álgebra do tipo L (álgebra cíclica) tem as propriedades 1, 2 e 3, com n substituído por r e $\mathbb{F}$ por $\mathbb{K}$.*

De posse destas ferramentas, Dickson faz alguns comentários a respeito do caso $r = 3$ e afirma que os detalhes ainda estão na forma de manuscritos. Na seqüência, mostra que se g (da relação (5.5)) não é uma norma em $\mathbb{K}(i)$, então a álgebra é com divisão. Em seguida, realiza um estudo detalhado dos casos $r = 2$ e $r = 4$ (onde mostra que existem álgebras do tipo da A do Teorema 1 com dezesseis unidades) e observa que um teorema mais geral sobre r foi desenvolvido por Wedderburn, em 1913 (*A Type of Primitive Algebras*, [WE4]), dizendo que a demonstração é breve e elegante:

“For a general value of r the last theorem was found in November, 1913, by Professor Wedderburn; his brief and elegant proof will appear . . .”¹⁵.

Considera agora $r = 2$ e $\text{car}(\mathbb{K}) \neq 2$. A equação irredutível satisfeita por i pode ser dada por

$$i^2 = c,$$

aplicando uma transformação linear em i . A álgebra L tem, então, as unidades $1, i, j, k$, onde

$$\begin{aligned} i^2 &= c, & j^2 &= g, & k^2 &= -cg, \\ ij &= k = -ji, & jk &= -gi = -kj, & ki &= -cj = -ik. \end{aligned}$$

Conforme provado, em 1912, no artigo *Linear Algebras* ([173]), esta álgebra é com divisão se, e só se, c não é um quadrado em $\mathbb{K}$ e $g \neq x^2 - cy^2$, com $x, y \in \mathbb{K}$. Então L é a álgebra dos quatérnios generalizados (em nota de rodapé, Dickson observa que a álgebra dos quatérnios ordinária é aquela em que $c = g = -1$ e $\mathbb{K} = \mathbb{R}$).

Prosseguindo em seu trabalho, Dickson mostra que não existe uma álgebra do tipo da Teorema 1 com oito unidades e afirma, em nota de rodapé, que então pode dar uma prova simples do teorema de Frobenius:

¹⁵Em seu artigo, Wedderburn cita este trabalho de Dickson dizendo que, para $r = 2$ e $r = 3$, ele mostrou que para g e θ escolhidos convenientemente a álgebra L é com divisão. Aqui, Wedderburn desenvolve estudos, para encontrar valores para r , θ e g que tornam as álgebras de Dickson (neste artigo, Wedderburn introduz esta denominação para as álgebras cíclicas) com divisão.

“We may thus give a remarkably simple proof of the famous theorem that a linear associative algebra (over the field of reals) in which division is always possible and unique is either the field of reals, the field of ordinary complex numbers or the system of real quaternions.”

Na mesma nota de rodapé, Dickson ainda afirma que, fazendo uso das primeiras linhas do sexto parágrafo (página 64) de [173], demonstra-se facilmente que se a álgebra possui mais que duas unidades, então tem uma subálgebra do tipo dos quatérnios:

“Indeed, it is very easily shown that if there be more than two units, the algebra has a subalgebra of the quaternions type [making use of these Transactions, vol:13 (1912), p. 64, first lines of §6].”

Dickson finaliza seus estudos acerca deste tipo de álgebras, provando que existem álgebras associativas com as propriedades 1, 2 e 3 e distintas de suas subálgebras.

5.4 O Exemplo de Álgebra com Divisão de Dimensão Maior que Quatro

5.4.1 O Livro *Algebras and their Arithmetics*

Este livro, publicado em 1923, transformou-se num marco no estudo das álgebras: por ser um dos primeiros livros a tratar da estrutura das álgebras de modo simples e completo, virou referência para a pesquisa acerca do assunto. Vale ressaltar que, como veremos abaixo, Scorza já havia publicado, em 1921, o primeiro livro a tratar da estrutura das álgebras; entretanto, pelos motivos também citados abaixo, este livro não teve a mesma importância da publicação de Dickson.

Em *Algebras and their Arithmetics*, Dickson desenvolve uma teoria bastante geral da aritmética de álgebras, que ele afirma ser o ápice da aritmética:

“Just as the final stage in the evolution of number was reached with the introduction of hypercomplex numbers (which make up a linear algebra), so also in arithmetic, which began with integers and was greatly enriched by the introduction of integral algebraic numbers, the final stage of its development is reached in the present new theory of arithmetics of linear algebras”¹⁶.

¹⁶“Assim como o estágio final na evolução de número foi alcançado com a introdução de números hiper-complexos (que constituem uma álgebra linear), então também em aritmética, que começou com inteiros e foi notavelmente enriquecida pela introdução de números algébricos inteiros, o estágio final de seu desenvolvimento é alcançado na presente nova teoria da aritmética de álgebras lineares.”

Esta nova teoria é baseada na teoria de álgebras sobre um corpo qualquer que, conforme já foi mencionado no presente trabalho, foi apresentada pela primeira vez por Wedderburn, em 1907 ([WE3]). No prefácio deste livro, Dickson observa que as demonstrações de alguns dos principais teoremas de [WE3] eram excessivamente complicadas e obscurecidas pela identificação de álgebras que têm as mesmas unidades, mas com coordenadas em corpos diferentes; entretanto, Scorza, em 1921, ([SZA]) deu uma prova mais simples do teorema sobre estrutura de álgebras simples, mas omitiu os mais importantes resultados sobre álgebras com divisão, assim como o principal teorema acerca de álgebras lineares. Mas, apesar disto, seu livro simplificou muito o entendimento da teoria abstrata de álgebras e, por isso, constituiu-se num importante material de apoio para a teoria apresentada aqui (embora ambas as teorias difiram em vários aspectos algébricos).

Além de Scorza, Dickson também sofreu grande influência de Wedderburn, que o auxiliou com inúmeras sugestões que propiciaram uma melhor compreensão dos resultados apresentados neste trabalho:

*“An outline of a new simpler proof of that theorem [sobre estrutura de álgebras] was placed at the disposal of the author by Wedderburn, with whom the author has been in constant correspondence while writing this book, and who made numerous valuable suggestions after reading the part of manuscript which deals with the algebraic theory”*¹⁷.

Dickson ainda agradece a contribuição de Wedderburn¹⁸, dizendo:

*“But the chief obligations of the author are due to Wedderburn, both for his invention of the general theory of algebras and for his cordial co-operation in the present attempt to perfect and simplify that theory and to render it readily accessible to general readers”*¹⁹.

¹⁷“Um rascunho de uma nova prova daquele teorema foi colocado à disposição do autor por Wedderburn, com quem o autor tem-se mantido em constante correspondência, enquanto escreve este livro, e que fez inúmeras sugestões valiosas, após ler a parte do manuscrito que trata da teoria algébrica.”

¹⁸Vale ressaltar que Dickson também foi auxiliado por E.H. Moore:

“Acknowledgements are due to Professor Moore, . . . , for valuable suggestions both on the manuscript and on the proofsheets of chapter on arithmetics” (“Agradecimentos também são feitos ao Professor Moore, . . . , pelas valiosas sugestões tanto no manuscrito como nas demonstrações do capítulo sobre aritmética”).

¹⁹“Mas, os principais agradecimentos do autor são feitos a Wedderburn, tanto por sua invenção da teoria geral de álgebras, como por sua cordial cooperação no esforço de aperfeiçoar e simplificar aquela teoria e torná-la prontamente acessível aos leitores em geral.”

No primeiro capítulo deste livro, Dickson define álgebra sobre um corpo qualquer e ilustra esta definição com a álgebra das matrizes quadradas sobre um corpo $\mathbb{F}$ qualquer. Também define a álgebra dos quatérnios e observa que se o corpo base é $\mathbb{R}$, então esta álgebra é com divisão. Já no segundo capítulo, define *conjunto linear*²⁰ com base $x_1, \dots, x_m$ como o conjunto das combinações lineares da forma $\sum \lambda_i x_i$, onde $\lambda \in \mathbb{F}$ e $x_1, \dots, x_m$ são quaisquer elementos de uma álgebra A (não necessariamente associativa). A partir desta definição, deduz várias propriedades de conjuntos lineares. No terceiro capítulo, Dickson define subálgebras invariantes; soma direta, redutibilidade e diferença de álgebras, onde estas não são supostas associativas. Também define álgebras simples (veja (A.5.2)).

O quarto capítulo é dedicado ao estudo de álgebras nilpotentes (A.4.5) e semi-simples (A.5.1), onde Dickson se utiliza dos resultados obtidos por B. Peirce sobre elementos idempotentes (A.5.3). Dentre eles, destacamos a decomposição de uma álgebra relativamente a um elemento idempotente²¹ (que foi de grande importância na demonstração apresentada por Wedderburn no seu teorema sobre estrutura de álgebras): seja A uma álgebra que contém pelo menos um elemento idempotente e . Escreva

$$x_1 = x - ex - xe + exe, \quad x_2 = ex - exe, \quad x_3 = xe - exe,$$

$$I = \sum x_i, \quad B = \sum (ex - xe),$$

onde as somas se estendem sobre todos os elementos x de A . Então

$$A = I + eB + Be + eAe$$

é chamada *decomposição da álgebra A relativa a um elemento idempotente e* .

O quinto capítulo é dedicado às álgebras com divisão e será estudado com maiores detalhes na próxima subseção. Nos sexto e sétimo capítulos, Dickson obtém resultados intermediários que levam à demonstração do principal teorema sobre estrutura de álgebras de Wedderburn (obtido em 1907 em [WE3] e já comentado em (1.4)), que Dickson apresenta no capítulo seguinte.

Já o nono capítulo trata de números algébricos inteiros, onde Dickson desenvolve propriedades essenciais para o estudo da teoria da aritmética de qualquer álgebra racional, que é apresentada no próximo capítulo. Ele observa que, com os resultados obtidos aqui (nono capítulo), esta teoria pode ser vista como uma generalização da teoria de números algébricos. Do mesmo modo como fez em seu trabalho *Arithmetic of Quaternions* ([118]), no longo e importante capítulo dez, Dickson desenvolve detalhadamente a aritmética de uma álgebra racional, assim como reproduz os estudos realizados em [118] sobre a aritmética dos

²⁰Também chamado de *complexo* por Wedderburn e *sistema* por Scorza.

²¹Conhecida como *decomposição de Peirce*.

quatérnios. Já no último capítulo deste livro, obtém as propriedades de corpos que são pré-requisitos para as teorias apresentadas nos capítulos anteriores. Para finalizar, este trabalho possui três apêndices, cujos dois primeiros também serão estudados, na próxima subseção e o terceiro apresenta alguns resultados complementares e problemas em aberto, acerca de álgebras.

5.4.2 Índice do Livro *Algebras and their Arithmetics*

TABLE OF CONTENTS

Chapter		Page
I.	INTRODUCTION, DEFINITIONS OF ALGEBRAS, ILLUSTRATIONS Fields. Linear transformations. Matrices. Linear dependence. Order, basal units, modulus. Quaternions. Equivalent and reciprocal algebras.	1
II.	LINEAR SETS OF ELEMENTS OF AN ALGEBRA Basis, order, intersection, sum, supplementary, product.	25
III.	INVARIANT SUB – ALGEBRAS, DIRECT SUM, REDUCIBILITY, DIFFERENCE ALGEBRAS	31
IV.	NILPOTENT AND SEMI – SIMPLE ALGEBRAS; IDEMPOTENT ELEMENTS Index. Properly nilpotent. Decomposition relative to an idempotent element. Principal and primitive idempotent elements. Semi – simple algebras	43
V.	DIVISION ALGEBRAS Criteria for a division algebra. Real division algebras. Division algebras of order n^2 and 9.	59
VI.	STRUCTURE ALGEBRAS Direct product. Simple algebras. Idempotent elements of a difference algebra. Condition for a simple matrice sub – algebra.	72
VII.	CHARACTERISTIC MATRICES, DETERMINANTS, AND EQUATIONS; MINIMUM AND RANK EQUATIONS Every algebra is equivalent to a matrice algebra. Transformation of units. Traces. Properly nilpotent.	92
VIII.	THE PRINCIPAL THEOREM ON ALGEBRAS Direct product of simple matric algebras. Division algebras as direct sums of simple matric algebras. Complex algebras.	118

Chapter		Page
IX.	INTEGRAL ALGEBRIC NUMBERS	128
	Quadratic numbers. Reducible polynomials. Normal form on integral algebraic numbers. Basis.	
X.	THE ARITHMETIC OF AN ALGEBRA	141
	Case of algebraic numbers. Units and associated elements. Failure of earlier conditions. Arithmetic of quaternions. Arithmetic of a direct sum. Existence of a basis for the integral elements of any rational semi-simple algebra. Integral elements of any simple algebra. Arithmetic of certain simple algebras. Equivalent matrices. The fundamental theorem on arithmetics of algebras. Normalized basal units of a nilpotent algebra. The two categories of complex algebras. Arithmetic of any rational algebra. Generalized quaternions. Application to Diophantine equations.	
XI.	FIELDS	200
	Indeterminates. Laws of divisibility of polynomials. Algebraic extension of any field. Congruences. Galois fields.	
Appendix		
I.	DIVISION ALGEBRAS OF ORDER n^2	221
II.	DETERMINATION OF ALL DIVISION ALGEBRAS OF ORDER 9; MISCELLANEOUS GENERAL THEOREMS ON DIVISION ALGEBRAS	226
III.	STATEMENT OF FURTHER RESULTS AND UNSOLVED PROBLEMS	235
INDEX		

5.4.3 O Primeiro Exemplo

Em 1914, no trabalho *Linear Associative Algebras and Abelian Equations* ([184]), Dickson apresenta condições para que uma álgebra associativa de dimensão nove seja com divisão. Entretanto, o primeiro exemplo de uma álgebra associativa de dimensão diferente de quatro foi realmente construído em detalhes, em 1923, no seu livro *Algebras and their Arithmetics* ([229]), conforme citado acima. Nesta subseção, estudaremos este exemplo e os tópicos relacionados a álgebras com divisão desenvolvidos neste trabalho.

Na primeira parte do quinto capítulo, ou seja, no parágrafo 43, Dickson define uma álgebra com divisão e usa o conceito de elementos idempotentes e de elementos nilpotentes, introduzidos por B. Peirce, para provar vários resultados acerca da divisibilidade de álgebras. Dentre eles, destacamos o

Teorema 2. *Se A tem um único elemento idempotente e e nenhum elemento propriamente nilpotente ²², então A é uma álgebra com divisão com unidade e .*

No parágrafo seguinte, ele faz um breve estudo sobre polinômios em uma única variável. Já no parágrafo 45, Dickson prova o teorema de Frobenius sobre álgebras com divisão reais. No seguinte, deriva álgebras com divisão daquelas já conhecidas e ilustra com um exemplo: considera o corpo $\mathbb{Q}(\rho)$ obtido pela extensão do corpo $\mathbb{Q}$ de todos os números racionais pela junção de uma raiz ρ de uma equação quadrática que tem coeficientes em $\mathbb{Q}$, é irredutível em $\mathbb{Q}$ e tem uma raiz real ρ . Então afirma que a álgebra dos quatérnios sobre o corpo real $\mathbb{Q}(\rho)$ é uma álgebra com divisão, que pode ser vista como uma álgebra sobre $\mathbb{Q}$ com as oito unidades da base sendo

$$1, \rho, i, i\rho = \rho i, j, j\rho = \rho j, k, k\rho = \rho k.$$

No parágrafo 47, Dickson apresenta as álgebras cíclicas e afirma, em nota de rodapé, que estas foram descobertas por ele e receberam de Wedderburn o nome de **álgebras de Dickson**:

“Discovered by the author and called “Dickson algebra” by Wedderburn.”

Já no parágrafo 48, **constrói o primeiro exemplo de uma álgebra com divisão de dimensão nove**. Para isto, observa, inicialmente, que qualquer raiz sétima ($\neq 1$) da unidade satisfaz à equação

$$\frac{\zeta^7 - 1}{\zeta - 1} = \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0. \quad (5.6)$$

Dividindo por ζ^3 , rearranjando os termos e fazendo a substituição

$$\zeta + \frac{1}{\zeta} = \xi, \quad \zeta^2 + \frac{1}{\zeta^2} = \xi^2 - 2, \quad \zeta^3 + \frac{1}{\zeta^3} = \xi^3 - 3\xi, \quad (5.7)$$

obtem

$$\xi^3 + \xi^2 - 2\xi - 1 = 0. \quad (5.8)$$

²²Se $a \neq 0$ é um elemento de uma álgebra A tal que ax e xa são nilpotentes para todo $x \in A$, dizemos que a é propriamente nilpotente.

Observando: do fato que se ϵ é uma raiz ($\neq 1$) de $\zeta^7 = 1$ então ϵ^2 e ϵ^4 também o são, tem-se que são raízes de (5.6). Portanto, por (5.7), as raízes de (5.8) são

$$\xi_1 = \epsilon + \frac{1}{\epsilon}, \quad \xi_2 = \epsilon^2 + \frac{1}{\epsilon^2} = \xi_1^2 - 2, \quad \xi_3 = \epsilon^4 + \frac{1}{\epsilon^4} = \xi_2^2 - 2.$$

Logo, as raízes de (5.8) são, de acordo com (5.1):

$$\xi_1 = \xi, \quad \xi_2 = \theta(\xi) \equiv \xi^2 - 2, \quad \xi_3 = \theta(\xi_2) = \theta[\theta(\xi)] \equiv \theta^2(\xi),$$

onde $\theta(\xi_3) = \theta^3(\xi) = \xi$. Como se mostra que (5.8) é irredutível em $\mathbb{Q}$, tem-se que é uma equação cíclica para o corpo $\mathbb{Q}$. Em seguida, Dickson prova que se $f(\xi_1)$ é um polinômio com coeficientes racionais, então sua norma $N(f)$ nunca é igual a um inteiro par não divisível por oito. Daí, obtém o seguinte:

Teorema. *Se γ é um inteiro par não divisível por 8, a álgebra sobre o corpo dos números racionais definida por*

$$x^3 + x^2 - 2x - 1 = 0, \quad xy = y(x^2 - 2), \quad y^3 = \gamma,$$

é uma álgebra com divisão de dimensão 9.

Com isto, aparece a primeira álgebra com divisão de dimensão nove (que não é um corpo).

No primeiro apêndice deste livro, Dickson estuda condições para que álgebras cíclicas de ordem n^2 (ou seja, de dimensão n^2) sejam com divisão. Para isto, considera a álgebra cíclica D sobre o corpo $\mathbb{F}$ com as n^2 unidades da base sendo

$$y^i x^j \quad (i, j = 0, 1, \dots, n-1),$$

tal que

$$\phi(x) = 0, \quad \phi(\theta(x)) = 0, \quad \dots, \quad \phi[\theta^{n-1}(x)] = 0, \quad \theta^n(x) = x, \quad (5.9)$$

$$xy = y\theta(x), \quad y^n = \gamma \quad (\gamma \in \mathbb{F}) \quad (5.10)$$

e prova o seguinte:

Teorema.²³ *Se nenhuma potência de γ menor que a n -ésima é a norma de um polinômio em x com coeficientes em $\mathbb{F}$, a álgebra D definida por (5.9) e (5.10) é uma álgebra com divisão.*

²³Dickson observa que este teorema já foi apresentado anteriormente e que a prova, mostrada neste livro, é uma ampliação daquela oferecida por Wedderburn, em 1914 ([WE4]).

Já o segundo apêndice é dedicado a determinar todas as álgebras de dimensão nove²⁴ e também trata de alguns teoremas mais gerais sobre álgebras com divisão. No primeiro teorema deste apêndice, Dickson mostra que se uma álgebra com unidade possui uma subálgebra com divisão com a mesma unidade, então seus elementos são o produto de um elemento da subálgebra por outro de um subconjunto da álgebra:

Teorema 1. *Se uma álgebra A de ordem α tem unidade e e contém uma subálgebra com divisão B de ordem β cuja unidade também é e , então existe um subconjunto de A de ordem γ tal que $A = BC$, com $\alpha = \beta\gamma$.*

Daí, obtém uma relação imediata entre as ordens de uma álgebra com divisão e de suas subálgebras no

Corolário 1. *A ordem de uma álgebra com divisão A é um múltiplo da ordem de qualquer subálgebra.*

Considere uma álgebra com divisão A sobre um corpo $\mathbb{F}$ e seja B a álgebra composta dos elementos de A que são comutativos com todo elemento de A ²⁵. A álgebra A é chamada *normal* se B tem ordem um, ou seja, $\mathbb{F}$ é o centro de A . Vale observar que o primeiro autor a considerar este tipo de álgebra foi Wedderburn, em 1921, no trabalho [WE5] (conforme veremos na seção (5.5)). Com esta definição, Dickson prova dois resultados sobre álgebras normais em:

Corolário 2. *A ordem de qualquer álgebra com divisão normal é um quadrado²⁶.*

e

Corolário 3. *Qualquer álgebra com divisão A cuja ordem é o quadrado de um primo p ou é normal ou é equivalente a um corpo.*

De posse destes resultados (e mais alguns outros sobre álgebras normais), Dickson caracteriza todas as álgebras com divisão de ordem nove no

Teorema 5. *Toda álgebra com divisão normal D de ordem 9 sobre um corpo $\mathbb{F} \neq \{1\}$ é gerada por elementos x e y tais que $xy = y\theta(x)$ e $y^3 = \gamma$, onde γ e os coeficientes do polinômio $\theta(x)$ pertencem a $\mathbb{F}$, enquanto que x , $\theta(x)$ e $\theta^2(x) = \theta[\theta(x)]$ são raízes de uma equação cúbica irredutível em $\mathbb{F}$.*

Com isto, Dickson conclui que toda álgebra com divisão de ordem nove ou é um corpo ou é do tipo do teorema acima.

²⁴Em nota de rodapé, Dickson afirma que estes resultados ampliam aqueles apresentados por Wedderburn, em 1921 ([WE5]).

²⁵Em notação matemática escrevemos $B = \{x \in A / xa = ax, \forall a \in A\}$.

²⁶Este resultado já havia sido provado por Wedderburn, em 1921 no trabalho [WE5].

5.4.4 O Artigo Algebras and their Arithmetics

Em nota de rodapé, os editores deste artigo afirmam que este trabalho relata os resultados de alguns trabalhos de Dickson e foi elaborado para comemorar o 75º aniversário da Associação Americana para o Progresso da Ciência (a convite do Comitê), realizado em Cincinnati, entre 27 de dezembro de 1923 e 02 de janeiro de 1924:

“A Report presented to the Society, by invitation of the program committee, at Cincinnati, December 28, 1923. This Report, the work of the author reported in it, and two other papers presented by him to the Society at the Cincinnati ... meetings formed the basis for the award to the author of the seventy-fifth anniversary prize of the American Association for the Advancement of Science for the most notable contribution to the advancement of science presented at the meetings of that Association and its affiliated societies at Cincinnati on December 27, 1923 to January 2, 1924.”

Dickson inicia este trabalho comentando brevemente que desde a descoberta dos quatérnios por Hamilton, tem crescido o interesse pela teoria de álgebras lineares associativas (também chamadas de números hipercomplexos) por autores como Cayley, Clifford e Sylvester na Inglaterra; Poincaré e Cartan na França; Weierstrass, Frobenius, Lipschitz, Molien, Scheffers e Study na Alemanha; Hurwitz e Du Pasquier na Suíça; Benjamin Peirce, C. S. Peirce, Taber, Wedderburn e Hazlett nos Estados Unidos. Entretanto, os artigos mais antigos contêm erros sérios e são um tanto obscuros, pois tratam apenas de algumas álgebras ou falham na tentativa de dar uma teoria mais geral, uma vez que os estudos são desenvolvidos sobre corpos específicos, como o dos complexos. Mas Dickson observa que os resultados obtidos para este corpo têm sido estendidos para álgebras sobre um corpo qualquer, fornecendo subsídios bastante importantes para o desenvolvimento da teoria de álgebras e de números:

“But the results obtained for this very special case have since been extended to algebras over any field, and it is the latter general subject which is the really important one both for algebra and for the theory of numbers.”

Em seguida, apresenta, de modo ilustrativo, a álgebra dos números complexos, a álgebra de matrizes sobre um corpo $\mathbb{F}$ e a álgebra dos quatérnios. Então passa à definição de álgebra com divisão (através do exemplo dos quatérnios reais), define subálgebra (através do exemplo dos complexos considerados como subálgebra dos quatérnios reais), define álgebra invariante e álgebra simples. A partir disto, cita o teorema fundamental que afirma que *toda álgebra simples é equivalente*²⁷ *a uma álgebra de matrizes sobre uma álgebra com divisão.*

²⁷Em linguagem moderna, este termo significa *isomorfa*.

Após definir álgebra nilpotente, álgebra semi-simples e soma direta de álgebras, observa que toda álgebra semi-simples ou é simples ou é a soma direta de álgebras simples e vale a recíproca. Ainda: Dickson cita que o *principal teorema das álgebras* afirma que:

“toda álgebra que não é nilpotente e nem semi-simples é a soma de sua única subálgebra maximal nilpotente invariante e uma subálgebra semi-simples”²⁸.

Dickson passa, então, a tratar da evolução da aritmética das álgebras, observando que seu desenvolvimento foi lento, apesar de o estudo da aritmética dos quatérnios ser naturalmente subsequente ao dos complexos inteiros. Ainda faz um breve comentário a respeito da teoria complicada e incompleta de Lipschitz e da teoria *satisfatória*²⁹, desenvolvida por Hurwitz, para os quatérnios inteiros. Com isto, conclui que, embora tenha sido desenvolvida para os quatérnios, a teoria de Hurwitz pode ser aplicada a qualquer álgebra associativa A sobre os racionais, definindo elementos inteiros de A como aqueles que pertencem a um conjunto, cujos elementos têm as seguintes propriedades:

C (Closure): A soma, a diferença e o produto de quaisquer dois elementos do conjunto também são elementos do conjunto;

B (Basis): O conjunto tem uma base finita; ou seja, contém elementos $b_1, \dots, b_k$ tais que todo elemento do conjunto é uma combinação linear dos b_i s com coeficientes inteiros;

U': O conjunto contém as unidades da base de A ;

M (Maximal): O conjunto é maximal (isto é, não está contido em um conjunto maior que tem as propriedades **C**, **B** e **U'**).

Dickson ainda menciona que um pupilo de Hurwitz, Du Pasquier, publicou um sem número de artigos nos quais troca a hipótese **U'** por uma hipótese mais branda **U**, que supõe que o conjunto contém a unidade 1 que faz o papel de unidade da multiplicação. Mas, tanto a definição de Hurwitz quanto a de Du Pasquier são insatisfatórias e ele ilustra este fato com o exemplo de uma álgebra especial que tem apenas dois elementos na base: 1 e e , onde $e^2 = 0$. Na seqüência, diz que obteve uma teoria satisfatória de elementos inteiros para qualquer álgebra racional, em seu livro *Algebras and their Arithmetics*. Aqui, ele usa os postulados **C**, **U** e **M** acima e, substituindo o postulado **B**, pelo

Postulado R (Equação do posto): Para todo elemento do conjunto, os coeficientes da equação do posto são inteiros ordinários³⁰.

²⁸Na sua formulação mais moderna, este teorema é conhecido como *Teorema de Wedderburn-Malcev* e a subálgebra maximal nilpotente, como *radical de Jacobson* da álgebra dada.

²⁹Expressão usada por Dickson.

³⁰Dickson observa que se $\xi_1, \dots, \xi_n$ são números racionais, então o elemento $x = \xi_1 u_1 + \dots + \xi_n u_n$ de uma álgebra racional A , com base $u_1, \dots, u_n$, é raiz de uma equação univocamente determinada da forma

$$x^r + c_1 x^{r-1} + \dots + c_r = 0,$$

Então obtém que esta teoria é uma generalização da teoria clássica dos números algébricos. Ainda observa que isto é uma extensão da teoria de Du Pasquier, assim como a de Hurwitz é uma extensão da teoria incompleta de Lipschitz e que muitos grandes resultados na matemática são obtidos desta maneira:

“Our satisfactory set may therefore be derived by a suitable enlargement of any one of Du Pasquier’s unsatisfactory sets. Similarly, Hurwitz obtained his satisfactory set of integral quaternions by a suitable enlargement of Lipschitz’s unsatisfactory set. There are many instances in the history of mathematics where success has been achieved by the principle of enlargement.”

A partir daí, deduz alguns resultados sobre a aritmética das álgebras, onde destacamos: *como qualquer álgebra racional A é a soma de sua subálgebra N invariante nilpotente maximal e uma subálgebra semi-simples S , então o teorema fundamental da aritmética estabelece que a aritmética de A é associada com a de S no sentido que todo elemento inteiro de A é o produto de um inteiro de S por uma unidade.* Em seguida, mostra que o estudo da aritmética de uma álgebra semi-simples se reduz ao estudo da aritmética de álgebras simples, que se reduz ao estudo da aritmética de álgebras de matrizes sobre uma álgebra com divisão D . Conclui, então, que o estudo da aritmética de todas as álgebras racionais se reduz ao estudo da aritmética da álgebra de matrizes sobre uma álgebra com divisão D :

“We have therefore reduced the study of the arithmetics of all rational algebras to the study of arithmetics of simple algebras, i.e., of matrix algebras over a division algebra D .”

Um subconjunto de A que satisfaz **C**, **B** e **U'** hoje é chamado de uma *ordem* em A , de modo que Dickson é também pioneiro em perceber a importância das ordens maximais, que, nos dias atuais, são um promissor tema de estudo e pesquisa. Veja, por exemplo, o livro *Maximal Orders*, de I. Reiner ([RE]). O estudo das ordens maximais de álgebras atualmente é considerado o equivalente não comutativo da teoria de números, tal como antecipado por Dickson.

5.5 A Construção de Novos Exemplos de Álgebras com Divisão

Em 1921, Wedderburn publica alguns resultados importantes acerca da teoria de álgebras com divisão no trabalho [WE5]. Observando que se pode considerar estas álgebras

onde $c_1, \dots, c_r$ são polinômios em $\xi_1, \dots, \xi_r$, e x não é raiz de nenhuma equação desta forma, de grau menor que r . Ele chama esta equação e equação do posto.

sobre seus centros e assumindo que elas são *centrais*³¹, mostra que a dimensão destas álgebras sobre seu centro é um quadrado. Neste trabalho, Wedderburn chama estas álgebras de *quadradas* e prova que toda álgebra quadrada de ordem nove é cíclica.

No segundo apêndice do livro *Algebras and their Arithmetics* ([229]), onde estuda as álgebras com divisão de ordem nove, Dickson chama estas álgebras de *normais*, definindo:

“A division algebra A over $\mathbb{F}$ is called normal if the products of its modulus by numbers of $\mathbb{F}$ are the only elements of A which are commutative with every element of A .”

A partir da segunda metade da década de 1920, Dickson passa a dedicar-se a desenvolver métodos para construir novas álgebras com divisão, com a publicação, em 1926, de *New Division Algebras* ([240]). Antes de estudarmos este trabalho, discutiremos brevemente o conceito de produto cruzado, cujas idéias estão implícitas neste artigo, de uma forma mais clara que a que aparece na definição de álgebras cíclicas. Segundo Jacobson ([JA]), este conceito surgiu inicialmente, em 1912, no trabalho [WE5] de Wedderburn e foi redescoberto, em 1923, por Cecioni em [CE1]. Em [BM], Brigaglia e Mammone observam que, também, no livro *Algebren und ihre Zahlentheorie* ([253]) Dickson desenvolve um pouco da teoria de produto cruzado, afirmando que os teoremas 13 e 14 do parágrafo 34 (que é dedicado ao assunto) são uma forma mais polida de apresentar os resultados de Cecioni. Eles ainda mencionam uma frase, presente no parágrafo citado acima, em que Dickson afirma estar em débito com Cecioni pelos resultados apresentados nestes teoremas:

*“Dieser Schritt ist eine Verbesserung des Beweises von Cecioni... Wir entleihen ihm auch Satz 14”*³² (p. 54).

Entretanto, segundo H. Hasse observou, em 1932 ([HAS]), a denominação de **produto cruzado** foi usada pela primeira vez, em 1929, por Emmy Noether (1882-1935):

*“...The proofs of the above theorems may be obtained in the simplest and most lucid manner by subordinating the theory of cyclic algebras or cyclically representable algebras to the theory of **crossed products** (**verschränkte Produkte**)”*³³ *developed recently by Emmy Noether”*³⁴.

³¹Uma álgebra A sobre um corpo $\mathbb{F}$ é chamada *central* se seu centro, denotado por $Z(A) = \{x \in A / ax = xa, \forall a \in A\}$, é o corpo $\mathbb{F}$.

³²“Este passo é um aperfeiçoamento da prova dada por Cecioni... Também tomamos emprestado dele o teorema 14”.

³³Ênfase de Hasse.

³⁴“...As provas dos teoremas acima podem ser obtidas de uma maneira mais lúcida e simples submetendo a teoria de álgebras cíclicas ou álgebras representáveis ciclicamente à teoria de **produtos cruzados**, desenvolvida recentemente por Emmy Noether.”

Neste ponto, em nota de rodapé, Hasse afirma que isto se deu numa conferência na Universidade de Göttingen, em 1929:

*“In a lecture at the University of Göttingen. Em seguida, continua: I have been permitted by the author to give here an account of this very important new theory. The publication by the author herself which will start from a larger base, namely the general theory of representations by matrices (linear substitutions), is likely to appear in the near future”*³⁵.

O interesse de Noether acerca do assunto deu-se através de seus estudos sobre como estender a teoria, já existente, para sistemas hipercomplexos comutativos a sistemas não comutativos. Porém, como ela afirma no capítulo onze de [BS], a principal dificuldade de sua teoria estava em obter uma formulação geral para corpos de Galois. Entretanto, Noether obtém uma extensão ao caso não comutativo considerando simultaneamente corpos e grupos — o “produto cruzado” — e suas constantes de multiplicação — os “sistemas de fatores”. Com isto, obtém uma álgebra normal simples sobre o corpo base e cada álgebra deste tipo pode, essencialmente, ser obtida desta forma. Mas ela atribui as idéias de produto cruzado a Dickson³⁶, assim como observa que Speiser, Schur e R. Brauer³⁷ desenvolveram a teoria de sistemas de fatores de um ponto de partida diferente de Dickson: partiram do problema de representações absolutamente irredutíveis. Em [BS], Noether diz:

*“...extension to the noncommutative has been obtained by the simultaneous consideration of fields and groups”*³⁸ *by means of the “crossed product” and its multiplication constants, the “factor systems”. In this way one obtains a simple normal algebra over the ground field and each such algebra is essentially obtainable thus. Such crossed products were first considered by Dickson, while the theory of factor systems was developed by Speiser, Schur, and R. Brauer from a totally different starting point, namely, from the problem of absolutely irreducible representations.”*

³⁵ “Eu obtive permissão da autora para apresentar aqui esta importante nova teoria. A publicação pela própria autora a qual se iniciará a partir de uma base maior, isto é a teoria geral de representações por matrizes (substituições lineares), provavelmente aparecerá num futuro próximo.”

³⁶ Conforme Brigaglia e Mammone mencionam em [BM], na famosa conferência proferida por Noether, em 1932, em Zurich, ela citou as contribuições de Dickson para o assunto dizendo:

“Such crossed products were first considered by Dickson.”

³⁷ *Über die Bildung des Formensystems der ternären biquadratischen Form*, Jour. f. d. reine u. angew. Math., v. 134, (1908), pp. 23-90.

³⁸ Ênfase de Noether.

Iniciaremos nossos estudos enunciando um resultado que apareceu, pela primeira vez, numa pequena monografia sobre álgebras associativas redigida por Th. Skolem, em 1927, e que será de grande importância para o desenvolvimento da teoria de produtos cruzados e álgebras em geral.

Teorema (Skolem-Noether): Seja A uma álgebra simples central sobre um corpo $\mathbb{F}$ qualquer. Sejam B e B' subálgebras simples de A , de dimensão finita sobre $\mathbb{F}$, que contêm $\mathbb{F}$. Se ϕ é um $\mathbb{F}$ -isomorfismo de B sobre B' ³⁹, então existe um elemento inversível $x \in A$ tal que $\phi(b) = x^{-1}bx$, para todo $b \in B$.

Se A é uma álgebra simples central sobre um corpo $\mathbb{K}$ e $\mathbb{F}$ é um corpo que contém $\mathbb{K}$, dizemos que $\mathbb{F}$ é um *corpo de decomposição* para A se $A \otimes_{\mathbb{K}} \mathbb{F}$ (produto tensorial de A por $\mathbb{F}$ sobre $\mathbb{K}$) é a álgebra das transformações lineares em um espaço vetorial sobre $\mathbb{F}$.

O próximo resultado afirma que existem corpos de decomposição que são extensões normais separáveis sobre $\mathbb{K}$ ⁴⁰. Pelo teorema de Skolem-Noether, basta considerar o problema da existência destes corpos para álgebras com divisão.

Lema (Noether): Seja A uma álgebra com divisão central sobre um corpo $\mathbb{K}$. Então existe um subcorpo maximal⁴¹ $\mathbb{L} \subset A$ que é separável.

O próximo resultado diz-nos que todo subcorpo maximal de A é um corpo de decomposição para A .

Lema: Seja A uma álgebra com divisão e seja $\mathbb{F}$ um subcorpo de A . Então $\mathbb{F}$ é maximal se, e só se, $C_A(\mathbb{F}) = \mathbb{F}$ ⁴².

Com isto, pode-se provar o

³⁹Dizemos que $\phi : B \rightarrow B'$ é um $\mathbb{F}$ -isomorfismo se ϕ é um isomorfismo que fixa todos os elementos de $\mathbb{F}$.

⁴⁰Dizemos que uma extensão algébrica $\mathbb{F}|\mathbb{K}$ de corpos é separável se todos os elementos de $\mathbb{F}$ são separáveis sobre $\mathbb{K}$, isto é se todo elemento x pertencente a $\mathbb{F}$ tiver como polinômio irredutível $\text{Irr}(x, \mathbb{K})$ um polinômio sem raízes múltiplas.

⁴¹Seja A uma álgebra com divisão de centro $\mathbb{K}$. Dizemos que um subcorpo $\mathbb{F}$ de A é um *subcorpo maximal* se não está contido em nenhum subcorpo maior de A . Observemos que, neste caso, necessariamente $\mathbb{F}$ contém $\mathbb{K}$, pois caso contrário $\mathbb{F}$ estaria contido propriamente em $\mathbb{K}(\mathbb{F})$, que é o corpo obtido pela adjunção dos elementos de $\mathbb{F}$ a $\mathbb{K}$.

⁴² $C_A(\mathbb{F}) = \{a \in A / ax = xa, \forall a \in A\}$ é chamado *centralizador* de $\mathbb{F}$ em A .

Teorema: Seja A uma álgebra com divisão de centro $\mathbb{K}$ e seja $\mathbb{F}$ um subcorpo maximal de A . Então

$$[A : \mathbb{K}] = ([\mathbb{F} : \mathbb{K}])^2.$$

Se $n = [\mathbb{F} : \mathbb{K}]$, então

$$A \otimes_{\mathbb{K}} \mathbb{F} \cong M_n(\mathbb{F}),$$

onde $M_n(\mathbb{F})$ é o conjunto das matrizes $n \times n$ com entradas em $\mathbb{F}$.

O próximo resultado dá-nos a existência de subcorpos maximais separáveis.

Teorema: Seja A uma álgebra com divisão de centro $\mathbb{K}$. Então A possui um subcorpo maximal separável sobre $\mathbb{K}$.

Considere, agora, que $\mathbb{L} \supset \mathbb{K}$ é uma extensão de corpos e seja $G(\mathbb{L}|\mathbb{K})$ o grupo dos automorfismos de $\mathbb{L}$ sobre $\mathbb{K}$. Dizemos que $\mathbb{L}$ é uma *extensão galoisiana* de $\mathbb{K}$ se $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e o corpo fixo de $G(\mathbb{L}|\mathbb{K})$ é $\mathbb{K}$. Assim, $\mathbb{L}$ é uma extensão galoisiana de $\mathbb{K}$ se, e só se, $\mathbb{L}$ é uma extensão normal e separável de $\mathbb{K}$. Temos, então, o seguinte

Teorema: Se A é uma álgebra com divisão de centro $\mathbb{K}$, então A admite um corpo de decomposição que é uma extensão galoisiana de $\mathbb{K}$ (porém, não necessariamente contida em A).

Suponha que A é uma álgebra simples central sobre $\mathbb{K}$, contendo como subcorpo maximal uma extensão galoisiana $\mathbb{L}$ sobre $\mathbb{K}$. Seja $G = G(\mathbb{L}|\mathbb{K})$ o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$. Fixemos $\dim_{\mathbb{K}} \mathbb{L} = n$, de modo que $\dim_{\mathbb{K}} A = n^2$ e a ordem de G é n . Seja $\sigma \in G$. Pelo teorema de Skolem-Noether, existe $a_{\sigma} \in A$ inversível tal que $a_{\sigma} x a_{\sigma}^{-1} = \sigma(x)$, para todo $x \in \mathbb{L}$. Ou seja, $a_{\sigma} x = \sigma(x) a_{\sigma}$, para todo $x \in \mathbb{L}$. Isto implica no fato que a_{σ} está determinado, a menos de multiplicação por elementos de $\mathbb{L}^*$.

Seja, agora, $\tau \in G$. Então

$$\sigma\tau(x) = a_{\sigma\tau} x a_{\sigma\tau}^{-1}. \quad (5.11)$$

Por outro lado,

$$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(a_{\tau} x a_{\tau}^{-1}) = a_{\sigma} a_{\tau} x a_{\tau}^{-1} a_{\sigma}^{-1}. \quad (5.12)$$

De (5.11) e (5.12), temos

$$a_{\sigma\tau} x a_{\sigma\tau}^{-1} = a_{\sigma} a_{\tau} x a_{\tau}^{-1} a_{\sigma}^{-1} = a_{\sigma} a_{\tau} x (a_{\sigma} a_{\tau})^{-1}.$$

Daí, concluímos que existe $\gamma_{\sigma,\tau} \in \mathbb{L}^*$ tal que

$$a_\sigma a_\tau = \gamma(\sigma, \tau) a_{\sigma\tau}.$$

Ou seja, existe $\gamma : G \times G \rightarrow \mathbb{L}^*$ tal que

$$a_\sigma a_\tau = \gamma(\sigma, \tau) a_{\sigma\tau}. \quad (5.13)$$

Se $\theta \in G$, de (5.13) segue que

$$\begin{aligned} a_\sigma a_\tau a_\theta &= a_\sigma (a_\tau a_\theta) = a_\sigma (\gamma(\tau, \theta) a_{\tau\theta}) = a_\sigma \gamma(\tau, \theta) a_\sigma^{-1} a_\sigma (a_{\tau\theta}) = \\ &= \sigma(\gamma(\tau, \theta)) a_\sigma a_{\tau\theta} = \sigma(\gamma(\tau, \theta)) \gamma(\sigma, \tau\theta) a_{\sigma\tau\theta}. \end{aligned}$$

Por outro lado,

$$a_\sigma a_\tau a_\theta = (a_\sigma a_\tau) a_\theta = \gamma(\sigma, \tau) a_{\sigma\tau} a_\theta = \gamma(\sigma, \tau) \gamma(\sigma\tau, \theta) a_{\sigma\tau\theta}.$$

Daí,

$$\gamma(\sigma, \tau) \gamma(\sigma\tau, \theta) = \sigma(\gamma(\tau, \theta)) \gamma(\sigma, \tau\theta).$$

Dizemos que toda γ que verifica a relação acima é um *2-cociclo* de G .

Obtemos, então, que todo elemento $a \in A$ pode ser escrito na forma

$$a = \sum_{\sigma \in G} x_\sigma a_\sigma, \quad x_\sigma \in \mathbb{L}, \quad (5.14)$$

onde

1. $a_\sigma y_\tau = \sigma(y_\tau) a_\sigma$;
2. $a_\sigma a_\tau = \gamma(\sigma, \tau) a_{\sigma\tau}$.

Isto implica em

$$(x_\sigma a_\sigma)(y_\tau a_\tau) = x_\sigma \sigma(y_\tau) \gamma(\sigma, \tau) a_{\sigma\tau}.$$

Observando que o conjunto $\{a_\sigma / \sigma \in G\}$ é linearmente independente sobre $\mathbb{L}$ e de (5.14), obtemos que é uma base de A sobre $\mathbb{L}$. Neste caso, dizemos que A é o *produto cruzado* de $\mathbb{L}$ e G em relação a γ .

É fácil ver que as álgebras de Dickson são um caso especial de produto cruzado quando o grupo de Galois é cíclico⁴³.

⁴³Este resultado foi provado, em 1921, por Wedderburn ([WE5]).

Em 1926, no artigo *New Division Algebras* ([240]), Dickson faz explicitamente esta construção para grupos abelianos que são produto direto de dois grupos cíclicos. Depois, estende o resultado para grupos abelianos finitos e, em seguida, para grupos solúveis finitos. Dickson reconhece a importância deste trabalho ao afirmar, na introdução, que estes estudos resultarão em algumas teses da Universidade de Chicago:

“Further developments of the paper will be given in Chicago theses.”

Restava ainda responder à pergunta se toda álgebra com divisão é uma álgebra cíclica sobre seu centro. Esta dúvida foi sanada por Albert em 1967, quando construiu, em [AL18], um produto cruzado não cíclico. Entretanto, permaneceu sem resposta, até 1972, a pergunta “toda álgebra com divisão central é um produto cruzado?”. Nessa data, Amitsur apresentou um contra-exemplo, em [AM1]: provou que para todo inteiro n que é divisível por um primo ímpar ou por 8, existe uma álgebra com divisão de dimensão n^2 sobre o seu centro, que não é um produto cruzado. Mais explicitamente, Amitsur considerou a álgebra com divisão genérica de dimensão n^2 , $\mathbb{Q}(X_1, \dots, X_m)$, gerada por $m \geq 2$ matrizes genéricas $n \times n$ (isto é, matrizes cujos coeficientes são indeterminadas comutativas sobre os racionais $\mathbb{Q}$).

Nos trabalhos seguintes, Dickson passa a considerar álgebras com divisão normais (ou seja, centrais). Em *New Division Algebras* ([257]), de 1928, ele descreve uma álgebra A normal com divisão de dimensão $4p^2$, com p primo, sobre um corpo $\mathbb{F}$ qualquer. Para isto, considera uma hipótese inicial e, a partir daí, conclui algumas propriedades desta álgebra.

Hipótese 1: Suponha que A contém um elemento i_1 satisfazendo uma equação $f(\omega^2) = 0$ de grau $2p$ com apenas potências pares de ω , cujos coeficientes estão em $\mathbb{F}$ e o de ω^{2p} é a unidade, e que é irredutível em $\mathbb{F}$, tal que os polinômios em i_1 são os únicos elementos de A que comutam com todo elemento de A .

Na linguagem atual, a hipótese 1 supõe que existe um elemento $i_1 \in A$ que é raiz de um polinômio da forma

$$f = \omega^{2p} + a_{p-1}\omega^{2(p-1)} + \dots + a_1\omega^2 + a_0$$

irredutível em $\mathbb{F}[\omega]$, tal que $Z(A) = \mathbb{F}(i_1)$.

Supondo que existe $i_2 \in A$ tal que i_2 comuta com i_1^2 , mas não comuta com i_1 , Dickson mostra que o conjunto

$$1, i_1, \dots, i_1^{2p-1}, i_2, i_1 i_2, i_1^2 i_2, \dots, i_1^{2p-1} i_2$$

é linearmente independente em $\mathbb{F}$.

Considerando S como sendo a subálgebra de A gerada por i_1 e i_2 , prova que S é uma álgebra normal sobre $\mathbb{F}(i_1^2)$ de dimensão 4 no

Lema 1: Seja i_2 um elemento de A que comuta com $I = i_1^2$, mas não com i_1 . A álgebra S gerada por i_1 e i_2 é de ordem $4p$. Ela pode ser considerada como uma álgebra de ordem 4 com a base $1, i_1, i_2, i_1 i_2$ sobre $\mathbb{F}(I)$; esta álgebra é normal. Em outras palavras, os polinômios em I são os únicos elementos de S que comutam com todo elemento de S .

Daí, conclui que as dimensões de S sobre $\mathbb{F}(i_1)$ e de $\mathbb{F}(i_1)$ sobre $\mathbb{F}(i_1^2)$ sobre $\mathbb{F}$ são 2; e as dimensões de $\mathbb{F}(i_1^2)$ sobre $\mathbb{F}$ e de A sobre S são p .

Esquemáticamente, tem-se

$$\begin{array}{c}
 p \left[\begin{array}{c} A \\ | \\ S \end{array} \right. \\
 2 \left[\begin{array}{c} | \\ Z(A) = \mathbb{F}(i_1) \\ | \\ \mathbb{F}(i_1^2) = Z(S) \\ | \\ \mathbb{F} \end{array} \right. \left. \right] 2 \\
 \left. \right] p
 \end{array}$$

Em seguida, Dickson considera a

Hipótese 2: Suponha que A contém elementos i_1 e z tais que i_1 satisfaz a hipótese 1 e os elementos

$$i_2 = z i_1 z^{-1}, \quad i_3 = z i_2 z^{-1}, \quad \dots, \quad i_p = z i_{p-1} z^{-1} \quad (5.15)$$

comutam com $I = i_1^2$, enquanto que i_2 não comuta com i_1 e nem com $i_2^2 \neq I$.

Ou seja, além da hipótese 1, supõe que existe $z \in A$ tal que todos os elementos (5.15) comutam com i_1^2 e i_2 não comuta com i_1 e $i_2^2 \neq i_1^2$. Então obtém o importante

Teorema 2: Todo elemento de A pode ser expresso de um único modo na forma

$$A_0 + A_1 z + \dots + A_{p-1} z^{p-1}, \quad (5.16)$$

onde cada A_i está em S . O produto de quaisquer duas somas (5.16) pode ser expresso como uma terceira soma dada por

$$zG = G'z, \quad z^p = s,$$

onde G , G' e s estão todos em S e são da forma

$$p(i_1) + q(i_1)i_2,$$

onde p e q são polinômios.

Este teorema mostra que o conjunto $\{1, z, z^2, \dots, z^{p-1}\}$ é base normalizante (veja definição A.4.3) de A sobre S , onde S é um anel com divisão (pois A é com divisão). Este é o primeiro exemplo de base normalizante sobre um anel com divisão que aparece na literatura.

Na seqüência, Dickson prova o

Teorema 3: S é uma álgebra de quatérnios generalizada sobre $\mathbb{F}(I)$ com base $1, i_1, y, i_1y$, onde $y = i_1i_2 - i_2i_1$.

Em resumo, neste trabalho Dickson mostra, em linguagem moderna, que toda álgebra central com divisão de dimensão $4p^2$, p primo, sobre um corpo $\mathbb{F}$ qualquer (com a restrição das hipóteses 1 e 2) é uma álgebra de quatérnios generalizada sobre seu centro, com base normalizante da forma $\{1, z, z^2, \dots, z^{p-1}\}$.

Já em 1930, no trabalho *Construction of Division Algebras* ([267]), Dickson considera uma álgebra Σ e um corpo $\mathbb{F}$ e supõe que G é o grupo de automorfismos de Σ que fixa os elementos de $\mathbb{F}$. A partir de algumas hipóteses para Σ , constrói abstratamente uma álgebra com divisão Γ . Inicialmente o faz quando o grupo G é cíclico. Em seguida, considera os casos em que G é abeliano com dois geradores e abeliano finito e faz algumas generalizações.

Na introdução deste artigo, Dickson afirma que está apresentando uma simplificação da teoria da construção das álgebras, com divisão, conhecidas e que esta simplificação é tão grande que seriam necessárias cerca de cem páginas, para obter-se os mesmos resultados usando o melhor método conhecido até o momento:

“We shall make a noteworthy simplification of the theory of the construction of a type of algebras Γ which includes all known division algebras. The simplification is so great that it would require a hundred pages to obtain our results by the best earlier method.”

Ele ainda observa que estes estudos servem de introdução para o seu trabalho anterior *New Division Algebras* ([240]), de 1926. Dickson faz esta observação porque, se considerarmos

$\Sigma = \mathbb{F}(i)$ onde i é uma raiz de um polinômio irredutível de grau p com o grupo de Galois $G(\mathbb{F}(i), \mathbb{F})$ cíclico, recaímos no caso considerado em [240].

O que é importante ressaltar em relação aos estudos desenvolvidos em [240], [257] e [267] é que eles contêm a gênese do produto cruzado, que se tornou uma ferramenta bastante útil para a simplificação na teoria de álgebras e representações.

Conclusão

A importância do trabalho de Leonard Eugene Dickson, na teoria de álgebras em geral e, em particular, na teoria de álgebras com divisão, é universalmente reconhecida. Por exemplo, M. Kline, em *Mathematical Thought from Ancient to Modern Times* ([KL]), hoje o texto mais importante sobre história da matemática, afirma:

*“Cayley não provou que a divisão, à esquerda e à direita, por elementos diferentes de zero, sempre é possível, e única, nos octônios. Isto foi mostrado por Dickson, em 1912 ([173]).”*⁴⁴

e

*“O estudo de álgebras lineares com um número finito, ou talvez infinito, de unidades geradoras (primárias), e com ou sem divisão, continuaram a ser um assunto ativo no século vinte. Homens, tais como L. E. Dickson e J. H. M. Wedderburn, contribuíram muito para o assunto.”*⁴⁵

Ainda:

*“J. H. M. Wedderburn (1882-1948), um professor da Universidade de Princeton, e Dickson provaram, simultaneamente, que todo corpo finito é, necessariamente, comutativo.”*⁴⁶

e

*“Até 1905, as únicas álgebras com divisão conhecidas eram os corpos comutativos e os quatérnios. Então, Dickson criou algumas novas, comutativas e não comutativas.”*⁴⁷

⁴⁴Página 792.

⁴⁵Página 794.

⁴⁶Página 1150.

⁴⁷Página 1151.

Quando iniciamos nossas pesquisas, pretendíamos entender a gênese das idéias que permitiram Dickson construir várias famílias de exemplos.

Para nossa surpresa, descobrimos que ele havia realizado muito mais: contribuiu para a formulação de alguns dos conceitos mais fundamentais da teoria de álgebras com divisão, onde destacamos, além da construção das álgebras cíclicas, das álgebras de Cayley-Dickson e dos quatérnios generalizados, o estudo da aritmética não comutativa, o fato de ter explicitado a noção de ordens maximais e o desenvolvimento de idéias fundamentais subjacentes à teoria de produto cruzado.

Com este trabalho, esperamos ter contribuído para que Dickson ocupe o seu verdadeiro lugar na história da matemática como precursor de grandes idéias que resultaram em importantes teoremas usados até os dias de hoje e também como um dos que contribuíram decisivamente para a formação da comunidade algebrista americana.

Apêndice A

Um Pouco de Matemática

A.1 Definições

Definição A.1.1 Dizemos que um conjunto $\mathbb{F}$ munido das operações de adição (denotada por $+$) e multiplicação (denotada por $*$) é um corpo se verifica os seguintes axiomas:

1. (Associatividade da Adição) Para quaisquer $x, y, z \in \mathbb{F}$, tem-se

$$(x + y) + z = x + (y + z);$$

2. (Existência do Elemento Neutro da Adição) Existe $0 \in \mathbb{F}$ tal que

$$x + 0 = x = 0 + x,$$

para todo $x \in \mathbb{F}$;

3. (Existência do Elemento Oposto da Adição) Para todo elemento $x \in \mathbb{F}$ existe um elemento $x' \in \mathbb{F}$ tal que

$$x + x' = e = x' + x;$$

4. (Comutatividade da Adição) Para quaisquer $x, y \in \mathbb{F}$,

$$x + y = y + x;$$

5. (Associatividade da Multiplicação) Para quaisquer $x, y, z \in \mathbb{F}$, tem-se

$$(x * y) * z = x * (y * z);$$

6. (Existência do Elemento Neutro da Multiplicação) Existe $1 \in \mathbb{F}$ tal que

$$x * 1 = x = 1 * x,$$

para todo $x \in \mathbb{F}$;

7. (Existência do Inverso da Multiplicação) Para todo elemento não nulo $x \in \mathbb{F}$ existe um elemento $x^{-1} \in \mathbb{F}$ tal que

$$x * x^{-1} = 1 = x^{-1} * x;$$

8. (Comutatividade da Multiplicação) Para quaisquer $x, y \in \mathbb{F}$,

$$x * y = y * x;$$

9. (Propriedade Distributiva) Para quaisquer $x, y, z \in \mathbb{F}$,

$$x * (y + z) = (x * y) + (x * z).$$

A.2 Álgebra Linear Associativa

Definição A.2.1 Considere o conjunto de todas n -uplas $(x_1, \dots, x_n)$, onde $x_i \in \mathbb{F}$, com $\mathbb{F}$ qualquer. Dizemos que a n -upla $(x_1, \dots, x_n)$ é igual a n -upla $(y_1, \dots, y_n)$ se $x_1 = y_1, \dots, x_n = y_n$ e definimos adição e subtração destas n -uplas por:

$$(x_1, \dots, x_n) \pm (y_1, \dots, y_n) = (x_1 \pm y_1, \dots, x_n \pm y_n).$$

O produto de $x = (x_1, \dots, x_n)$ por qualquer constante $\alpha \in \mathbb{F}$ é definido por:

$$\alpha x = x \alpha = (\alpha x_1, \dots, \alpha x_n).$$

As n unidades deste conjunto são definidas por:

$$e_1 = (1, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1).$$

e mostra-se que são independentes em relação ao corpo $\mathbb{F}$. Desta forma, a n -upla x acima pode ser expressa na forma

$$x = x_1 e_1 + x_2 e_2 + \dots + x_n e_n.$$

Um elemento x como acima era chamado *número hipercomplexo* ou, às vezes, *número complexo*.

Assim, se $x = \sum_{i=1}^n x_i e_i$ e $y = \sum_{j=1}^n y_j e_j$, temos

$$x \pm y = \sum_{k=1}^n (x_k \pm y_k) e_k \quad (\text{A.1})$$

e $\alpha x = x\alpha = \sum_{i=1}^n (\alpha x_i) e_i$.

Assuma que quaisquer dois números complexos x e y podem ser multiplicados, de modo que valha a distributividade, do seguinte modo:

$$xy = \sum_{i,j=1}^n x_i y_j e_i e_j, \quad (\text{A.2})$$

tal que o produto xy é um número complexo $\sum z_i e_i$ com coordenadas em $\mathbb{F}$ e

$$e_i e_j = \sum_{k=1}^n \gamma_{ijk} e_k, \quad (\text{A.3})$$

com $i, j = 1, \dots, n$ e $\gamma_{ijk} \in \mathbb{F}$.

Dizia-se, então, que o conjunto de todos os números hipercomplexos $\sum x_i e_i$ com coordenadas no corpo $\mathbb{F}$, munido da adição (e subtração) definida em (A.1) e da multiplicação definida em (A.2), forma uma *álgebra linear* (sistema de números hipercomplexos ou sistema de números complexos) sobre o corpo $\mathbb{F}$, com unidades $e_1, \dots, e_n$ (linearmente independentes em relação a $\mathbb{F}$) e tábua de multiplicação definida por (A.3).

Observe que a associatividade ou a comutatividade não são assumidas.

A.3 Grupos

Definição A.3.1 Dizemos que uma operação $\circ$ sobre um conjunto G define uma estrutura de grupo sobre G se, e só se, verifica os seguintes axiomas:

1. (Propriedade Associativa) Para quaisquer $x, y, z \in G$, temos

$$(x \circ y) \circ z = x \circ (y \circ z);$$

2. (Existência do Elemento Neutro) Existe $e \in G$ tal que

$$x \circ e = x = e \circ x$$

para todo $x \in G$;

3. (Existência do Elemento Inverso) Para todo $x \in G$, existe $x' \in G$ tal que

$$x \circ x' = e = x' \circ x.$$

Se a operação $\circ$ satisfaz

1. (Propriedade Comutativa) Para quaisquer $x, y \in G$, vale

$$x \circ y = y \circ x,$$

então diremos que G é um *grupo comutativo* ou *abeliano*.

A.4 Álgebras

Neste ponto, é conveniente introduzir o conceito de álgebra (associativa) sobre um corpo arbitrário. Vamos restringir-nos às álgebras de dimensão finita, pois estas são o objeto de estudo deste trabalho.

Definição A.4.1 Seja $\mathbb{F}$ um corpo. Uma álgebra associativa sobre $\mathbb{F}$ (ou $\mathbb{F}$ -álgebra ou simplesmente álgebra) é um espaço vetorial A de dimensão finita sobre $\mathbb{F}$ no qual está definida uma multiplicação

$$(a, b) \mapsto ab$$

satisfazendo às seguintes condições:

1. $(ab)c = a(bc)$
2. $a(b+c) = ab+ac$ e $(b+c)a = ba+ca$
3. $\alpha(ab) = (\alpha a)b = a(\alpha b)$

quaisquer que sejam $a, b, c \in A$ e $\alpha \in \mathbb{F}$.

Logo, uma álgebra A de dimensão n sobre um corpo $\mathbb{F}$ consiste de todas as combinações lineares

$$a = \sum_{i=1}^n \alpha_i \epsilon_i$$

de n elementos básicos (unidades) $\epsilon_1, \dots, \epsilon_n$ com coeficientes $\alpha_i \in \mathbb{F}$.

Como exemplo de álgebra, temos o conjunto dos números complexos, que formam uma álgebra bidimensional sobre o corpo dos números reais. Outro exemplo é o conjunto das matrizes $n \times n$ sobre um corpo $\mathbb{F}$, que forma uma álgebra de dimensão n^2 sobre $\mathbb{F}$.

Tipos especiais de álgebras são obtidos quando impomos certas restrições na estrutura da multiplicação. Assim, uma álgebra A se diz *comutativa* se $ab = ba$ para quaisquer $a, b \in A$. Dizemos que A é uma *álgebra com unidade*, se existe $1 \in A$ tal que $1 \neq 0$ e $1a = a1 = a$ para todo $a \in A$. Se existe tal elemento, ele é único e é chamado *unidade* de A . Já um elemento $a \in A$ se diz *invertível* se existe $a' \in A$ tal que $aa' = a'a = 1$. Neste caso, a' é único e será chamado de *inverso* de a (e denotado por a^{-1}). Dizemos, então, que A é uma *álgebra com divisão*, se todo elemento não nulo de A é invertível (os corpos são exemplos de álgebras com divisão).

Como mencionamos ao longo dos nossos estudos, Frobenius determinou todas as álgebras com divisão sobre os reais em

Teorema de Frobenius: *As únicas álgebras com divisão sobre os reais são o corpo dos números reais, o corpo dos números complexos e a álgebra dos quatérnios reais.*

Na seqüência, consideramos os subsistemas, que são definidos respeitando-se as estruturas em questão. Então temos:

Definição A.4.2 Dizemos que um subconjunto B é uma subálgebra da álgebra A sobre $\mathbb{F}$ se B é um subespaço vetorial de A , que é fechado em relação à multiplicação (isto é, se $a, b \in B$, então $ab \in B$).

Por exemplo, o corpo $\mathbb{C}$ dos números complexos quando considerado como uma $\mathbb{R}$ -álgebra possui apenas duas subálgebras não nulas: $\mathbb{R}$ e o próprio $\mathbb{C}$.

Considere agora uma álgebra qualquer A e seja Z o conjunto que consiste de todos os elementos de $z \in A$ que satisfazem $az = za$ para todo $a \in A$. Verifica-se, facilmente, que Z é uma subálgebra. Seus elementos são chamados de *centrais* em A e Z é chamado de *centro* de A . Claramente A é comutativa se $A = Z$. É fácil ver que o centro da álgebra dos quatérnios reais é precisamente $\mathbb{R}$.

Continuando com algumas definições, considere duas álgebras A e A' sobre o mesmo corpo $\mathbb{F}$. Uma aplicação

$$\varphi : A \rightarrow A'$$

é chamada um *homomorfismo* se preserva tanto a estrutura de espaço vetorial, quanto a estrutura multiplicativa de A ; ou seja,

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(\alpha a) = \alpha \varphi(a), \quad \varphi(ab) = \varphi(a)\varphi(b),$$

quaisquer que sejam $a, b \in A$ e $\alpha \in \mathbb{F}$. Dizemos que φ é um *isomorfismo*, se é um homomorfismo bijetivo e que é um *automorfismo* se é um isomorfismo e $A = A'$.

Considere uma álgebra A com unidade e suponha que B é uma subálgebra de A com a mesma unidade. Temos, então, a seguinte

Definição A.4.3 Dizemos que o conjunto $\{1 = x_1, \dots, x_n\}$ é uma *base normalizante* de B sobre A se

1. Todo elemento b de B pode ser escrito de modo único como

$$b = \beta_1 x_1 + \dots + \beta_n x_n,$$

com $\beta_i \in A$.

2. Existem automorfismos $\sigma_1, \dots, \sigma_n$ de A tais que $x_i \beta = \sigma_i(\beta) x_i$ para todo $\beta \in A$. Do fato que $\sigma_1 = 1$, temos que σ_1 é o automorfismo identidade.

Suponha, agora, que B é um subespaço vetorial da álgebra A que é invariante à esquerda em relação à multiplicação por elementos de A (ou seja $ab \in B$ para todo $a \in A$ e $b \in B$). Então B se diz um *ideal à esquerda* de A . De modo análogo, define-se *ideal à direita* de A . Por exemplo, se A é uma álgebra qualquer e $a \in A$, os múltiplos à esquerda e à direita de a ,

$$Aa = \{xa / x \in A\} \quad \text{e} \quad aA = \{ax / x \in A\},$$

são, respectivamente, ideais à esquerda e à direita de A . Um subconjunto B de A se diz *ideal bilateral* ou simplesmente *ideal* de A , se é, simultaneamente, um ideal à esquerda e à direita. Assim como somamos elementos de uma álgebra, também podemos somar seus ideais, de maneira que todo elemento da álgebra seja escrito de modo único, como soma de elementos destes ideais:

Definição A.4.4 Seja $\{J_i\}_{i \in I}$ uma família de ideais de uma álgebra A . Dizemos que A é uma *soma direta* desta família de ideais se

1. $A = \sum_{i \in I} J_i$
2. $J_i \cap (\sum_{h \neq i} J_h) = (0)$, para todo $i \in I$.

Seja $a \in A$. Indicamos o produto aa por a^2 ; aaa por a^3 e assim por diante. Dizemos, então, que a é *nilpotente* se $a^m = 0$ para algum inteiro positivo m . Se B e C são ideais de A , indicamos por BC o conjunto de todas as somas finitas

$$b_1 c_1 + \dots + b_r c_r, \quad b_i \in B, \quad c_i \in C, \quad r \geq 1.$$

É imediato que BC é um ideal de A . Então definimos as potências de B indutivamente por

$$B^n = B^{n-1}B,$$

onde $B^1 = B$. Assim B^n consiste de todas as somas finitas

$$\sum_{i=1}^r b_{i_1} b_{i_2} \cdots b_{i_n}, \quad b_{i_j} \in B \text{ e } r \geq 1.$$

Definição A.4.5 Dizemos que B é *nilpotente*, se alguma potência de B é zero. Neste caso, o menor inteiro m tal que $B^m = 0$ é chamado de *índice de nilpotência* de B .

Por exemplo, seja $A = (\epsilon_1, \epsilon_2)$ uma álgebra bidimensional sobre um corpo $\mathbb{F}$ com a seguinte tabela de multiplicação

$$\epsilon_1^2 = \epsilon_2, \quad \epsilon_1 \epsilon_2 = \epsilon_2 \epsilon_1 = \epsilon_2^2 = 0.$$

Então A é uma álgebra nilpotente com índice de nilpotência 3.

A.5 Teoremas de Estrutura

Definição A.5.1 Dizemos que uma álgebra finita A é *semi-simples*, se o único ideal nilpotente de A é o ideal (0) .

Definição A.5.2 Dizemos que uma álgebra A é *simples* se $A^2 \neq 0$ e os únicos ideais de A são os triviais (ou seja, (0) e o próprio A).

Seja A uma álgebra com divisão. Pode-se demonstrar, então, que a álgebra $M_n(A)$ das matrizes $n \times n$ com coeficientes em A é uma álgebra simples.

Estamos, agora, em condições de enunciar o teorema de Wedderburn:

Teorema A.5.1 1. Toda álgebra semi-simples, de dimensão finita, é uma soma direta de álgebras simples.

2. Toda álgebra simples, de dimensão finita, é isomorfa a uma álgebra de matrizes $M_n(D)$, onde D é um anel com divisão. Além disso, se $M_n(D) \cong M_{n'}(D')$, então $n = n'$ e $D \cong D'$.

Definição A.5.3 Dizemos que um elemento $e \neq 0$ de uma álgebra é *idempotente* se $e^2 = e$. Se e_i, e_j são elementos idempotentes de uma álgebra, dizemos que eles são *ortogonais* se $e_i e_j = 0$.

Os elementos idempotentes têm um papel fundamental na teoria de álgebras. Em particular, destacamos o seguinte

Teorema A.5.2 *Seja A uma álgebra semi-simples. Então existe uma família de elementos $e_1, \dots, e_s \in A$ tais que:*

1. $e_i^2 = e_i$, $1 \leq i \leq s$;
2. $e_i e_j = 0$, se $i \neq j$;
3. $1 = e_1 + \dots + e_s$;
4. e_i é central, $1 \leq i \leq s$;
5. Se $e_i = e'_i + e''_i$, com e'_i, e''_i idempotentes ortogonais centrais, então $e'_i = 0$ ou $e''_i = 0$.

A.6 Exemplos de Álgebras

A.6.1 Os Quatérnios Reais

Seja $\mathbb{H}$ o $\mathbb{R}$ -espaço vetorial de dimensão quatro, cujos elementos da base são $1, i, j, k$; ou seja

$$\mathbb{H} = \{x_0 + x_1 i + x_2 j + x_3 k \mid x_0, x_1, x_2, x_3 \in \mathbb{R}\}.$$

Defina a soma de dois elementos de $\mathbb{H}$ por

$$(x_0 + x_1 i + x_2 j + x_3 k) + (y_0 + y_1 i + y_2 j + y_3 k) = (x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k.$$

A multiplicação é definida distributivamente por

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik. \end{cases}$$

É fácil verificar que vale a associatividade da multiplicação em $\mathbb{H}$.

O $\mathbb{R}$ -espaço vetorial $\mathbb{H}$, munido desta multiplicação, é uma álgebra e é chamada de *quatérnios reais*. Dentre as propriedades dos quatérnios reais, temos que todo elemento não nulo de $\mathbb{H}$ é inversível. Portanto, $\mathbb{H}$ é uma $\mathbb{R}$ -álgebra com divisão.

A.6.2 Quatérnios Sobre um Corpo $\mathbb{F}$ Qualquer

Considere o $\mathbb{F}$ -espaço vetorial

$$\mathbb{H}(\mathbb{F}) = \mathbb{F} \oplus \mathbb{F}i \oplus \mathbb{F}j \oplus \mathbb{F}k$$

e defina distributivamente a multiplicação em $\mathbb{H}(\mathbb{F})$ por

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik. \end{cases}$$

O $\mathbb{F}$ -espaço vetorial $\mathbb{H}(\mathbb{F})$, munido desta multiplicação (que se mostra facilmente associativa), é uma álgebra e é chamada *quatérnios sobre o corpo $\mathbb{F}$* . Dentre suas propriedades, destacamos que $\mathbb{H}(\mathbb{F})$ tem divisores do zero se, e só se, a equação $x^2 + y^2 = -1$ tem solução em $\mathbb{F}$. Daí, obtemos o seguinte

Teorema A.6.1 *São equivalentes:*

1. $\mathbb{H}(\mathbb{F})$ não tem divisores do zero;
2. A equação $x^2 + y^2 = -1$ não possui solução em $\mathbb{F}$;
3. $\mathbb{H}(\mathbb{F})$ é uma álgebra com divisão.

Observemos: quando $\mathbb{F} = \mathbb{R}$, obtemos a álgebra dos quatérnios.

A.6.3 Quatérnios Generalizados

Seja $\mathbb{F}$ um corpo com $\text{car}(\mathbb{F}) \neq 2$ e sejam $a, b \in \mathbb{F}$, com $a, b \neq 0$. Considere o $\mathbb{F}$ -espaço vetorial A de dimensão quatro, cujos elementos da base são $1, i, j, k$. Defina distributivamente a multiplicação por

$$\begin{cases} i^2 = a \\ j^2 = b \\ ij = -ji = k. \end{cases}$$

Como vale a associatividade, obtém-se

$$\begin{cases} k^2 = -ab \\ ik = -ki = aj \\ jk = -kj = -bi. \end{cases}$$

A $\mathbb{F}$ -álgebra A é chamada *quatérnios generalizados* e é denotada por $A = \left(\frac{a, b}{\mathbb{F}} \right)$.

Para cada $x = x_0 + x_1i + x_2j + x_3k \in A$ defina o conjugado de x por $\bar{x} = x_0 - x_1i - x_2j - x_3k$ e a norma de x por $N(x) = x\bar{x}$. Então temos o

Teorema A.6.2 *São equivalentes:*

1. A é uma álgebra com divisão;
2. Se $x \in A - \{0\}$, então $N(x) \neq 0$;
3. Se $c_0, c_1, c_2 \in \mathbb{F}$ satisfazem $c_0^2 = ac_1^2 + bc_2^2$, então $c_0 = c_1 = c_2 = 0$.

Observemos: quando $\mathbb{F} = \mathbb{R}$ e $a = b = -1$ temos que A é a álgebra dos quatérnios reais, ou seja, $\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}} \right)$.

A.6.4 Álgebras Cíclicas

Seja $\mathbb{F}$ um corpo e considere um polinômio f de grau n com coeficientes em $\mathbb{F}$ (ou seja, $f \in \mathbb{F}[x]$) irredutível. Suponha que as raízes de f podem ser representadas por:

$$a, \theta(a), \theta^2(a) = \theta[\theta(a)], \dots, \theta^{n-1}(a),$$

onde $\theta(x) \in \mathbb{F}[x]$ e $\theta^n(a) = a$, onde a não está em $\mathbb{F}$. Neste caso, dizemos que $f(x)$ é uma equação cíclica sobre $\mathbb{F}$. Por exemplo, $x^2 + 1 = 0$ é uma equação cíclica sobre $\mathbb{R}$, pois i é uma raiz e $\theta(x) = -x$.

Seja $x^n - \delta \in \mathbb{F}[x]$ irredutível e seja b em uma extensão de $\mathbb{F}$ uma de suas raízes. Então $b^n = \delta$. Considere, agora, os elementos da forma:

$$b^i a^j, \quad \text{com } 1 \leq i, j \leq n.$$

Defina a multiplicação distributiva e associativamente entre a e b por:

$$ab = b\theta(a).$$

Deste modo, obtemos

$$a^j b = b[\theta(a)]^j$$

e

$$ab^h = b^h \theta^h(a).$$

Daí,

$$a^j b^h = b^h [\theta^h(a)]^j,$$

o que nos permite definir a multiplicação de dois elementos $b^i a^j$ e $b^h a^k$ por:

$$(b^i a^j)(b^h a^k) = b^{i+h} [\theta^h(a)]^j a^k. \quad (\text{A.4})$$

Através de cálculos simples, mostra-se que este produto é associativo.

Considere o conjunto:

$$D = \left\{ \sum k_{ij} b^i a^j / k_{ij} \in \mathbb{F} \right\}$$

munido da multiplicação definida em (A.4). É fácil verificar que D , com esta multiplicação, é uma álgebra de dimensão n^2 sobre $\mathbb{F}$ e dizemos que D é uma *álgebra cíclica*.

Como vimos em 5.3, Dickson provou o seguinte

Teorema A.6.3 *Se δ não é a norma de nenhum elemento de $\mathbb{F}(a)$, então D é uma álgebra com divisão.*

A.6.5 Álgebras Cíclicas de Dimensão Quatro

Seja $\mathbb{F}$ um corpo tal que $\text{car}(\mathbb{F}) \neq 2$ e considere o polinômio $f(x) = x^2 + 2\alpha x + \beta$ irreduzível sobre $\mathbb{F}$. Seja a uma raiz de f . Neste caso, substituindo a por $\alpha + a$ se necessário¹, podemos supor que a é uma raiz de um polinômio $x^2 + \gamma$, onde γ não é um quadrado em $\mathbb{F}$. Deste modo, $\theta(a) = -a$ é raiz de f .

Considere, agora, o polinômio $x^2 - \delta$ irreduzível sobre $\mathbb{F}$, onde δ não é norma de nenhum elemento de $\mathbb{F}(a)$, e seja b raiz de $x^2 - \delta = 0$. Então:

$$D = \left\{ \sum k_{ij} b^i a^j / k_{ij} \in \mathbb{F} \right\}$$

munido do produto (A.4) é uma álgebra de dimensão quatro e tem base $\{1, i, j, k\}$. De $\theta(a) = -a$, temos que $ab = b\theta(a) = -ba$. Logo, $D = \left(\frac{\gamma, \delta}{\mathbb{F}} \right)$, ou seja, D é a álgebra dos quatérnios generalizados.

¹Do fato que a é raiz de f , obtemos que $a^2 + 2\alpha a + \beta = 0 = (a^2 + 2\alpha a + \alpha^2) + (\beta - \alpha^2)$. Daí, $(a + \alpha)^2 + (\beta - \alpha)^2 = 0$ e, portanto, $(a + \alpha)$ é raiz de $x^2 + (\beta - \alpha)^2 = 0$.

A.6.6 Álgebras de Cayley-Dickson

Seja A uma álgebra com involução de dimensão n sobre um corpo $\mathbb{F}$ e seja l um símbolo. Se $a, b, c, d \in A$, defina:

$$(a + bl)(c + dl) = (ac + \alpha \bar{d}b) + (da + b\bar{c})l, \quad (\text{A.5})$$

onde $\alpha \in A$, $l^2 = \alpha$ e $\bar{x}$ representa o conjugado de x . Então, $A + Al$, munida da multiplicação definida em (A.5), é uma álgebra e é chamada de *álgebra de Cayley-Dickson*.

Por exemplo, considere a álgebra $\mathbb{H}$ dos quatérnios reais e o símbolo e , onde $e^2 = -1$. Então a, álgebra definida por $\mathbb{H} + \mathbb{H}e$ é uma álgebra de Cayley-Dickson de dimensão oito e, como já vimos em 5.2, representa os octônios.

Dentre as propriedades destas álgebras, destacamos o seguinte:

Teorema A.6.4 *Seja A uma álgebra e considere a álgebra de Cayley-Dickson $A + Al$, definida acima. Então, A é comutativa se, e só se, $A + Al$ é associativa.*

Apêndice B

Obras de Dickson

- [1] *On the Number of Inscriptible Regular Polygons*, NYMS Bull., v. 3, (1894), pp. 123-125.
- [2] *Lowest Integers Representing Sides of a Right Triangle*, AMM, v. 1, (1894), pp. 6-11.
- [3] *The Simplest Model for Illustrating the Conic Sections*, AMM, v. 1, (1894), pp. 261.
- [4] *The Inscription of Regular Polygons*, AMM, v. 1, (1894), pp. 299-301, 342-345, 376-377, 423-425; v. 2, pp. 7-9, 38-40.
- [5] *Some Fallacies of an Angle Trisector*, AMM, v. 2 (1895), pp. 71-72.
- [6] *A Quadratic Cremona Transformation Defined by a Conic*, AMM, v. 2, (1895), pp. 218-221.
- [7] *Gergonne's Pile Problem*, AMS Bull., v. 1, (1895), pp. 184-186.
- [8] *On the Inscription of Regular Polygons*, AM, v. 9, (1895), pp. 73-84.
- [9] *Cyclic Numbers*, QJM, v. 27, (1895), pp. 366-377.
- [10] *A Quadratic Cremona Transformation Defined by a Conic*, CMP Rend., v. 9, (1895), pp. 256-259.
- [11] *Analytic Functions Suitable to Represent Substitutions*, AJM, v. 18, (1896), pp. 210-218.
- [12] *The Analytic Representation of Substitutions on a Power of a Prime Number of Letters With a Discussion of the Linear Groups*, AM, v. 11, (1897), pp. 65-120, 162-183 (Doctoral diss.).

- [13] *System of Continuous and Discontinuous Simple Groups*, AMS Bull., v. 3, (1897), pp. 265-273.
- [14] *Higher Irreducible Congruences*, AMS Bull., v. 3, (1897), pp. 381-389.
- [15] *A Triply Infinite System of Simple Groups*, QJM, v. 29, (1897), pp. 169-178.
- [16] *Orthogonal Group in a Galois Field*, AMS Bull., v. 4, (1898), pp. 196-200.
- [17] *Systems of Simple Groups Derived from the Orthogonal Group*, AMS Bull., v. 4, (1898), pp. 382-389.
- [18] *The Structure of the Hypoabelian Groups*, AMS Bull., v. 4, (1898), pp. 495-510.
- [19] *Concerning a Linear Homogeneous Group in $C_{m,q}$ Variables Isomorphic to the General Linear Homogeneous Group in m Variables*, AMS Bull., v. 5, (1898), pp. 120-135.
- [20] *A New Solution of the Cubic Equation*, AMM, v. 5, (1898), pp. 38-39.
- [21] *The Quadratic Cremona Transformation*, Calif. Acad. Sci., Proc., s. 3, Math.-Phys., v. 1, (1898), pp. 13-23.
- [22] *The Structure of Certain Linear Groups With Quadratic Invariants*, LMS Proc., v. 30, (1898), pp. 70-98.
- [23] *The First Hypoabelian Group Generalized*, QJM, v. 30, (1898), pp. 1-16.
- [24] *Systems of Simple Groups Derived from the Orthogonal Group*, Calif. Acad. Sci., Proc., s. 3, Math.-Phys., v. 1, (1898), pp. 29-46; (1899), pp. 47-57.
- [25] *The Largest Linear Homogeneous Group with an Invariant Pfaffian*, AMS Bull., v. 5, (1899), 338-342.
- [26] *The Known Finite Simple Groups*, AMS Bull., v. 5, (1899), pp. 470-475.
- [27] *Report on the Recent Progress in Theory of Linear Groups*, AMS Bull., v. 6, (1899), pp. 13-27.
- [28] *Determination of the Structure of All Linear Homogeneous Groups in a Galois Field which are Defined by a Quadratic Invariant*, AJM, v. 21, (1899), pp. 193-256.
- [29] *A Generalization of Fermat's Theorem*, AM, s. 2, v. 1, (1899), pp. 31-36.
- [30] *The Group of Linear Homogeneous Substitutions on mq Variables which is Defined by the Invariant $\phi \equiv \sum_{i=1}^m \xi_{i_1} \xi_{i_2} \cdots \xi_{i_q}$* , LMS Proc., v. 31, (1899), pp. 200-208.

-
- [31] *Concerning the Four Known Simple Linear Groups of Order 25920, with an Introduction to the Hyperabelian Linear Groups*, LMS Poc., v. **31**, (1899), pp. 30 -68.
 - [32] *The Abstract Groups Isomorphic with the Symmetric Group on k Letters*, LMS Proc., v. **31**, (1899), pp. 351-353.
 - [33] *Simplicity of the Abelian Group on Two Pairs of Indices in the Galois Field of Order 2^n , $n > 1$* , QJM, v. **30**, (1899), pp. 383-384.
 - [34] *A Class of Linear Groups Including the Abelian Group*, QJM, v. **31**, (1899), pp. 60-66.
 - [35] *The Structure of the Linear Homogeneous Groups Defined by the Invariant $\lambda_1 \xi_1^r + \lambda_2 \xi_2^r + \dots + \lambda_m \xi_m^r$* , MA, v. **52**, (1899), pp. 561-581.
 - [36] *Sur une Généralisation du Théorème de Fermat*, CR Paris, v. **128**, (1899), pp. 1083-1085.
 - [37] *Sur Plusieurs Groupes Linéaires Isomorphes au Groupe Simple d'Ordre 25920*, CR Paris, v. **128**, (1899), pp. 873-875.
 - [38] *Definition of the Abelian, the Two Hypoabelian, and a Related Linear Groups, as Quotient-Groups of the Groups of Isomorphisms of Certain Elementary Groups*, AMS Trans., v. **1**, (1900), pp. 30-38.
 - [39] *A New Definition of the General Abelian Linear Group*, AMS Trans., v. **1**, (1900), pp. 91-96.
 - [40] *Determination of an Abstract Simple Group of Order $2^7.3^6.5.7$ Holoedrally Isomorphic with a Certain Orthogonal Group and with a Certain Hiperabelian Group*, AMS Trans., v. **1**, (1900), pp. 353-370, 509.
 - [41] *Proof of the Existence of the Galois Field of Order p^r , for Every Integer r and Prime Number p* , AMS Bull., v. **6**, (1900), pp. 203-204.
 - [42] *Isomorphism Between Certain Systems of Simple Linear Groups*, AMS Bull., v. **6**, (1900), pp. 323-328.
 - [43] *Certain Subgroups of the Betti-Mathieu Group*, AJM, v. **22**, (1900), pp. 49-54.
 - [44] *Canonical Form of a Linear Homogeneous Substitutions on a Galois Field*, AJM, v. **22**, (1900), pp. 121-137.

- [45] *Concerning the Cyclic Subgroups of the Simple Group G of All Linear Fractional Substitutions of Determinant Unity in Two Non-Homogeneous Variables with Coefficients in an Arbitrary Galois Field*, AJM, v. **22**, (1900), pp. 231-252.
- [46] *An Abstract Simple Group of Order 25920*, LMS Proc., v. **32**, (1900), pp. 3-10.
- [47] *Linear Substitutions Commutative with a Given Substitutions*, LMS Proc., v. **32**, (1900), pp. 165-170.
- [48] *Proof of the Non-Isomorphism of the Simple Abelian Group on $2m$ Indices and the Simple Orthogonal Group on $2m + 1$ Indices, for $m > 2$* , QJM, v. **32**, (1900), pp. 42-63.
- [49] *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig, (1901).
- [50] *Canonical Forms of Quaternary Abelian Substitutions in an Arbitrary Galois Field*, AMS Trans., v. **2**, (1901), pp. 103-138.
- [51] *Theory of Linear Groups in an Arbitrary Field*, AMS Trans., v. **2**, (1901), pp. 363-394.
- [52] *Concerning Real and Complex Continuous Groups*, AMS Bull., v. **7**, (1901), pp. 340-350.
- [53] *The Configurations of the 27 Lines on a Cubic surface and the 28 Bitangents to a Quartic Curve*, AMS Bull., v. **8**, (1901), pp. 63-70.
- [54] *Distribution of the Ternary Linear Homogeneous Substitutions in a Galois Field into Complete Sets of Conjugate Substitutions*, AJM, v. **23**, (1901), pp. 37-40.
- [55] *Representation of Linear Groups as Transitive Substitution Groups*, AJM, v. **23**, (1901), pp. 337-377.
- [56] *On Systems of Isothermal Curves*, AMM, v. **8**, (1901), pp. 187-192.
- [57] *Concerning the Abelian and Related Linear Groups*, LMS Proc., v. **33**, (1901), pp. 313-325.
- [58] *Linear Groups in an Infinite Field*, LMS Proc., v. **34**, (1901), pp. 185-205.
- [59] *A Class of Groups in an Arbitrary Realm Connected with the Configuration of the 27 Lines on a Cubic Surface*, QJM, v. **33**, (1901), pp. 145-173.
- [60] *Théories des Groupes Linéaires dans un Domaine Arbitraire de Rationalité*, CR Paris, v. **132**, (1901), pp. 1547-1548.

-
- [61] *The Alternating Group on Eight Letters and the Quaternary Linear Congruence Group Modulo Two*, MA, v. 54, (1901), pp. 564-569.
 - [62] *The Known Systems of Simple Groups and their Inter-Isomorphism*, Intern. Congress Mathems., Paris, (1902), pp. 225-229.
 - [63] *The Groups of Steiner in Problems of Contact*, AMS Trans., v. 3, (1902), pp. 38-45.
 - [64] *On the Group Defined for Any Given Field by the Multiplication Table of Any Given Finite Group*, AMS Trans., v. 3, (1902), pp. 285-301.
 - [65] *The Groups of Steiner in Problems of Contact* (second paper), AMS Trans., v. 3, (1902), pp. 377-382.
 - [66] *A Class of Simple Transitive Linear Groups*, AMS Bull., v. 8, (1902), pp. 394-401.
 - [67] *Cyclic Subgroups of the Simple Ternary Linear Fractional Group in a Galois Field*, AJM, v. 24, (1902), pp. 1-12.
 - [68] *Canonical Form of a Linear Homogeneous Transformation in an Arbitrary Realm of Rationality*, AJM, v. 24, (1902), pp. 101-108.
 - [69] *Geometrical Derivation of Certain Trigonometric Formulae*, AMM, v. 9, (1902), pp. 36-37.
 - [70] *Factors of a Certain Determinant of Order Six*, AMM, v. 9, (1902), pp. 66-68.
 - [71] *The Order of a Certain Senary Linear Group*, AMM, v. 9, (1902), pp. 149-152.
 - [72] *A Matrix Defined by the Quaternion Group*, AMM, v. 9, (1902), pp. 243-248.
 - [73] *An Elementary Exposition of Frobenius's Theory of Group-Characters and Group-Determinants*, AM, s. 2, v. 4, (1902), pp. 25-49.
 - [74] *On the Groups Defined for an Arbitrary Field by the Multiplication Tables of Certain Finite Groups*, LMS Proc., v. 35, (1902), pp. 68-80.
 - [75] *The Abstract Group Simply Isomorphic with the Group of Linear Fractional Transformations in a Galois Field*, LMS Proc., v. 35, (1902), pp. 292-305.
 - [76] *Generational relations of an Abstract Simple Group of Order 4080*, LMS Proc., v. 35, (1902), pp. 306-319.
 - [77] *Theorems on the Residues of Multinomial Coefficients with Respect to a Prime Modulus*, QJM, v. 33, (1902), pp. 378-384.

- [78] *The Hyperorthogonal Groups*, MA, v. 55, (1902), pp. 521-572.
- [79] *Ternary Orthogonal Group in a General Field*, U. Chicago Decennial Pub., v. 9, (1902), pp. 27-34.
- [80] *Groups Defined for a General Field by the Rotation Groups*, U. Chicago Decennial Pub., v. 9, (1902), pp. 35-51.
item[[80A]] *College Algebra*, New York, (1902), Answers, New York, (1904).
- [81] *Introduction to the Theory of Algebraic Equations*, New York, (1903).
- [82] *Definitions of a Field by Independent Postulates*, AMS Trans., v. 4, (1903), pp. 13-20.
- [83] *Definitions of a Linear Associative Algebra by Independent Postulates*, AMS Trans., v. 4, (1903), pp. 21-26.
- [84] *On the Subgroups of Order a Power of p in the Quaternary Abelian Group in the Galois Field of Order p^n* , AMS Trans., v. 4, (1903), pp.371-386.
- [85] *On the Reducibility of Linear Groups*, AMS Trans., v. 4, (1903), pp. 434-436.
- [86] *Three Sets of Generational Relations Defining the Abstract Simple Group of Order 504*, AMS Bull., v. 9, (1903), pp. 194-204.
- [87] *Generational Relations Defining the Abstract Simple Group of Order 660*, AMS Bull., v. 9, (1903), pp. 204-206.
- [88] *The Abstract Group G Simply Isomorphic with the Alternating Group on Six Letters*, AMS Bull., v. 9, (1903), pp. 303-306.
- [89] *Fields whose Elements are Linear Differential Expressions*, AMS Bull., v. 10, (1903), pp. 30-31.
- [90] *Three Algebraic Notes*, AMM, v. 10, (1903), pp. 219-226.
- [91] *A Generalization of Symmetric and Skew-symmetric Determinants*, AMM, v. 10, (1903), pp. 253-256.
- [92] *Generational Relations for the Abstract Group Simply Isomorphic with the Linear Fractional Group in the $\mathbb{GF}[2^n]$* , LMS Proc., v. 35, (1903), pp. 443-454.
- [93] *Addition to the Paper on the Four Known Simple Groups of Order 25920*, LMS Proc., s. 2, v. 1, (1903), pp. 283-284.

-
- [94] *The Subgroups of Order a Power of 2 of the Simple Quinary Orthogonal Group in the Galois Field of Order $p^n = 8l + 3$* , AMS Trans., v. 5, (1904), pp. 1-38.
 - [95] *Determination of all Subgroups of the Known Simple Group of Order 25920*, AMS Trans., v. 5, (1904), pp. 126-1660.
 - [96] *Two Systems of Subgroups of the Quaternary Abelian Group in a General Galois Field*, AMS Bull., v. 10, (1904), pp. 178-184.
 - [97] *On the Subgroups of Order a Power of p in the Linear Homogeneous and the Fractional Groups in the $\mathbb{GF}[p^n]$* , AMS Bull., v. 10, (1904), pp. 385-397.
 - [98] *Memoir on Abelian Transformations*, AJM, v. 26, (1904), pp. 243-318.
 - [99] *A Property of the Group G_2^{2n} all of whose Operators Except Identity are of Period 2*, AMM, v. 11, (1904), pp. 203-206.
 - [100] *Determination of all Groups of Binary Linear Substitutions with Integral Coefficients Taken Modulo 3 and of Determinant Unity*, AM, s. 2, v. 5, (1904), pp. 140-144.
 - [101] *Application of Groups to a Complex Problem in Arrangements*, AM, s. 2, v. 6, (1904), pp. 31-44.
 - [102] *A New Extension of Dirichlet's Theorem on Prime Numbers*, MM, v. 33, (1904), pp. 155-161.
 - [103] *On the Minimum Degree of Resolvents for the p -Section of the Periods of Hyperelliptic Functions of Four Periods*, DMV Jahr., v. 13, (1904), pp. 559-560.
 - [104] *The Minimum Degree τ of Resolvents for the p -Section of the Periods of Hyperelliptic Functions of Four Periods*, AMS., v. 6, (1905), pp. 48-57.
 - [105] *Definitions of a Group and a Field by Independent Postulates*, AMS Trans., v. 6, (1905), pp. 198-204.
 - [106] *On Semi-Groups and the General Isomorphism Between Finite Groups*, AMS Trans., v. 6, (1905), pp. 205-208.
 - [107] *On Hypercomplex Numbers Systems*, AMS Trans., v. 6, (1905), pp. 234-348.
 - [108] *The Group of a Tactical Configuration*, AMS Bull., v. 11, (1905), pp. 177-179.
 - [109] *On the Class of the Substitutions of Various Linear Groups*, AMS Bull., v. 11, (1905), pp. 426-432.

- [110] *A General Theorem on Algebraic Numbers*, AMS Bull., v. 11, (1905), pp. 482-486.
- [111] *Determination of the Ternary Modular Groups*, AJM, v. 27, (1905), pp. 189-202.
- [112] *Subgroups of Order a Power of p in the General and Special m -ry Linear Homogeneous Groups in the $\text{GF}[p^n]$* , AJM, v. 27, (1905), pp. 280-302.
- [113] *On the Cyclotomic Functions*, AMM, v. 12, (1905), pp. 86-89.
- [114] *Graphical Methods in Trigonometry*, AMM, v. 12, (1905), pp. 129-133.
- [115] *Expressions for the Elements of a Determinant in Terms of the Minors of a Given Order. Generalization of a Theorem Due to Studnicka*, AMM, v. 12, (1905), pp. 217-221.
- [116] *On the Real Elements of Certain Classes of Geometrical Configurations*, AM, s. 2, v. 6, (1905), pp. 141-150.
- [117] *Determination of all Subgroups of the Three Highest Powers of p in the Group G of all m -ary Linear Homogeneous Transformations Modulo p* , QJM, v. 36, (1905), pp. 373-384.
- [118] *A New System of Simple Groups*, MA. v. 60, (1905), pp. 137-150.
- [119] *On Finite Algebras*, GN, (1905), pp. 358-393.
- [120] *On Quadratic, Hermitian and Bilinear Forms*, AMS Trans., v. 7, (1906), pp. 275-292.
- [121] *Linear Algebras in which Division is Always Uniquely Possible*, AMS Trans., v. 7, (1906), pp. 370-390.
- [122] *On Commutative Linear Algebras in which Division is Always Uniquely Possible*, AMS Trans., v. 7, (1906), pp. 514-522.
- [123] *Criteria for the Irreducibility of Functions in a Finite Field*, AMS Bull., v. 13, (1906), pp. 1-8.
- [124] *On Theory of Equations in a Galois Field*, AMS Bull., v. 13, (1906), pp. 8-10.
- [125] *On the Quaternary Linear Homogeneous Groups Modulo p of Order a Multiple of p* , AJM, v. 28, (1906), pp. 1-16.
- [126] *On Linear Algebras*, AMM, v. 13, (1906), pp. 201-205.

-
- [127] *The Abstract Form of the Special Linear Homogeneous Group in a Arbitrary Field*, QJM, v. 38, (1907), pp. 141-145.
- [128] *The Abstract Form of the Abelian Linear Groups*, QJM, v. 38, (1907), pp. 145-157.
- [129] *Invariants of Binary Forms Under Modular Transformations*, AMS Trans., v. 8, (1907), pp. 205-232.
- [130] *Modular Theory of Group-Matrices*, AMS Trans., v. 8, (1907), pp. 389-398.
- [131] *Algebraic Numbers and Forms*, AMS Bull., v. 13, (1907), pp. 348-362.
- [132] *The Symmetric Group on Eight Letters and the Senary First Hypoabelian Group*, AMS Bull., v. 13, (1907), pp. 386-389.
- [133] *Modular Theory of Group Characters*, AMS Bull., v. 13, (1907), pp. 477-488.
- [134] *On Quadratic Forms in a General Field*, AMS Bull., v. 14, (1907), pp. 108-115.
- [135] *Note on the Volume of a Tetrahedron in Terms of the Coordinates of the Vertices*, AMM, v. 14, (1907), pp. 117-118.
- [136] *Invariants of the General Quadratic Form Modulo 2*, LMS Proc., s. 2, v. 5, (1907), pp. 301-324.
- [137] *Representations of the General Symmetric Group as Linear Group in Finite and Infinite Fields*, AMS Trans., v. 9, (1908), pp. 121-148.
- [138] *On Triple Algebras and Ternary Cubic Forms*, AMS Bull., v. 14, (1908), pp. 160-169.
- [139] *On Higher Congruences and Modular Invariants*, AMS Bull., v. 14, (1908), pp. 313-318.
- [140] *Criteria for the Irreducibility of a Reciprocal Equation*, AMS Bull., v. 14, (1908), pp. 426-430.
- [141] *On the Canonical Forms and Automorphisms of Ternary Cubic Forms*, AJM, v. 30, (1908), pp. 117-128.
- [142] *Invariantive Reduction of Quadratic Forms in the $GF[2^n]$* , AJM, v. 30, (1908), pp. 263-281.
- [143] *The Galois Group of a Reciprocal Quartic Equation*, AMM, v. 15, (1908), pp. 71-78.

- [144] *On the Factorization of Large Numbers*, AMM, v. 15, (1908), pp. 217-222.
- [145] *Second Paper - A Class of Groups in an Arbitrary Realm Connected with the Configuration of the 27 Lines on a Cubic Surface*, QJM, v. 39, (1908), pp. 205-209.
- [146] *On Families of Quadratic Forms in a General Field*, QJM, v. 39, (1908), pp. 316-333.
- [147] *On the Last Theorem of Fermat (Second Paper)*, QJM, v. 40, (1908), pp. 27-45.
- [148] *On the Congruence $x^n + y^n + z^n \equiv 0 \pmod{p}$* , Crelle's J., v. 135, (1908), pp. 134-141.
- [149] *On the Last Theorem of Fermat*, MM, v. 38, (1908), pp. 14-32.
- [150] *Definite Forms in a Finite Field*, AMS Trans., v. 10, (1909), pp. 109-122.
- [151] *General Field of a Modular Invariants*, AMS Trans., v. 10, (1909), pp. 123-158.
- [152] *Equivalence of Pairs of Bilinear or Quadratic Forms under Rational Transformation*, AMS Trans., v. 10, (1909), pp. 347-360.
- [153] *On the Representation of Numbers by Modular Forms*, AMS Bull., v. 15, (1909), pp. 338-347.
- [154] *Rational Reduction of a Pair of Binary Quadratic Forms; Their Modular Invariants*, AJM, v. 31, (1909), pp. 103-146.
- [155] *A Theory of Invariants*, AJM, v. 31, (1909), pp. 337-354.
- [156] *On the Representations of Numbers as the Sum of Two Squares*, AMM, v. 16, (1909), pp. 85-87.
- [157] *Rational Edged Cuboids with Equal Volumes and Equal Surfaces*, AMM, v. 16, (1909), pp. 107-114.
- [158] *Modular Invariants of a General System of Linear Forms*, LMS Proc., s. 2, v. 7, (1909), pp. 430-444.
- [159] *On Commutative Linear Groups*, QJM, v. 40, (1909), pp. 167-196.
- [160] *Combinants*, QJM, v. 40, (1909), pp. 349-366.
- [161] *Lower Limit for the Number of Sets of Solutions of $x^n + y^n + z^n \equiv 0 \pmod{p}$* , Crelle's J., v. 135, (1909), pp. 181-188.
- [162] *On Certain Diophantine Equations*, MM, v. 39, (1909-10), pp. 86-87.

-
- [163] *On the Factorization of Integral Functions with p -Adic Coefficients*, AMS Bull., v. 17, (1910), pp. 19-23.
- [164] *On the Negative Discriminants for which There is a Single Class of Positive Primitive Binary Quadratic Forms*, AMS Bull., v. 17, (1911), pp. 534-537.
- [165] *Constructions with Ruler and Compasses; Regular Polygons*, J.W.A. Young, Monographs on Topics of Modern Math..., New York, (1911), pp. 351-386.
- [166] *An Invariant Investigation of Irreducible Binary Modular Forms*, AMS Trans., v. 12, (1911), pp. 1-18.
- [167] *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem*, AMS Trans., v. 12, (1911), pp. 75-98.
- [168] *Binary Modular Groups and Their Invariants*, AJM, v. 33, (1911), pp. 175-192.
- [169] *Notes on the Theory of Numbers*, AMM, v. 18, (1911), pp. 109-11.
- [170] *Note on Cubic Equations and Congruences*, AM, s. 2, v. 12, (1911), pp. 149-152.
- [171] *Note on Modular Invariants*, QJM, v. 42, (1911), pp. 158-161.
- [172] *On Non-Vanishing Forms*, QJM, v. 42, (1911), pp. 162-171.
- [173] *Linear Algebras*, AMS Trans., v. 13, (1912), pp. 59-73.
- [174] *Proof of the Finiteness of Modular Covariants*, AMS Trans., v. 14, (1913), pp. 299-310.
- [175] *On Binary Modular Groups and their Invariants*, AMS Bull., v. 20, (1913), pp. 132-134.
- [176] *Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors*, AJM, v. 35, (1913), pp. 413-422.
- [177] *Even Abundant Numbers*, AJM, v. 135, (1913), pp. 423-426.
- [178] *Amicable Number Triples*, AMM, v. 20, (1913), pp. 84-92.
- [179] *On the Rank of a Symmetrical Matrix*, AM, s. 2, v. 15, (1913), pp. 27-28.
- [180] *Theorems and Tables on the Sum of Divisors of a Number*, QJM, v. 44, (1913), pp. 264-296.
- [181] *Algebraic Invariants*, New York, (1914), x+100p.

- [182] *Linear Algebras*, Cambridge, (1914), viii+73p.
- [183] *On Invariants and the Theory of Numbers*, AMS Colloq. Pub., (1914), vi+110p.
- [184] *Linear Associative Algebras and Abelian Equations*, AMS Trans., v. 15, (1914), pp. 31-46.
- [185] *Invariants in the Theory of Numbers*, AMS Trans., v. 15, (1914), pp. 497-503.
- [186] *On the Trisection of an Angle and the Construction of Regular Polygons of 7 and 9 Sides*, AMM., v. 21, (1914), pp. 259-262.
- [187] *The Invariants, Seminvariants and Linear Covariants of the Binary Quartic Form Modulo 2*, AM, s. 2, v. 15, (1914), pp. 114-117.
- [188] *The Points of Inflexion of a Plane Cubic Curve*, AMM, s. 2, v. 156, (1914), pp. 50-66.
- [189] *Modular Invariants of the System of a Binary Cubic, Quadratic, and Linear Form*, QJM, v. 45, (1914), pp. 373-384.
- [190] *Elementary Theory of Equations*, New York, (1914), v+184p.
- [191] *Projective Classification of Cubic Surfaces, Modulo 2*, AM, s. 2, v. 16, (1915), pp. 139-157.
- [192] *Quartic Curves Modulo 2*, AMS Trans., v 16, (1915), pp. 111-120.
- [193] *Invariants, Seminvariants, and Covariants of the Ternary and Quadratic Form Modulo 2*, AMS Bull., v. 21, (1915), pp. 174-179.
- [194] *On the Relation Between Linear Algebras and Continuous Groups*, AMS Bull., v. 22, (1915), pp. 53-61.
- [195] *Invariant Theory of Plane Cubic Curves Modulo 2*, AJM, v. 37, (1915), pp. 107-116.
- [196] *Geometric and Invariantive Theory of Quartic Curves Modulo 2*, AJM, v. 37, (1915), pp. 337-354.
- [197] *Invariantive Classification of Pairs of Conics Modulo 2*, AJM, v. 37, (1915), pp. 355-358.
- [198] *Classification of Quartic Curves Modulo 2* MM, v. 44, (1915), pp. 189-192.
- [199] *Recent Progress in the Theories of Modular and Formal Invariants and in Modular Geometry*, NAS Proc., v. 1, (1915), pp. 1-4.

-
- [200] *The Straight Lines on Modular Cubic Surfaces*, NAS Proc., v. 1, (1915), pp. 248-253.
 - [201] *Theory and Applications of Finite Groups* (with Miller and Blichfeldt), New York, (1916), vii+390p. Reproduzido com correções, New York, (1938).
 - [202] *An Extension of the Theory of Numbers by Means of Correspondences Between Fields*, AMS Bull., v. 23, (1916), pp. 109-111.
 - [203] *Fermat's Last Theorem and the Origin and Nature of Algebraic Numbers*, AM, s. 2, v. 18, (1917), pp. 161-187.
 - [204] *History of the Theory of Numbers* (Carnegie Institution), v. 1, *Divisibility and Primality*, (1919), xii+486p; v. 2, *Diophantine Analysis*, (1920), xxv+803p; v. 3, *Quadratic and Higher Forms*, (1923), v+313p. Reproduzido com número reduzido de páginas, New York, G.E. Stechert and Co., 3v., (1934).
 - [205] *On Quaternions and their Generalization and the History of the Eight Square Theorem*, AM, s. 2, v. 20, (1919), pp. 155-171.
 - [206] *Mathematics in War Perspective*, AMS Bull., v. 25, (1919), pp. 289-311. AMS Ret. P add. 27 Dec. (1918).
 - [207] *Applications of the Geometry of Numbers to Algebraic Numbers*, AMS Bull., v. 25, (1919), pp. 453-455.
 - [208] *Les Polynomes Égaux à des Déterminants*, CR Paris, v. 171, (1920), pp. 1360-1362.
 - [209] *Some Relations Between the Theory of Numbers Other Branches of Mathematics*, Intern. Congress. Maths., Strasbourg, (1921), pp. 41-56.
 - [210] *Homogeneous Polynomials with a Multiplication Theorem*, Intern. Congress. Maths., Strasbourg, (1921), pp. 215-230.
 - [211] *Determination of all General Homogeneous Polynomials Expressible as Determinants with Linear Elements*, AMS Trans., v. 22, (1921), pp. 167-179.
 - [212] *Fallacies and Misconceptions in Diophantine Analysis*, AMS Bull., v. 27, (1921), pp. 312-319.
 - [213] *A New Method in Diophantine Analysis*, AMS Bull., v. 27, (1921), pp. 353-365.
 - [214] *Algebraic Theory of the Expressibility of Cubic Forms as Determinants, with Application to Diophantine Analysis*, AJM, v. 43, (1921), pp. 102-125.
 - [215] *Rational Triangles and Quadrilaterals*, AMM, v. 28, (1921), pp. 244-250.

- [216] *Reducible Cubic Forms Expressible Rationally as Determinants*, AM, s. 2, v. 23, (1921), pp. 70-74.
- [217] *A Fundamental System of Covariants of the Ternary Cubic Forms*, AM, s. 2, v. 23, (1921), pp. 78-82.
- [218] *Arithmetic of Quaternions*, LMS Proc., v. 20, (1921), pp. 225-232.
- [219] *La Composition des Polynomes*, CR Paris, v. 172, (1921), pp. 636-640.
- [220] *Quaternions and their Generalizations*, NAS Proc., v. 7, (1921), pp. 109-114.
- [221] *Perfect and Amicable Numbers*, Scientific Mo., v. 12, (1921), pp. 349-354.
- [222] *Why it is Impossible to Trisect an Angle or to Construct a regular Polygon of Seven or Nine Sides by Ruler and Compasses*, MT, v. 14, (1921), pp. 217-223.
- [223] *Progrés Recents dans la Théorie des Nombres*, Sphinx CEdipe, v. 16, (1921), 32p. suppl. (em acordo com o índice do periódico).
- [224] *Plane Trigonometry with Practical Applications*, Chicago, (1922), xi+176+35p.
- [225] *First Course in the Theory of Equations*, New York, (1922), vi+168p.
- [226] *Impossibility of Restoring Unique Factorization in a Hypercomplex Arithmetic*, AMS Bull., v. 28, (1922), pp. 438-442.
- [227] *The Theory of Numbers: its Principal Branches*, Scientia, (1922), pp. 421-430.
- [228] *Report of Committee on Algebraic Numbers* (NRC, with Vandiver, etc), (1923), 96p.
- [229] *Algebras and their Arithmetics*, Chicago, U. Chicago Press, (1923), xiii+241p. re-printed, New York, Stechert, (1938).
- [230] *Integral Solutions of $x^2 - my^2 = zw$* , AMS Bull., v. 29, (1923), pp. 464-467.
- [231] *The Rational Linear Algebras of Maximum and Minimum Ranks*, LMS Proc., v. 22, (1923), pp. 145-162.
- [232] *A New Simple Theory of Hypercomplex Integers*, Journ. d. Mathém., s. 9, v. 2, (1923), pp. 281-326.
- [233] *Algebras and their Arithmetics*, AMS Bull., v. 30, (1924), pp. 247-257.
- [234] *Quadratic Fields in which Factorization is Always Possible*, AMS Bull., v. 30, (1924), pp. 328-334.

-
- [235] *On the Theory of Numbers and Generalized Quaternions*, AJM, v. 46, (1924), pp. 1-16.
 - [236] *Differential Equations from the Group Standpoint*, AM, s. 2, v. 25, (1924), pp. 287-378.
 - [237] *Resolvent Sextics of Quintic Equations*, AMS Bull., v. 31, (1925), pp. 515-523.
 - [238] *Algèbres Nouvelles de Division*, CR Paris, v. 181, (1925), pp. 836-838.
 - [239] *Modern Algebraic Theories*, Chicago, (1926), ix+276p. Trad. alemã: *Höhere Algebra*, Leipzig, (1926), vii+242p.
 - [240] *New Division Algebras*, AMS Trans., v. 28, (1926), pp. 207-234.
 - [241] *All Integral Solutions of $ax^2 + bxy + cy^2 = w_1w_2 \cdots w_n$* , AMS Bull., v. 32, (1926), pp. 644-648.
 - [242] *Quadratic Forms which Represent all Integers*, NAS Proc., v. 12, (1926), pp. 756-757.
 - [243] *Singular Case of Pairs of Bilinear, Quadratic, or Hermitian Forms*, AMS Trans., v. 29, (1927), pp. 239-253.
 - [244] *Integers Represented by a Positive Ternary Quadratic Form*, AMS Bull., v. 33, (1927), pp. 63-70.
 - [245] *A Generalization of Waring's Theorem on Nine Cubes*, AMS Bull., v. 33, (1927), pp. 299-300.
 - [246] *Extension of Waring's Theorem on Fourth Powers*, AMS Bull., v. 33, (1927), pp. 219-327.
 - [247] *All Positive Integers are Sums of Values of a quadratic Function of x* , AMS Bull., v. 33, (1927), pp. 713-720.
 - [248] *Quartenary Quadratic Forms Representing all Integers*, AJM, v. 49, (1927), pp. 39-56.
 - [249] *Generalizations of Waring's Theorem on Fourth, Sixth, and Eighth Powers*, AJM, v. 49, (1927), pp. 241-250.
 - [250] *Extensions of Waring's Theorem on Nine Cubes*, AMM, v. 34, (1927), pp. 177-183.
 - [251] *Ternary Quadratic Forms and Congruences*, AM, s. 2, v. 28, (1927), pp. 333-341.

- [252] *Recent Light on Classic Problems in the Theory of Numbers*, APS Proc., v. 66, (1927), pp. 281-286.
- [253] *Algebren und ihre Zahlentheorie*, Zürich, (1927), viii+308+1p.
- [254] *Simpler Proofs of Waring's Theorem on Cubes, with Various Generalizations*, AMS Trans., v. 30, (1928), pp. 1-18.
- [255] *Generalizations of the Theorem of Fermat and Cauchy on Polygonal Numbers*, AMS Bull., v. 34, (1928), pp. 63-72.
- [256] *Extended Polygonal Numbers*, AMS Bull., v. 34, (1928), pp. 205-217.
- [257] *New Division Algebras*, AMS Bull., v. 34, (1928), pp. 555-560.
- [258] *Additive Number Theory for all Quadratic Functions*, AJM, v. 50, (1928), pp. 1-48.
- [259] *Quadratic Functions or Forms, Sums of whose Values Give all Positive Integers*, Journ. d. Mathém., s. 9, v. 7, (1928), pp. 319-336.
- [260] *Further Development of the Theory of Arithmetics of Algebra*, Inter. Congress Mathems., Toronto, (1928), pp. 173-184.
- [261] *Outline of the Theory to date of the Arithmetics of Algebras*, Inter. Congress Mathems., Toronto, (1928), pp. 95-102.
- [262] *A New Theory of Linear Transformations and Pairs of Bilinear Forms*, Inter. Congress Mathems., Toronto, (1928), pp. 361-363.
- [263] *Introduction to the Theory of Numbers*, Chicago, (1929), viii+183p. Trad. alemã: *Einführung in die Zahlentheorie*, Leipzig, (1931), viii+175p.
- [264] *Universal Quadratic Forms*, AMS Trans., v. 31, (1929), pp. 164-189.
- [265] *The Forms $ax^2 + by^2 + cz^2$ which Represent all Integers*, AMS Bull., v. 35, (1929), pp. 55-59.
- [266] *Studies in the Theory of Numbers*, Chicago, (1930), x+230p.
- [267] *Construction of Division Algebras*, AMS Trans., v. 32, (1930), pp. 319-334.
- [268] *Proof of a Waring Theorem on Fifth Powers*, AMS Bull., v. 37, (1931), pp. 549-553.
- [269] *Minimum Decompositions into Fifth Powers*, BAAS, Math. Tables, III, (1933), vi+400p.

-
- [270] *Recent Progress on Waring's Theorem and its Generalizations*, AMS Bull., v. 39, (1933), pp. 701-727.
- [271] *Minimum Decomposition into n -th Powers*, AJM, v. 55, (1933), pp. 593-602.
- [272] *Waring's Problem for Cubic Functions*, AMS Trans., v. 36, (1934), pp. 1-12.
- [273] *A New Method for Waring Theorems with Polynomial Summands*, AMS Trans., v. 36, (1934), pp. 731-748.
- [274] *Waring's Problem for Ninth Powers*, AMS Bull., v. 40, (1934), pp. 487-493.
- [275] *The Converse of Waring's Problem*, AMS Bull., v. 40, (1934), pp. 711-714.
- [276] *Two-Fold Generalizations of Cauchy's Lemma*, AJM, v. 56, (1934), pp. 513-528.
- [277] *Polygonal Numbers and Related Waring Problem*, QJMO, v. 5, (1934), pp. 283-290.
- [278] *Universal Waring Theorem for Eleventh Powers*, LMS Journ., v. 9, (1934), pp. 201-206.
- [279] *Researches on Waring's Problem*, Carnegie Institution, Wash., (1935), v+257p.
- [280] *Cyclotomy and Trinomial Congruences*, AMS Trans., v. 37, (1935), pp. 363-380.
- [281] *Cyclotomy when e is Composite*, AMS Trans., v. 38, (1935), pp. 187-200.
- [282] *Congruences Involving Only e -th Powers*, Acta Arith., v. 1, (1935), pp. 161-167.
- [283] *Linear Algebras with Associativity not Assumed*, DMJ, v. 1, (1935), pp. 113-125.
- [284] *Cyclotomy, Higher Congruences, and Waring's Problem*, AJM, v. 57, (1935), pp. 391-424.
- [285] *A New Method for Waring Theorems with Polynomial Summands, II*, AMS Trans., v. 39, (1936), pp. 205-208.
- [286] *A Generalization of Waring's Problem*, AMS Bull., v. 42, (1936), pp. 525-529.
- [287] *The Waring Problem and its Generalizations*, AMS Bull., v. 42, (1936), pp. 833-842.
- [288] *Waring Theorems of New Type*, AJM, v. 58, (1936), pp. 41-248.
- [289] *Proof of the Ideal Waring Theorem for Exponents 7-180*, AMJ, v. 58, (1936), pp. 521-529.

- [290] *Solution of Waring's Problem*, AJM, v. 58, (1936), pp. 530-535.
- [291] *On Waring's Problem and its Generalization*, AM, s. 2, v. 537, (1936), pp. 293-316.
- [292] *Universal Waring Theorems with Cubic Summands*, Acta Arith., v. 2, (1936), pp. 184-196.
- [293] *The Ideal Waring Theorem for Twelfth Powers*, DMJ, v. 2, (1936), pp. 192-204.
- [294] *Universal Waring Theorems*, MMP, v. 43, (1936), pp. 391-400.
- [295] *Biographical Memoir of Eliakim Hastings Moore, 1862-1932* (com G.A. Bliss), NAS Biog. Mem., v. 17, (1936), pp. 83-102.
- [296] *Herbert Ellsworth Slaught* (com G.A. Bliss), Science, v. 86, (1937), pp. 72-73.
- [297] *New Waring Theorems for Polygonal Numbers*, QJMO, v. 8, (1937), pp. 62-65.
- [298] *Universal Forms $\sum a_i x_i^n$ and Waring's Problem*, Acta Arith., v. 2, (1937), pp. 177-196.
- [299] *Revisões de livros de Page, Cahen, Dedekind, Bachmann, Zindler, Bauer, Burkhardt, de Séguier, Cajori, Tannery, König, Galois, Minkowski, Sylvester, Hensel, Bell em AMS Bull.*, (1899-1928).

Apêndice C

O Livro *History of Theory of Numbers*

Apesar do tema deste livro não estar relacionado com as pesquisas desenvolvidas nesta tese, pela magnitude desta obra (publicada em três volumes), será desenvolvido um breve estudo acerca de suas contribuições para a história da teoria de números. Assim como seu livro *Linear Group with an Exposition of the Galois Field Theory* ([49]) foi extremamente importante para o desenvolvimento da teoria de grupos lineares finitos (com Dickson tornando-se o maior especialista no assunto, com a publicação desta obra, em 1901), *History of Theory of Numbers* ([204]) teve um papel fundamental para a compreensão da teoria de números, pois nesta obra ele faz um estudo detalhado acerca do assunto, esgotando-o por completo. Nas próximas seções será realizado um resumo dos tópicos abordados, ao longo dos três magníficos volumes desta estupenda obra.

C.1 O Primeiro Volume

Este volume foi publicado em 1919 e, no primeiro capítulo, Dickson realiza um estudo detalhado de números perfeitos, perfeitamente múltiplos e números “amigos”. Define um número perfeito como aquele que é igual à soma de seus divisores diferentes dele próprio (os primeiros números perfeitos encontrados foram 6 e 28¹) e apresenta algumas de suas propriedades, como o resultado provado por Euclides que o número $2^{p-1}(2^p - 1)$ é um número perfeito se $2^p - 1$ é um primo. Já um número perfeitamente múltiplo é definido como aquele cuja soma de seus divisores é um múltiplo dele; e dois números são chamados “amigos” se cada um deles é igual à soma dos divisores do outro (onde um número não conta como divisor de si mesmo). Esta definição já havia sido dada por Pitágoras, que exibiu o par de números “amigos” 1184 e 1210. Aqui Dickson exhibe novos pares deste tipo de números.

¹Alguns estudiosos da Bíblia atribuem à propriedade, que define os números perfeitos, o papel que estes tiveram na descrição da criação do Universo.

No segundo capítulo, Dickson explicita expressão para a soma $\sigma(n)$ de todos os divisores de n e apresenta a história dos dois problemas de Fermat para resolver $\sigma(x^3) = y^2$ e $\sigma(x^2) = y^3$ e o problema de John Wallis, para encontrar solução diferente de $x = 4$ e $y = 5$ de $\sigma(x^2) = \sigma(y^2)$.

Fermat afirmou, em 1640, que tinha uma prova do fato (hoje conhecido como teorema de Fermat — um dos teoremas fundamentais da teoria de números) que se p é um primo e x é um inteiro qualquer, então $x^{p-1} - 1$ é divisível por p . Embora o caso $x = 2$ já fosse conhecido dos chineses, desde antes de 500 a.C., a primeira demonstração foi publicada por Euler, em 1735. Euler também foi responsável, em 1760, pela importante generalização do caso de um primo p para o caso n inteiro qualquer: se $\phi(n)$ denota o número de inteiros positivos menores que n e relativamente primos com n , então $x^{\phi(n)} - 1$ é divisível por n para todo inteiro x relativamente primo com n . Outro *elegante* teorema (termo usado por Dickson), de John Wilson e publicado por Waring, em 1770², afirma que se p é um primo, então $1 + 1 * 2 * 3 \cdots * (p - 1)$ é divisível por p ; entretanto, o primeiro a apresentar uma demonstração para este fato foi, em 1771, Lagrange, que também observou que a recíproca é verdadeira. Já em 1801, Gauss apresentou (e sugeriu métodos para provar) generalizações do teorema de Wilson: se P denota o produto de inteiros positivos menores que A e relativamente primos com A , então $P + 1$ é divisível por A se $A = 4$, p^m ou $2p^m$, onde p é um primo ímpar, enquanto que $P - 1$ é divisível por A se A não é escrito em nenhuma destas três formas. Várias provas destes resultados são apresentadas no terceiro capítulo, assim como várias generalizações.

No quarto capítulo, Dickson apresenta propriedades do quociente $\frac{u^{p-1} - 1}{p}$, que tem papel importante na investigação do último teorema de Fermat (ou seja, a impossibilidade de se escrever $x^n + y^n = z^n$ para $n > 2$ e x, y e z inteiros positivos), cuja história é apresentada no capítulo final do segundo volume.

Já algumas das inúmeras propriedades e generalizações da função de Euler ϕ (definida anteriormente) são apresentadas no quinto capítulo, enquanto que as propriedades do conjunto de todas as frações irredutíveis, ordenadas pela sua magnitude, cujos numeradores são menores ou iguais a m e os denominadores são menores ou iguais a n (chamadas séries de Farey quando $m = n$), são discutidas no capítulo seguinte. Algumas das propriedades de frações decimais periódicas, e suas generalizações, são tratadas no fim do capítulo, fornecendo uma concreta introdução ao capítulo sete, que apresenta vários teoremas, tratando expoentes, raízes primitivas e congruências binomiais e cita uma longa lista de raízes primitivas de primos menores que 10.000.

As raízes imaginárias de congruências, introduzidas por Galois, permitiram não apenas uma importante extensão da teoria de números, mas também propiciou uma gama

²Este teorema já havia sido apresentado num manuscrito por Leibniz.

enorme de generalizações de teoremas como, por exemplo, a aplicação de grupos de congruência linear à teoria ordinária de números. Em vez dos resíduos dos inteiros módulo p , consideram-se os resíduos de polinômios na variável x com coeficientes inteiros, em relação a um primo p e a um polinômio $f(x)$ de grau n que é irredutível módulo p . Os resíduos são os p^n polinômios em x de grau $n-1$ cujos coeficientes são escolhidos do conjunto $\{0, 1, \dots, p-1\}$. Estes resíduos formam um corpo de Galois, cujos elementos podem ser adicionados, subtraídos, multiplicados e divididos (exceto pelo zero) entre si. Como uma generalização do teorema de Fermat, Galois provou que a potência $p^n - 1$ de qualquer resíduo, exceto zero, é congruente à unidade em relação ao par p e $f(x)$, introduziu uma raiz indefinida i de $f(x) \equiv 0 \pmod{p}$ e considerou os resíduos módulo p dos polinômios em i . Este assunto é estudado, em detalhes, ao longo do oitavo capítulo, cujos tópicos finais são congruências cúbicas e miscelânea de resultados sobre congruências.

No nono capítulo, são dadas expressões de Legendre para o expoente da maior potência de um primo p que divide $m!$ e a generalização do produto de quaisquer inteiros em progressão aritmética. Também são estudados vários teoremas sobre divisibilidade de um produto de fatoriais por outro produto.

Já no capítulo seguinte, são dados diversos teoremas e fórmulas relacionados à soma de k th potências de todos os divisores de n , ou de seus divisores pares ou ímpares, ou daqueles cujos divisores complementares são pares, ou ímpares, ou exatamente sth potências.

No capítulo onze, Dickson apresenta vários teoremas sobre máximo divisor comum e mínimo múltiplo comum, sobre máximos divisores que são ímpares, ou têm propriedades específicas, e sobre valores médios. Já o capítulo doze é dedicado ao estudo da divisibilidade entre dois números, onde ele cita inúmeros artigos elementares, enquanto que o seguinte trata da história dos números primos, transcrevendo inúmeros artigos que enumeram primos em diversos intervalos e primos da forma $4n+1$. No capítulo quatorze, menciona trabalhos sobre a fatoração de um número como a diferença ou a soma de dois quadrados.

No capítulo quinze, Dickson estuda valores para n que tornam $F_n = 2^{2^n} + 1$ primo. Enquanto Fermat acreditava que isto valia para todo n (o que ele provou, em 1640, ser verdade para $n = 1, 2, 3, 4$), Euler observou, em 1739, que F_n não é primo para $n = 5$. Mais tarde, Gauss provou que um polígono regular de p lados pode ser construído com régua e compasso se p é um primo da forma $F_n = 2^{2^n} + 1$ e afirmou, corretamente, que a construção é impossível se p não é desta forma. Tendo em vista os artigos a que se refere neste capítulo, Dickson observa que F_n é composto se $n = 5, 6, 7, 8, 9, 11, 12, 18, 23, 36, 38$ e 73 .

Já o capítulo dezesseis trata dos fatores dos números da forma $a^n \pm b^n$ e de alguns trinômios, enquanto o seguinte estuda os divisores dos termos de uma série recorrente e, em particular, das funções de Lucas

$$u_n = \frac{a^n - b^n}{a - b}, \quad v_n = a^n + b^n,$$

onde a e b são raízes de $x^2 - Px + Q = 0$, com P e Q inteiros relativamente primos. Estas funções foram usadas por Lucas, para obter uma extensão da generalização de Euler do teorema de Fermat. No fim deste capítulo, Dickson ainda cita vários trabalhos sobre a teoria algébrica de séries recorrentes.

O capítulo dezoito é dedicado ao estudo da teoria dos números primos, onde Dickson observa que Euclides forneceu uma demonstração simples e elegante do fato de que o conjunto dos números primos é infinito, enquanto Legendre deu uma prova insuficiente de que toda progressão aritmética $n, n + m, n + 2m, \dots$, com n e m relativamente primos, contém uma infinidade de primos. Ainda estuda primos em progressão aritmética, números de primos em intervalos determinados, o postulado de Bertrand sobre a existência de pelo menos um primo entre x e $2x - 2$ para $x > 3$ e outros diversos resultados sobre a teoria de números primos. Já o capítulo dezenove trata de inversão de várias funções, apresentando diversas generalizações e fórmulas relacionadas ao assunto. No capítulo final, Dickson apresenta resultados elementares envolvendo algarismos de números, principalmente quando escritos na base 10.

No fim deste volume, ainda são apresentados um índice de autores nele contido e uma lista de símbolos usados ao longo dos capítulos.

C.1.1 Índice do Primeiro Volume

TABLE OF CONTENTS

Chapter		Page
I.	Perfect, multiply perfect, and amicable numbers	3
II.	Formulas for the number and sum of divisors, problems of Fermat and Wallis	51
III.	Fermat's and Wilson's theorems, generalizations and converses; symmetric functions of $1, 2, \dots, p - 1$, modulo p	59
IV.	Residue of $(u^{p-1} - 1)/p$ modulo p	105
V.	Euler's ϕ -function, generalizations; Farey series	113
VI.	Periodical decimal fractions; periodic fractions; factors of $10^n \pm 1$	159
VII.	Primitive roots, exponents, indices, binomial congruences	181
VIII.	Higher congruences	223
IX.	Divisibility of factorials and multinomial coefficients	263
X.	Sum and number of divisors	279
XI.	Miscellaneous theorems on divisibility, greatest common divisor, least common multiple	327
XII.	Criteria for divisibility by a given number	337
XIII.	Factor tables, lists of primes	347
XIV.	Methods of factoring	357

Chapter		Page
XV.	Fermat numbers $F_n = 2^{2^n} + 1$	375
XVI.	Factors of $a^n \pm b^n$	381
XVII.	Recurring series; Lucas' u_n, v_n	393
XVIII.	Theory of prime numbers	413
XIX.	Inversion of functions; Möbius' function $\mu(n)$; numerical integrals and derivatives	441
XX.	Properties of the digits of numbers	453
	Author index	467
	Subject index	484

C.2 O Segundo Volume

Este volume foi publicado em 1920, e o primeiro capítulo é dedicado ao estudo de números *triangulares*, cuja noção Dickson afirma remeter a Pitágoras que os representou como pontos distribuídos como chumbinhos numa pilha triangular de chumbinhos (*The notion of triangular numbers 1, 3, 6, ... goes back to Pythagoras, who represented them by points arranged as are the shot in the base of a triangular pile of shot*) que, de modo análogo, pode ser estendido a um número *poligonal* de m lados (chamado número m -gonal) e a um número *piramidal*. O estudo desenvolve-se com a apresentação do mais importante teorema sobre o assunto, atribuído a Fermat, que afirma: *todo inteiro positivo é triangular ou é uma soma de dois ou três números triangulares; todo inteiro positivo é um quadrado ou é uma soma de dois, três ou quatro quadrados; e pentagonal ou uma soma de dois, três, quatro ou cinco números pentagonais; e analogamente para quaisquer números poligonais*. Euler, que também se interessou pelo estudo de números poligonais, resolveu vários problemas sobre o assunto; entretanto, provou o teorema de Fermat acima, apenas para o caso dos quadrados e observou que o caso de números triangulares é equivalente ao fato de que todo inteiro positivo da forma $8n + 3$ é uma soma de três quadrados. Este resultado é um caso especial do teorema: *todo inteiro positivo que não seja da forma $8n + 7$ ou $4n$ é uma soma de três quadrados*, provado de um modo bastante complicado por Legendre em 1798 e, de uma maneira mais simples, por Gauss, em 1801, durante o estudo de formas quadráticas. Em 1813-15, Cauchy, finalmente, provou que todo número é uma soma de m números m -gonais e cuja demonstração foi imediatamente simplificada por Legendre. Começaram, assim, a surgir novas provas para o referido teorema e algumas extensões destes resultados.

O capítulo seguinte começa com a explicação do método apresentado pelo hindu Brahme Gupta, no século dezessete, para resolver a equação $ax + by = c$. O método consiste em divisões mútuas de a e b , assim como no processo de Euclides para encontrar o máximo

divisor comum deles. Uma prova mais simples de que a equação é solúvel, quando a e b são relativamente primos, foi dada por Euler em 1760, observando que se dividir $c - ax$ ($x = 0, 1, \dots, b-1$) por b , obtêm-se os restos distintos $0, 1, \dots, b-1$ na mesma ordem, com o resto zero implicando na solução. Desde que o mesmo princípio fundamenta a prova da generalização de Euler $a^\beta \equiv 1 \pmod{b}$ para $\beta = \phi(b)$ do teorema de Fermat, torna-se simples resolver esta equação, uma vez que é o mesmo que resolver a congruência $ax \equiv c \pmod{b}$ - bastando, para isto, multiplicar ambos os membros por $a^{\beta-1}$. Isto foi feito, em 1829, por Binet, Libri e Cauchy. Também se pode usar, para resolver esta equação, o teorema generalizado de Wilson, que afirma que o produto de inteiros menores que, e relativamente primos com, b é $\equiv \pm 1 \pmod{b}$. Em 1905, Lerch expressou a solução de $ax \equiv 1 \pmod{b}$ como uma soma envolvendo a maior função inteira.

Na aritmética chinesa do século primeiro, apareceu o problema de encontrar-se um número que possua restos 2, 3 e 2 quando divididos por 3, 5 e 7, respectivamente, com uma regra levando à resposta $23 + 3 * 5 * 7n$. O mesmo problema, surgido na aritmética grega de Nicomachus, em torno de 100 d.C., com a resposta 23, tem essencialmente a seguinte solução (dada por Beveridge, Euler e Gauss alguns séculos depois): para obter-se um número x que possua os restos $r_1, r_2, \dots$, quando divididos por $m_1, m_2, \dots$, respectivamente, onde $m_1, m_2, \dots$ são relativamente primos dois a dois, deve-se encontrar números $\alpha_1, \alpha_2, \dots$, tais que $\alpha_i \equiv 1 \pmod{m_i}$ e $\alpha_i \equiv 0 \pmod{\frac{m}{m_i}}$, onde m é o produto $m_1 m_2 \dots$; então tem-se que $x = \alpha_1 r_1 + \alpha_2 r_2 + \dots$ é uma resposta. Já no século dezessete, o chinês Yih-hing estendeu esta regra para o caso em que $m_1, m_2, \dots$ são inteiros quaisquer: expressando o mínimo múltiplo comum de $m_1, m_2, \dots$ como um produto $m = \mu_1 \mu_2 \dots$ de fatores relativamente primos entre si e tais que μ_i divide m_i , encontrou números $\alpha_1, \alpha_2, \dots$ tais que $\alpha_i \equiv 1 \pmod{\mu_i}$, $\alpha_i \equiv 0 \pmod{\frac{m}{\mu_i}}$; então tem-se que $x = \alpha_1 r_1 + \alpha_2 r_2 + \dots$ ³.

Já o problema de encontrar o número de soluções inteiras positivas de $ax + by = c$, onde a, b, c são inteiros positivos foi estudado por Paoli, em 1780, por Hermite, em 1855-58, e por muitos outros. Entretanto, sistemas de equações do tipo $x + y + z = m$ e $ax + by + cz = n$, onde m, n, a, b, c são inteiros positivos dados e as incógnitas deverão ser inteiros positivos, já haviam aparecido em manuscritos chineses e árabes, que datam dos séculos sexto e décimo, respectivamente, e foram estendidos para sistemas com um número qualquer de equações lineares, em um número qualquer de incógnitas, com coeficientes inteiros positivos. Nestes estudos, Dickson cita os mais importantes trabalhos em sistemas de equações lineares ou congruências, atribuídos a Heger (1858), H.J.S. Smith (1859, 1861, 1871), Weber (1872, 1896), Frobenius (1878-79), Kronecker (1886) e Steinitz (1896).

³Conhecido como Teorema Chinês do Resto, este problema tem aplicação em questões que envolvem os calendários; por exemplo, para encontrar o ano x do calendário Juliano quando o ciclo solar, o ciclo lunar ou a *Prescrição Romana* (ciclo de quinze anos, usado no Império Romano para calcular taxas de juros) são os números dados r_1, r_2, r_3 , obtêm-se um número que tem restos r_1, r_2, r_3 quando divididos por 28, 19 e 15, respectivamente, sendo estes o período (em anos) dos ciclos solar, lunar e Prescrição.

Dickson finaliza este capítulo com uma série de teoremas *modernos* (expressão utilizada por ele), como, por exemplo, o teorema de Minkowski (de grande importância para a teoria de números algébricos) que afirma que, se $f_1, \dots, f_n$ são funções lineares homogêneas de $x_1, \dots, x_n$ com quaisquer coeficientes reais cujo determinante é unitário, então pode-se determinar valores inteiros não todos nulos para $x_1, \dots, x_n$ tais que cada f_i , tomada positiva, não exceda a unidade.

O terceiro capítulo deste volume aborda as partições, que têm aplicações importantes em funções simétricas e invariantes algébricos. Dickson observa que o primeiro estudo foi desenvolvido por Euler, em 1741, quando investigou os problemas de encontrar o número de maneiras possíveis em que um número n (por exemplo 6) pode ser escrito como a soma de um número dado m (como 2) de partes distintas ($6=5+1=4+2$), e o número de maneiras n é uma soma de m partes iguais, ou distintas (neste caso, $6=3+3$ também é contada). Os números em questão são os coeficientes de x^n nas expansões de $\frac{x^{m(m+1)/2}}{D}$ e $\frac{x^m}{D}$, respectivamente, em séries de potências de x , onde

$$D = (1-x)(1-x^2) \cdots (1-x^m).$$

Este tipo de função serve para enumerar todas as partições de um determinado tipo e são chamadas *funções geradoras*. Euler fez uso delas para desenvolver seus estudos sobre partições, assim como diversos outros autores, como Jacobi, Ferrers, Sylvester, Battaglini, Brioschi, Vahlen e outros.

O quarto capítulo trata de triângulos racionais, objeto de vários problemas estudados nos capítulos seguintes. Aqui, Dickson observa que Diophantus sabia que se os lados de um triângulo retângulo são expressos por números racionais, então eles são proporcionais a $2mn$, $m^2 - n^2$, $m^2 + n^2$ e diz-se que o triângulo tem seus lados *formados a partir de dois números m e n* . Pythagoras e Plato já haviam dado casos especiais. Entre os vários problemas sobre triângulos retângulos racionais, abordados por Diophantus, Vieta, Bachet, Girard, Fermat, Frenicle, De Billy, Ozanam, Euler e citados neste trabalho, destacam-se: encontrar n ($n \geq 3$) triângulos retângulos racionais de áreas iguais, ou dois cujas áreas têm um mesmo raio dado. O capítulo seguinte também trata de triângulos racionais, mas aqueles cujos lados e áreas são racionais, e estende os estudos para quadriláteros racionais que têm diagonal racional. Nestes estudos, Dickson cita que Euler, durante o período 1773-1782, escreveu uma série de quatro artigos sobre triângulos, cujos lados e medianas são todos racionais, enquanto Bachet, em 1621, trabalhou com o caso em que uma única mediana é racional ou um único ângulo bissector é racional. Dickson finaliza este capítulo com artigos sobre pirâmides racionais, ângulos triedrais e triângulos esféricos.

Nos capítulos seguintes, Dickson passa a estudar um assunto de grande interesse desta teoria que é a representação de números como soma de n quadrados, citando a história

do seu desenvolvimento. Diophantus já sabia como expressar o produto da soma de dois quadrados como uma soma de dois quadrados de dois modos:

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2.$$

Embora soubesse que nenhum número da forma $4n - 1$ é a soma de dois quadrados, não conseguiu determinar condições para um número ser escrito como soma de dois quadrados, fato que se deve a Girard (em 1625) e a Fermat (alguns anos mais tarde)⁴, que afirmou que todo primo da forma $4n + 1$ é uma soma de dois quadrados. Euler empenhou-se durante sete anos em demonstrar este teorema, apresentando uma prova completa, em 1749, e, ainda, publicou demonstrações mais simples e elegantes, em 1773 e em 1783. Já Legendre, em 1798, e Gauss, em 1801, apresentaram uma expressão para o número de representações de um inteiro como soma de dois quadrados, enquanto que Jacobi, em 1829, deduziu (a partir de séries infinitas para funções elípticas) e provou, aritmeticamente, (junto com Dirichlet, em 1840) uma expressão mais elegante.

Em relação ao problema dos três quadrados, Diophantus afirmou que nenhum número da forma $8m + 7$ é a soma de três quadrados, o que foi provado por Descartes. Já Fermat observou que nenhum número da forma $4^n(8m + 7)$ pode ser escrito como soma de três quadrados⁵. Muitos autores sucederam-se em estudar o problema, como, por exemplo, Hurwitz que, em 1907, obteve uma expressão simples para o número de soluções de $x^2 + y^2 + z^2 = n^2$.

Já Diophantus usou soma de quatro quadrados racionais para expressar os números 5, 13 e 30⁶. Por isso, Bachet e Fermat atribuem-lhe os pré-requisitos para o teorema que afirma que *todo inteiro positivo é a soma de quatro quadrados inteiros*. Este teorema despertou a atenção de Euler (dedicando-lhe cerca de quarenta anos de estudos), que publicou, em 1751, alguns fatos importantes acerca do assunto, incluindo sua fórmula que expressa o produto de duas somas de quatro quadrados como uma soma de quatro quadrados. A primeira demonstração do teorema acima deve-se a Lagrange, em 1772; já no ano seguinte, Euler apresentou uma prova mais simples e elegante do que a de Lagrange; em 1801, Gauss observou que o teorema segue do fato de que qualquer número que tem resto 1, 2, 5 ou 6, quando dividido por 8, é a soma de três quadrados; em 1813, Cauchy mostrou que qualquer número ímpar k é uma soma de quatro quadrados, cujas raízes algébricas são ímpares e estão entre $\sqrt{3k-2} - 1$ e $\sqrt{4k}$. Em 1873, Réalis provou também que todo número $N = 4n + 2$ é uma soma de quatro quadrados, cuja soma de suas raízes algébricas é qualquer um dos números

⁴Fermat também sabia como determinar o número de maneiras possíveis e diferentes que um dado número pode ser escrito como soma de dois quadrados.

⁵Durante muitos anos Euler tentou, em vão, provar este teorema. Do mesmo modo, Legendre também não encontrou demonstração para todos os casos.

⁶Embora não tenha apresentado condições para que um número possa ser escrito como soma de quatro quadrados, ele obteve condições necessárias para representação de um número como soma de dois ou três quadrados.

$0, 2, 4, \dots, 2\mu$, onde μ^2 é o maior quadrado menor que N . Dickson ainda cita alguns artigos de Torelli, Glaisher e Petr sobre o assunto.

Muitos dos artigos mencionados no oitavo capítulo provam a existência de soluções para a congruência $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$, onde a, b e c não são divisíveis pelo primo p . O correspondente problema para o caso de n incógnitas é estudado no décimo capítulo.

No nono capítulo, Dickson dedica-se a artigos elementares que apresentam relações entre quadrados, especialmente sobre n quadrados, cuja soma é um quadrado. Seguindo uma sugestão de Jacobi, Eisenstein afirmou, em 1847, que o número de representações de um número ímpar como uma soma de oito quadrados é igual a 16 vezes a soma dos cubos dos seus divisores. Também apresentou, sem provar, fórmulas que expressam o número de representações de m por 5 ou 7 quadrados, como somas dos símbolos de Legendre-Jacobi de resíduos quadráticos módulo m . Já em 1860-65, Liouville apresentou vários teoremas sobre representação por 10 e 12 quadrados (aparentemente deduzidos de séries de funções elípticas) que foram provados e generalizados por Bell, em 1919, e também foram demonstrados por Humbert e Petr, em 1907, usando funções teta. Em 1867, H.J.S. Smith apresentou resultados gerais sobre representações por 5 e 7 quadrados⁷. Vários estudos sobre representações por cinco quadrados também foram desenvolvidos por Stieltjes, Hermite, Pepin e Hurwitz, assim como Gegenbauer, Boulyguine, Mordell, Hardy e Ramanujan apresentaram trabalhos sobre representação por n quadrados.

O assunto desenvolvido no capítulo onze está intimamente relacionado com os tópicos estudados no nono capítulo. Aqui, Dickson faz um resumo de dezoito artigos publicados por Liouville, em 1858-65, nos quais apresenta resultados (aparentemente obtidos a partir de expansões de funções elípticas) que expressam muitas igualdades entre somas de valores de funções, quando seu argumento envolve os divisores dos dois (ou mais) números cuja soma é dada. Dickson finaliza o capítulo citando artigos que, juntos, provam todas as fórmulas (exceto uma apresentada no sexto artigo), além de provar alguns teoremas relacionados com o tema.

No capítulo doze, Dickson cita mais de trezentos artigos que tratam da solução da equação $ax^2 + bx + c = y^2$ (observando que Diophantus encontrou este tipo de equação em, pelo menos, quarenta dos problemas que estudou) e mostra como obter soluções racionais quando a ou c são quadrados ou quando $b = 0$. Sabe-se que, para encontrar soluções inteiras para esta equação (que constitui um problema bem mais difícil do que encontrar soluções racionais), o hindu Brahmegupta, no século sétimo, tentou fornecer um método, sem muito

⁷Dickson observa que este artigo não era conhecido dos membros da comissão que recomendou o grande prêmio de ciências de 1882, da Academia de Ciências de Paris, para a representação por cinco quadrados: *This paper was unknown to the members of the commission whose recommendation led the Paris Academy of Sciences to propose for its grand prix des sciences mathématiques for 1882 the subject of representation by 5 squares.*

sucesso, que foi melhor esclarecido pelo também hindu Bháscara no século doze⁸. Já Fermat afirmou, em 1657⁹, que uma equação do tipo $x^2 - Ay^2 = 1$, que recebeu o nome de equação *Pelliana*, após ser estudada por John Pell, tem inúmeras soluções inteiras se A é um inteiro positivo que não seja um quadrado e propôs, como um desafio, que os matemáticos ingleses Lord Brouncker e John Wallis encontrassem uma solução para tal equação. Eles obtiveram sucesso em seus estudos e forneceram um método para solucionar a equação¹⁰; porém, não provaram a existência de infinitas soluções. Este teorema é, na realidade, o mais simples e primeiro dos casos conhecidos do teorema geral de Dirichlet, sobre a existência de unidades em qualquer corpo algébrico ou domínio e tem grande importância no estudo da teoria de formas quadráticas binárias. Além disso, o problema de encontrar todas as soluções racionais de equações de segundo grau em duas variáveis reduz-se a achar as soluções de $x^2 - Ay^2 = B$, pois seguem de uma de suas soluções e das soluções de $x^2 - Ay^2 = 1$. Dickson finaliza observando que os mais notáveis trabalhos sobre equações Pellianas se devem a Legendre, Gauss, Dirichlet, Jacobi e Perott.

O capítulo treze trata de equações do segundo grau, incluindo $axy + bx + cy + d = 0$, $x^2 - y^2 = g$, $ax^2 + bxy + cy^2 = dz^2$ e $ax^2 + bxy + cy^2 = d$ e suas formas homogêneas $aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0$. Dickson observa que H.J.S. Smith exibiu um critério para determinar suas soluções inteiras e que Legendre, em 1785, usou o método de Lagrange supracitado para $x^2 - Ay^2 = B$, para provar o teorema que afirma: *se dois dos inteiros a, b, c não têm um fator comum e se nenhum deles é nulo ou divisível por um quadrado, então $ax^2 + by^2 + cz^2 = 0$ tem soluções inteiras não todas nulas se, e só se, $-bc, -ac$ e $-ab$ são resíduos quadráticos de a, b e c , respectivamente, e a, b e c não possuem todos o mesmo sinal*. Já no capítulo catorze, são apresentados vários artigos elementares sobre quadrados em progressões aritméticas ou geométricas, observando que, enquanto existe uma fórmula simples e geral para três quadrados, em progressão aritmética (conhecida por Vieta, Fermat e Frenicle), não existem quatro quadrados distintos que estão em progressão aritmética.

O capítulo dezesseis trata da história de números congruentes, onde um número k se diz congruente se é racional e se existe outro racional x tal que $x^2 + k$ e $x^2 - k$ são quadrados racionais¹¹. Este tópico dominou os manuscritos do século décimo e alguns trabalhos do século onze. Em 1225, Pisano afirmou, mas não provou completamente, que nenhum número

⁸Os gregos já haviam dado aproximações para raízes quadradas que podem ser interpretadas como soluções de $ax^2 + 1 = y^2$ para os casos $a = 2$ ou $a = 3$.

⁹Em 1659, Fermat afirmou possuir uma prova deste fato pelo método decrescente.

¹⁰Em 1765, Euler exibiu este método de uma maneira mais simples, usando frações progressivas de $\sqrt{A}$, mas não provou a existência de infinitas soluções. Este fato foi mostrado por Lagrange que, em 1769-70, apresentou um método direto de encontrar todas as soluções inteiras de $x^2 - Ay^2 = B$ e de uma equação de grau n , desenvolvendo suas raízes em frações progressivas.

¹¹Dickson observa que Diophantus já sabia que $x^2 + y^2 = z^2$ implica em $z^2 \pm 2xy = (x \pm y)^2$, o que torna $2xy$ um número congruente.

congruente é um quadrado, o que implica que a área de um triângulo retângulo racional nunca é um quadrado e que a diferença de dois biquadrados não é um quadrado. Entre os mais importantes autores que estudaram números congruentes, Dickson cita Euler, Genocchi, Woepcke, Collins e Lucas. Os capítulos dezessete e dezoito são dedicados a sistemas ou equações de duas funções quadráticas e três ou mais funções quadráticas, respectivamente.

No capítulo dezenove, Dickson trata do problema de encontrar três inteiros x , y e z tais que $x^2 + y^2$, $x^2 + z^2$ e $y^2 + z^2$ são todos quadrados perfeitos, o que é equivalente a encontrar um paralelepípedo retangular, cujos vértices e diagonais das faces são valores racionais¹² e foram estudados por Euler, Gill e Legendre, entre outros. Já o capítulo vinte estuda soluções para $x^2 + 2 = t^3$, na qual Euler mostrou que cada fator $x \pm \sqrt{-2}$ deve ser o cubo de um número $p + q\sqrt{-2}$, onde p e q são inteiros, e Fermat afirmou que a única solução é $x = 5$.

No capítulo vinte e um, Dickson desenvolve, sobre as equações de Diophantus de grau três (que expressam a diferença entre dois cubos racionais como uma soma de dois cubos racionais positivos), estudo citando cerca de quinhentos artigos. Este problema foi estudado por diversos matemáticos, dentre os quais se destacam Vieta, Girard, Fermat, Euler, Legendre, Binet, Lagrange e Hermite. Já o capítulo seguinte, trata das equações de Diophantus de grau quatro, onde Dickson menciona cerca de quatrocentos artigos. Este assunto também foi estudado por Euler, Fermat e Lagrange, assim como por Leibniz, entre outros.

Dickson declara que o capítulo vinte e três, que trata das equações de Diophantus de grau maior que quatro, é o mais importante deste volume, por relatar trabalhos que oferecem métodos gerais para se resolver equações *diophantinas*, e observa que Lagrange mostrou como usar frações progressivas para resolver $f = c$, quando f é uma forma binária de grau qualquer. Runge e Maillet obtiveram condições para a existência de infinitos pares de soluções inteiras de $f(x, y) = 0$, onde f é um polinômio irreduzível, com coeficientes inteiros. Thue provou que, se $U(x, y)$ é um polinômio homogêneo irreduzível de grau maior que dois e com coeficientes inteiros e se c é uma constante dada, então $U = c$ tem apenas um número finito de pares de soluções inteiras. Maillet forneceu uma generalização para polinômios não-homogêneos U .

Hilbert e Hurwitz, num trabalho conjunto de 1890-91, provaram que qualquer equação homogênea, com coeficientes inteiros, que representa uma curva de *genus* zero pode ser transformada numa equação linear ou quadrática. Poincaré, em 1901, mostrou o mesmo resultado e o estendeu, determinando quando uma curva de *genus* unitário pode ser transformada numa curva de ordem p .

O capítulo seguinte trata de conjuntos de inteiros com somas iguais à soma de suas

¹²Dickson observa que se também acrescentar a hipótese de a diagonal do sólido ser racional, este problema tornar-se-á muito difícil e ainda não havia sido resolvido.

potências (por exemplo, a , b , c e $a + b + c$ têm a mesma soma e a mesma soma de quadrados que $a + b$, $a + c$ e $b + c$), apresentando setenta artigos sobre o assunto.

No capítulo vinte e cinco, Dickson apresenta um exemplo típico da teoria de números, onde um teorema é mostrado facilmente de modo empírico, mas oferece grande dificuldade para se provar matematicamente: Waring, em 1770, anunciou que provou empiricamente, mas fracassou na tentativa de demonstrar, matematicamente, que *todo inteiro positivo é uma soma de no máximo 9 cubos positivos, uma soma de no máximo 19 biquadrados e, em geral, uma soma de um número limitado de m -ésimas potências*. Este último fato foi mostrado por Hilbert, em 1909, embora não tenha determinado o valor preciso do número N_m tal que todo inteiro positivo é uma soma de, no máximo, m -ésimas potências positivas. Mais tarde, Hardy e Littlewood mostraram, usando funções analíticas, que $N_m \leq (m-2)2^{m-1} + 5$, fornecendo 9 cubos, 21 biquadrados, 53 potências quintas etc. Dickson ainda observa que, em alguns trabalhos anteriores, foi provado que todo número racional positivo é uma soma de três cubos racionais e uma soma de quatro cubos positivos racionais.

O capítulo final deste volume fornece uma história condensada do último teorema de Fermat, estudando mais de trezentos trabalhos sobre o assunto. Dickson considera que este teorema em si não é de especial importância para a matemática, mas sua história o é, pois inspirou Kummer, na sua invenção dos números ideais¹³, que é um dos mais importantes ramos da matemática moderna.

C.2.1 Índice do Segundo Volume

TABLE OF CONTENTS

Chapter		Page
I.	POLYGONAL, PYRAMIDAL AND FIGURATE NUMBERS	1
II.	LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	41
	Solution of $ax + by = c$	41
	Solution of $ax \equiv b \pmod{m}$ without Fermat's theorem	54
	Solution of $ax \equiv b \pmod{m}$ by Fermat's or Wilson's theorem	55
	Chinese problem of remainders	57
	Number of positive integral solutions of $ax + by = n$	64
	One linear equation in three unknowns	71

¹³Numa tentativa de provar o último teorema de Fermat, Kummer, em 1843, estendeu as noções de inteiro, primo, fatoração etc; a certos conjuntos chamados *números algébricos* e deu uma prova da validade do teorema. Entretanto, no ano seguinte, Dirichlet apontou um erro na demonstração. Para tentar consertá-la, definiu uma nova classe de números chamados *números ideais*; entretanto, também não conseguiu dar uma prova geral. Mais tarde, Dedekind estendeu a noção de número algébrico e substituiu — na sua teoria — os números ideais de Kummer por certos conjuntos, que chamou também de ideais.

Chapter		Page
	One linear equation in $n > 3$ unknowns	73
	System of linear equation	77
	One linear congruence in two or more unknowns	86
	System of linear congruences	88
	Linear forms, approximation	93
III.	PARTITIONS	101
IV.	RATIONAL RIGHT TRIANGLES	165
	Methods of solving $x^2 + y^2 = z^2$	165
	Sides divisible by 3, 4, or 5	171
	Number of right triangles with a give side	172
	Right triangles of equal area	172
	Right triangles whose areas have a given ratio	174
	Other problems involving only area	175
	Problems involving area and other elements	176
	Right triangles whose legs differ by unity	181
	Difference or sum of legs given	183
	Two right triangles with equal differences of legs, and larger leg of one equal to hypotenuse of the other	184
	Problems involving the sides, but not the area	186
	Right triangles with a rational angle – bisector	188
	Tables of right triangles with integral sides	189
V.	TRIANGLES, QUADRILATERALS, AND TETRAHEDRA	191
	Rational or Heron triangles	191
	Pairs of rational triangles	201
	Triangles whose sides and medians are all rational	202
	Triangles with a rational median and rational sides parallelograms with rational sides and diagonals	205
	Heron triangles with a rational median, Heron parallelograms	207
	Triangles with one or more rational angle – bisectors	209
	Triangles with a linear relation between the angles	213
	Triangles whose area need not be rational	214
	Rational quadrilaterals	216
	Rational inscribed polygons	221
	Rational pyramids and trihedral angles	221
VI.	SUM OF TWO SQUARES	225
VII.	SUM OF THREE SQUARES	259
VIII.	SUM OF FOUR SQUARES	275
IX.	SUM OF n SQUARES	305
	Representation as a sum of 5 or more squares	305
	Relation between squares	318
X.	NUMBER OF SOLUTIONS OF QUADRATIC CONGRUENCES IN n UNKNOWN	325
XI.	LIIOUVILLE'S SERIES OF EIGHTEEN ARTICLES	329
XII.	PELL EQUATION; $ax^2 + bx + c$ MADE A SQUARE	341

Chapter		Page
XIII.	FURTHER SINGLE EQUATIONS OF THE SECOND DEGREE	401
	Equations linear in one unknown	401
	Solution of $x^2 - y^2 = g$	402
	Solution of $ax^2 + bxy + cy^2 = dz^2$	404
	Solution of $ax^2 + by^2 = c$	407
	Solution of $ax^2 + bxy + cy^2 = k$	408
	$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$	402
	$ax^2 + by^2 + cz^2 = 0$ (except $x^2 + y^2 = 2z^2$)	419
	Further single quadratic equations in $n \geq 3$ unknowns	428
XIV.	SQUARES IN ARITHMETICAL OR GEOMETRICAL PROGRESSION	435
	Three squares in arithmetical progression	435
	Four squares in arithmetical progression	440
	Numbers in arithmetical progression all but one being squares	440
	Squares in geometrical progression	441
XV.	TWO OR MORE LINEAR FUNCTIONS MADE SQUARES	443
XVI.	TWO QUADRATIC FUNCTIONS OF ONE OR TWO UNKNOWNNS MADE SQUARES	459
	Congruent numbers; $x^2 \pm k$ both squares	459
	Concordant forms : $x^2 + my^2$, $x^2 + ny^2$ both squares. Related problems	472
	$x^2 + y$ and $x + y^2$ both squares	478
	$x^2 + y - 1$ and $x + y^2 - 1$ both squares	479
	$x^2 + 2fxy + hy^2$ and $x^2 + 2gxy + ky^2$ both squares	480
	Two functions of one unknow made squares	482
	Other pairs of quadratic functions made squares	483
XVII.	SYSTEMS OF TWO EQUATIONS OF DEGREE TWO	485
	Two quadratic equations in two unknowns	485
	Problems of Heron and Planude; generalizations	485
	System $x = 2y^2 - 1$, $x^2 = 2z^2 - 1$	487
	Number and its square both sums of 2 consecutives squares	488
	Miscellaneous systems of two equations	489
XVIII.	THREE OR MORE QUADRATIC FUNCTIONS OF ONE OR TWO UNKNOWNNS MADE SQUARES	491
	$a^2x^2 + dx$, $b^2x^2 + ex$, $\dots$ made squares	491
	Three linear and quadratic functions of x , y made squares	492
	Four quadratic functions of x , y made squares	493
XIX.	SYSTEMS OF THREE OR MORE EQUATIONS OF DEGREE TWO IN THREE OR MORE UNKNOWNNS	497
	$x^2 + y^2$, $x^2 + z^2$, $y^2 + z^2$, all squares	497
	Four squares whose sums by threes are squares	502
	Three squares whose differences are squares	505
	Three squares, sum of any two less third a square	507
	Further sets of three or more linear functions of three or more squares made squares	509
	Quadratic forms in x and y , x and z , y and z , made squares	511
	$xy + a$, $xz + a$, $yz + a$, all squares	513

Chapter	Page
Problems related to the last one	515
Product of any two of 4 or 5 numbers increased by 1 a square	517
Product of any two of 4 numbers increased by n a square	519
Other products of numbers in pairs increased by linear functions made squares	520
Further equations whose quadratic terms are sums of products	522
Squares increased by linear functions made squares	524
Square of each of three numbers plus product of remaining two a square	526
Miscellaneous systems of equations of degree two	527
Rational orthogonal substitutions	530
XX. QUADRATIC FORM MADE AN n TH POWER	533
Binary quadratic form made a cube	533
Binary quadratic form made an n th power	539
$a_1x_1^2 + \dots + a_nx_n^2$ made a cube or higher power	543
XXI. EQUATIONS OF DEGREE THREE	545
Impossibility of $x^3 + y^3 = z^3$	545
Two equal sums of two cubes	550
Three equal sums of two cubes	561
Solutions of $2(z^3 + x^3) = y^3 + t^3$	562
Relations between five or more cubes	563
Sum of three cubes made a square	566
Binary cubic form made a cube	566
Binary cubic form made a square	569
Numbers the sum of two rational cubes : $x^3 + y^3 = Az^3$	572
Sum or difference of two cubes a square	578
Sum of cubes of numbers in arithmetical progression a cube	582
Sum of cubes of numbers in arithmetical progression a square	585
Homogeneous cubic equation $F(x, y, z) = 0$	588
Ternary cubic form made a constant	593
Miscellaneous single equations of degree three	595
Systems of equations of degree three in two unknowns	599
Systems of equations of degree three in three unknowns	602
To find n numbers the cube of whose sum increased (or decreased) by any one of them gives a cube	607
Systems of equations of degree 3 in $n \geq 4$ unknowns	612
XXII. EQUATIONS OF DEGREE FOUR	615
Sum or difference of two biquadrates never a square; area of a rational right triangle never a square	615
$2x^4 - y^4 = \square$ right triangles whose hypotenuse and sum of legs are squares; $x^2 + y^2 = B^4$, $x + y = A^2$. Also, $x^4 - 2y^4 = \square$, $z^4 + 8w^4 = \square$	620
$ax^4 + by^4 = cz^2$	627
$ax^4 + by^4 + dx^2y^2$ made a square	634

Chapter	Page
Quadratci function made a square	639
$A^4 + B^4 = C^4 + D^4$	644
$A^4 + hB^4 = C^4 + hD^4$	647
Sum of three biquadrates never a biquadrate	648
Sum of four or more biquadrates a biquadrate	648
Equal sums of biquadrates	653
Relations involving both biquadrates and squares	657
Miscellaneous single equations of degree four	660
To find n numbers whose sum is a square and sum of squares is a biquadrate	665
Miscellaneous systems of equations of degree four	667
XXIII. EQUATIONS OF DEGREE n	673
Folotion of $f = c$, where f is a binary form	673
Conditions for an infinitude of solutions of $f(x, y) = 0$	674
Rational points on the plane curve $f(x, y, z) = 0$	675
Equations formed from linear functions	677
Product of consecutive integers not an exact power	679
Further proprieties of products of consecutive integers	680
Sum of n th powers an n th power	682
Two equal sums of n th powers	684
Miscellaneous results on sums of like powers	684
Rational solutions of $x^y = y^x$	687
Product of factors $\frac{(x+1)}{x}$ equal to such a fraction	687
Optic formula, $\frac{1}{x_1} + \dots + \frac{1}{x_n} = \frac{1}{a}$	688
Miscellaneous single equations of degree $n > 4$	691
Miscellaneous systems of equations of degree $n > 4$	700
XXIV. STES OF INTEGERS WITH EQUAL SUMS OF LIKE POWERS	705
An equivalent problem in the theory of logarithms	714
XXV. WARING'S PROBLEM AND RELATED RESULTS	717
Waring's problem	717
Numbers expressible as sums of unlike powers	725
Every number a sum of three rational cubes	726
Every positive number a sum of 4 positive rational cubes	727
XXVI. FERMAT'S LAST THEOREM, $ax^r + by^s = cz^t$, AND THE CONGRUENCE	
$x^n + y^n \equiv z^n \pmod{p}$	731
AUTHOR INDEX	777
SUBJECT INDEX	799

C.3 O Terceiro Volume

Publicado em 1923, não é tão extenso quanto os outros. No seu prefácio, Dickson declara que a receptividade dos dois primeiros livros o encorajaram a completar a trilogia,

com aquele que ele considera ser o mais importante da série. No primeiro capítulo, observa que Euler foi o primeiro a publicar, em 1761 e 1763, provas de que todo primo da forma $6n+1$ pode ser representado por $x^2 + 3y^2$ e que todo primo da forma $8n+1$ pode ser escrito como $x^2 + 2y^2$. Fermat, em 1654, apresentou (sem provar) estes e alguns outros teoremas. Em 1773, Lagrange, a partir de sua teoria geral de redução e equivalência de formas quadráticas binárias, provou vários destes resultados. Em 1798, com o auxílio das leis de reciprocidade para resíduos quadráticos, Legendre simplificou e estendeu os métodos de Lagrange (embora sua demonstração não estivesse completa). Em 1801, Gauss introduziu vários conceitos novos e estendeu a teoria em várias direções. Em 1851, Hermite desenvolveu seu método fundamental de redução contínua, que está intimamente relacionado à teoria geométrica introduzida por Smith, em 1876 (cuja aplicação se encontra em funções modulares elípticas), e simplificada por Hurwitz, em 1894, por Klein, em 1890 e 1896 e por Humbert, em 1916 e 1917. Já em 1874, Selling apresentou importantes métodos de redução, tanto para formas definidas quanto indefinidas; em 1880, Poincaré estendeu os métodos de representação dos números $a + b\sqrt{D}$ por pontos e formas e, em 1881 e 1905, construiu invariantes aritméticas transcendentais. Kronecker, em 1883, e Stouff, em 1889, estudaram redução e equivalência sob tipos especiais de substituições.

Já no segundo capítulo, Dickson afirma que Gauss, em *Disquisitiones Arithmeticae*, resolveu $4p = t^2 + 27u^2$ em termos de números originados na teoria de raízes p -ésimas da unidade, com $p = 3m + 1$ primo. Em seus estudos de resíduos biquadráticos e aplicando a teoria de raízes da unidade (*ciclotomia*), Gauss obteve os resíduos módulo p de x, y em $x^2 + y^2 = p$, onde $p = 4k + 1$ é um primo. Como uma aplicação da ciclotomia, Jacobi obteve que se $p = 3n + 1$ é um primo, então $4p = a^2 + 27b^2$; e que se $p = 7n + 1$ é um primo, então $p = L^2 + 7M^2$. Já Stern afirmou (sem provar) que se $p = 6n + 1 = a^2 + 27b^2$ é um primo, então $(n+1)(n+2) \cdots (2n) \equiv -(2n+1)(2n+2) \cdots (3n) \pmod{p}$. Clausen provou esta fórmula e obteve que o sinal correto é negativo se $p \equiv 7 \pmod{12}$ e positivo para $p \equiv 1 \pmod{12}$. Usando os símbolos introduzidos por Jacobi em sua teoria, Cauchy obteve teorema para o caso em que Δ é um inteiro $\equiv 3 \pmod{4}$ não divisível por um quadrado, $p = \Delta n + 1$ é um primo ímpar e a e b percorrem os inteiros menores que Δ e primos com Δ para os quais

$$\left(\frac{a}{\Delta}\right) = +1, \quad \left(\frac{b}{\Delta}\right) = -1,$$

respectivamente. Bachmann mostrou o teorema de Cauchy para o caso em Δ é primo e Pepin provou, por ciclotomia, que se $p = 3\omega + 1$ é um primo, então $4p = x^2 + 3y^2$. Já Oltramare afirmou que todo primo $p = 8m + 3$ pode ser escrito na forma $x^2 + 2y^2$, onde $x \equiv \pm 2^{2m}\psi(m) \pmod{p}$, com $\psi(m) = (m+1) \cdots (2m)/(m!)$; todo primo $p = 6m + 1$ pode ser escrito como $x^2 + 3y^2$, com $x \equiv \pm 2^{m-1}\psi(m)$; e que todo primo $p = 14m + 1$ pode ser representado por $x^2 + 7y^2$, com

$$x \equiv \pm 2^{6m-1} \frac{\psi(2m)\psi(3m)}{\psi(m)} \pmod{p}.$$

Dickson finaliza este capítulo apresentando vários outros resultados acerca da representação de primos.

O capítulo seguinte é dedicado ao estudo de composição de formas quadráticas binárias, começando pela composição de duas formas em duas variáveis $f(x, y) \bullet f'(x', y') = F(X, Y)$, onde X e Y são funções bilineares de x, y e x', y' . Gauss foi o primeiro a estudar o assunto, mas suas provas exigiam longos cálculos. A fim de simplificar este trabalho algébrico, Dirichlet e Dedekind substituíram as formas a serem compostas por formas equivalentes. O hindu Brahmegupta e Euler usaram a composição

$$(x^2 - ey^2)(x'^2 - ey'^2) = X^2 - eY^2, \quad X = xx' \mp eyy', \quad Y = xy' \mp x'y,$$

para encontrar soluções inteiras para $e\xi^2 + 1 = \eta^2$. Gauss estudou o problema de transformar a forma

$$F = AX^2 + 2BXY + CY^2 \tag{C.1}$$

no produto de duas formas

$$f = ax^2 + 2bxy + cy^2, \quad f' = a'x'^2 + 2b'x'y' + c'y'^2 \tag{C.2}$$

através de substituições lineares

$$X = pxx' + p'xy' + p''yx' + p'''yy', \quad Y = qxx' + q'xy' + q''yx' + q'''yy', \tag{C.3}$$

cujos oito coeficientes, assim como os de F , f , e f' , são todos inteiros. Graves provou que se pode expressar o produto das formas $f_1 f_2 f_3$ por f_4 , onde $f_4 = ax_i^2 + bx_i y_i + cy_i^2$. Já Arndt observou que, para encontrar todas as formas F' passíveis de serem transformadas no produto de duas formas dadas f e f' , dada uma forma F composta de f e f' , é necessário apenas encontrar todas as formas F' que contêm F propriamente. Bazin obteve condições necessárias para que a forma (C.1) seja transformada no produto das formas (C.2) através das substituições (C.3). Smith definiu composição de n formas e provou que se F é a composta de $\phi, f_3, \dots, f_n$ e ϕ é a composta de f_1 e f_2 , então F é a composta de $f_1, \dots, f_n$. Dickson finaliza este capítulo com vários resultados acerca de composição de formas quadráticas.

No quarto capítulo, Dickson separa classes de formas quadráticas em ordens e *genus*, através de seus valores de certas invariantes aritméticas, obtendo-se composição de ordens e de *genus* (se compusermos qualquer forma de uma determinada ordem (*genus*) com uma de outra ordem (*genus*), sempre obtemos uma forma de uma única terceira ordem (*genus*)). Aqui, Dickson faz um breve estudo destas composições. No curto capítulo seguinte, Dickson aborda determinantes.

O longo sexto capítulo, escrito por G.H. Cresse (1871-??), é dedicado ao estudo de classes de formas quadráticas binárias com coeficientes inteiros, cujos primeiros trabalhos remetem a Gauss. Este estabeleceu uma relação entre o número h de classes propriamente primitivas de determinante negativo $-D$ e o número de representações próprias de D como soma de três quadrados. Através do estudo de equações modulares elípticas, Kronecker deduziu fórmulas recorrentes para o número de classes. Expandindo os coeficientes em certas funções periódicas, Hermite obteve várias relações do mesmo tipo, cujo método foi estendido por Petr. Já Humbert deduziu todas as relações de Kronecker e apresentou outras do mesmo tipo. Seguindo sugestões de Dedekind, em seus estudos de classes de ideais de corpos quadráticos de discriminante D , Kronecker escolheu a forma representativa $ax^2 + bxy + cy^2$, com b podendo ser par ou ímpar, e considerou como primitivas apenas as formas cujos coeficientes não têm divisor comum. Kronecker simplificou, então, os resultados de Dirichlet e estabeleceu uma relação em termos de funções teta elípticas entre o número de classes de dois discriminantes. Com o auxílio de resíduos quadráticos, Lerch e outros autores reduziram os cálculos do número de classes.

No sétimo capítulo, Dickson ainda estuda formas quadráticas binárias, mas agora aquelas cujos coeficientes são complexos inteiros¹⁴, observando que Dirichlet considerou formas do tipo $(a, b, c) = ax^2 + 2bxy + cy^2$, com a , b e c complexos inteiros, cujo determinante $D = b^2 - ac$ não é o quadrado de um complexo inteiro e estudou formas equivalentes¹⁵. Smith definiu caracteres e *genus* de formas (a, b, c) com coeficientes complexos inteiros — a menos de pequenas alterações, a teoria de composição de formas dada por Gauss (tratada no terceiro capítulo deste volume) aplica-se a formas complexas. Minnigerode estendeu a definição e as propriedades de caracteres e a distribuição de classes em *genus* (dada por Dirichlet e estudada no quarto capítulo) para formas $f = (a, b, c)$ com coeficientes complexos. Bianchi estendeu esta teoria a vários corpos quadráticos imaginários. Já Heine trabalhou com formas quadráticas binárias, cujos coeficientes são polinômios em uma variável. Vários outros autores estudaram este tópico, dentre os quais destacam-se Mathews, Western, Fricke, Klein e Hurwitz. No capítulo seguinte, Dickson realiza um breve estudo acerca do número de classes de formas quadráticas binárias com coeficientes complexos inteiros.

O nono capítulo é dedicado às formas quadráticas em três variáveis. Dickson comenta que Gauss fez um estudo preliminar destas formas como uma mera digressão de suas pesquisas sobre formas em duas variáveis, com o propósito de determinar o número exato do *genus* destas. Seeber foi o primeiro a obter desigualdades envolvendo os coeficientes de uma forma cúbica positiva P , mas seus métodos e provas eram muito complicados. Gauss,

¹⁴Dizemos que $d + ci$ é um complexo inteiro se c e d são inteiros.

¹⁵Aplicando a (a, b, c) uma transformação linear com coeficientes complexos inteiros de determinante ϵ , obtém-se uma forma (a', b', c') de determinante $D' = D\epsilon^2$ e, neste caso, diz-se que a forma (a', b', c') está contida em (a, b, c) . Se vale a inclusão contrária, então $D' = \pm D$ e $\epsilon = \pm 1$ ou $\epsilon = \pm i$. Se $D' = +D$, de modo que $\epsilon = \pm 1$, diz-se que as duas formas são *equivalentes*.

na sua revisão do livro de Seeber, deu uma representação geométrica simples das formas P . Dirichlet trocou o cálculo de Seeber por intuição geométrica, definindo um paralelepípedo correspondente a cada forma P . No mesmo ano, e nos seguintes também, Hermite apresentou teorias aritméticas de redução de formas quadráticas em n variáveis — tanto definidas como indefinidas. Neste meio-tempo, Eisenstein iniciou seus estudos acerca de *genus* e número de classes destas formas e teve pesquisas continuadas por Smith, Meyer, Mordell e Humbert. Já Selling introduziu um novo método de redução, que foi simplificado por Charve, Poincaré e Got. Dickson ainda cita que

“a mais completa exposição da teoria aritmética de formas quadráticas em três ou mais variáveis está em Arithmetik der Quadratischen, de 1898, de Bachmann.”

No décimo capítulo, Dickson estuda formas quadráticas, em quatro variáveis, enquanto que o capítulo seguinte trata das formas quadráticas em n variáveis. Aqui se estudam métodos de redução de formas quadráticas, equivalência entre formas, número de classes, transformações nelas mesmas, caracteres, *genus*, transformações racionais e representação de inteiros ou formas quadráticas por outras formas quadráticas. Entre os autores que pesquisaram acerca do assunto, destacam-se Eisenstein, Jacobi, Hermite, Lebesgue, Smith e Minkowski.

Nos capítulos doze e treze, Dickson estuda formas cúbicas, em duas, três ou mais variáveis, respectivamente, sob a perspectiva de autores como Eisenstein, Hermite, Cayley, Pepin, Mathews, Delaunay, Meyer e outros. Já o capítulo quatorze trata formas de grau maior ou igual a quatro, reportando importantes trabalhos de Eisenstein, Lipschitz, Poincaré, Minkowski e Hermite (para formas decomponíveis).

Nos capítulos quinze e dezesseis, Dickson estuda formas Hermetianas binárias¹⁶ e formas Hermetianas em n variáveis e suas conjugadas, respectivamente. No breve capítulo dezessete, trata de matrizes de formas bilineares e de substituições lineares, citando os trabalhos de Hermite, Smith, Kronecker, Frobenius, Stieltjes e outros.

O capítulo dezoito (que também é bastante curto) é dedicado às representações analíticas de substituições por polinômios módulo p . Aqui, Dickson cita os estudos de Hermite, Betti, Mathieu, Polignac, Lloyd Tanner e dele próprio. Já no capítulo final, trata de covariantes e invariantes modulares, segundo suas próprias pesquisas e de McAtee, Hurwitz,

¹⁶ Considere a forma (estudada por Hermite)

$$f(v, u; v_0, u_0) = Avv_0 + Bvu_0 + B_0v_0u + Cuu_0,$$

onde A e C são reais, B e B_0 são imaginários conjugados e v_0 e u_0 são os conjugados de v e u , respectivamente. A forma f é chamada *forma Hermetiana*.

Sanderson, Glenn e Hazlett; e de redução de formas modulares aos tipos canônicos, seguindo o trabalho de Jordan, Séguier, Wilson e dele mesmo.

Assim como nos outros volumes, Dickson finaliza este livro com um índice de autores nele contido e uma lista de símbolos, usados ao longo dos capítulos.

C.3.1 Índice do Terceiro Volume

TABLE OF CONTENTS

Chapter	Page
I. REDUCTION AND EQUIVALENCE OF BINARY QUADRATIC FORMS, REPRESENTATION ON INTEGERS	1
II. EXPLICIT VALUE OF x, y IN $x^2 + \Delta y^2 = g$	55
III. COMPOSITION OF BINARY QUADRATIC FORMS	60
IV. ORDERS AND GENERA; THEIR COMPOSITION	80
V. IRREGULAR DETERMINANTS	89
VI. NUMBER OF CLASSES OF BINARY QUADRATIC FORMS WITH INTEGRAL COEFFICIENTS	92
VII. BINARY QUADRATIC FORMS WHOSE COEFFICIENTS ARE COMPLEX INTEGERS OR INTEGERS OF A FIELD	198
VIII. NUMBER OF CLASSES OF BINARY QUADRATIC FORMS WITH COMPLEX INTEGRAL COEFFICIENTS	203
IX. TERNARY QUADRATIC FORMS	206
X. QUATERNARY QUADRATIC FORMS	225
XI. QUADRATIC FORMS IN n VARIABLES	234
XII. BINARY CUBIC FORMS	253
XIII. CUBIC FORMS IN THREE OR MORE VARIABLES	259
XIV. FORMS OF DEGREE $n \geq 4$	262
XV. BINARY HERMITIAN FORMS	269
XVI. HERMITIAN FORMS IN n VARIABLES AND THEIR CONJUGATES	279
XVII. BILINEAR FORMS, MATRICES, LINEAR SUBSTITUTIONS	284
XVIII. REPRESENTATION BY POLYNOMIALS MODULO p	289
Analytic Representation of Substitutions, Polynomials Representing All Integers Modulo p	289
Polynomials Representing Only Numbers of Prescribed Nature	291
XIX. CONGRUENCE THEORY OF FORMS	
Modular Invariants and Covariants	293
Reduction of Modular Forms to Canonical Types	298
Formal Modular Invariants and Covariants	299
AUTHOR INDEX	303
SUBJECT INDEX	309

Bibliografia

- [AL1] A.A. Albert, *New Results in the Theory of Normal Division Algebras*, AMS Trans., v. **32**, (1930), pp. 171-185.
- [AL2] A.A. Albert, *Normal Division Algebras Satisfying Mild Assumptions*, Proc. Nat. Acad. Sci., USA, v. **14**, (1928), pp. 904-906.
- [AL3] A.A. Albert, *On the Structure of Normal Division Algebra*, Ann. of Math., s. **2**, v. **30**, (1929), pp. 322-338.
- [AL4] A.A. Albert, *Normal Division Algebras in $4p^2$ Units, p an Odd Prime*, Ann. of Math., s. **2**, v. **30**, (1929), pp. 583-590.
- [AL5] A.A. Albert, *A Determination of All Normal Division Algebra in Sixteen Units*, AMS Trans., v. **31**, (1929), pp. 253-260.
- [AL6] A.A. Albert, *A Note on an Important Theorem on Normal Division Algebras*, AMS Bull., v. **36**, (1930), pp. 567-576.
- [AL7] A.A. Albert, *A Construction of All Non-Commutative Rational Division Algebras of Order Eight*, Ann. of Math., s. **2**, v. **31**, (1930), pp. 567-576.
- [AL8] A.A. Albert, *A Note on Cycle Algebras of Order Sixteen*, AMS Bull., v. **37**, (1931), pp. 727-730.
- [AL9] A.A. Albert, *Division Algebras Over an Algebraic Field*, AMS Bull., v. **37**, (1931), pp. 777-784.
- [AL10] A.A. Albert, *Normal Division Algebras of Order 2^{2m}* , Proc. Nat. Acad. Sci., USA, v. **17**, (1931), pp. 389-392.
- [AL11] A.A. Albert, *Normal Division Algebras of Degree Four Over an Algebraic Field*, AMS Trans., v. **34**, (1932), pp. 363-372.
- [AL12] A.A. Albert, *On Normal Simple Algebras*, AMS Trans., v. **34**, (1932), pp. 620-625.
- [AL13] A.A. Albert, *A Construction of Non-Cyclic Normal Division Algebras*, AMS Bull., v. **38**, (1932), pp. 449-456.
- [AL14] A.A. Albert, *A Note on Normal Division Algebras of Order Sixteen*, AMS Bull., v. **38**, (1932), pp. 703-706.
- [AL15] A.A. Albert, *On Primary Normal Division Algebras of Degree Eight*, AMS Bull., v. **39**, (1933), pp. 265-272.
- [AL16] A.A. Albert, *Non-Cyclic Algebras of Degree and Exponent Four*, AMS Trans., v. **35**, (1933), pp. 112-121.

- [AL17] A.A. Albert, *Leonard Eugene Dickson: 1874 - 1954*, AMS Bull., v. 61, (1955), pp. 331-345.
- [AL18] A.A. Albert, *New Results on Associative Division Algebras*, J. Algebra., v. 5, (1967), pp. 110-132.
- [AM1] A. Amitsur, *On Central Division Algebras*, Isr. J. Math., v. 12, (1972), pp. 408-420.
- [AM1] A. Amitsur, *Division Algebras: A Survey*, Contemporary Math., v. 13, (1982), pp. 3-26.
- [AM2] A. Amitsur, *Highlights in the History of the Finite Dimensional Central Division Algebras*, em L. Rowen *Ring Theory*, em homenagem a A. Amitsur, The Weizmann Science Press of Israel, (1989).
- [AR] E. Artin, *The Influence of J. H. M. Edderburn on the Development of Modern Algebra*, AMS Bull., v. 56, (1950), pp. 65-72.
- [BE] E.T. Bell, *Fifty Years of Algebra in America: 1888-1938*, Semicentennial Addresses of the American Mathematica Society, (1938).
- [BG1] A. Brigaglia, *La Teoria Generale delle Algebre in Italia dal 1919 al 1937*, Riv. Stor. Sci., v. 2, (1984), pp. 199-237.
- [BG2] A. Brigaglia, *Algebra e Geometria (1860-1940):II Contributo Italiano* Supp. ai Rend. Circolo Mat. di Palermo, s. 2, v. 36, (1994), pp. 334-339.
- [BI] G.D. Birkhoff, *Fifty Years of American Mathematics*, Semicentennial Addresses of the American Mathematical Society, (1938).
- [BO] C.B. Boyer, *A History of Mathematics*, John Wiley, New York, (1968).
- [BM] A. Brigaglia and P. Mammone, *Francesco Cecioni and the Construction of Division Algebras*, Rend. Circolo Mat. di Palermo, s. II, v. 36, (1994), pp. 27-46.
- [BS] J.W. Brewer and M.K. Smith, *Emmy Noether - A Tribute to her Life and Work*, Marcel Dekker Inc., (1981).
- [BU] F.F. Burchsted, *Sources for the History of Mathematics in the Archives of American Mathematics*, A Century of Mathematics in America - Part III, (1989).
- [CE1] F. Cecioni, *Sopra un tipo di Algebre prive di divisori dello zero*, Rend. Circolo Mat. di Palermo, v. 47, (1923), pp. 27-254.
- [CE2] F. Cecioni, *Sulla Caratteristica del Prodotto di Due Matrici*, Periodico di Mat., v. 24, (1909), pp. 253-265.
- [CE3] F. Cecioni, *Sulle Algebre Prive di Unità*, Annali di Mat., (1921).
- [CR] R. Cooke and V.F. Rickey, *W. E. Story of Hopkins and Clark*, A Century of Mathematics in America - Part III, (1989).
- [DU] W.L. Duren, Jr, *Graduate Student at Chicago in the Twenties*, AMM, v. 83, (1976), pp. 243-247.
- [EW] S. Epstein and J.H.M. Wedderburn, *On the Structure of Hypercomplex Number Systems*, AMS Trans., v. 6, (1905), pp. 172-178.
- [FE] B. Felfenswalb, *Álgebras de Dimensão Finita*, 12^o Colóquio Brasileiro de Matemática, IMPA, Rio de Janeiro, (1979).
- [HA] H. Halberstein and R.C. Ingram, *The Mathematical Papers of Sir William Rowan Hamilton*, v. III, Cambridge Univ. Press, London, (1967).

- [HAS] H. Hasse, *Theory of Cyclic Algebras over an Algebraic Number Field*, AMS Trans., v. **34**, (1932), pp. 171-214.
- [HAW] T. Hawkins, *Hypercomplex Numbers, Lie Groups and the Creation of Group Representation Theory*, Arch. Hist. Exact. Sci., v. **8**, (1972), pp. 243-287.
- [HI] D. Hilbert, *Fundamentos de La Geometria*, Publicaciones del Instituto "Jorge Juan" de Matematicas, Madrid, (1953).
- [HU1] E.V. Huntington, *A Complete Set of Postulates for the Theory of Absolute Continuous Magnitude*, AMS Trans., v. **3**, (1902), pp. 264-279.
- [HU2] E.V. Huntington, *Simplified Definition of a Group*, AMS Bull., v. **8**, (1902), pp. 296-300.
- [HU3] E.V. Huntington, *A Second Definition of a Group*, AMS Bull., v. **8**, (1902), pp. 388-391.
- [HU4] E.V. Huntington, *Definitions of a Field by Sets of Independent Postulates*, AMS Trans., v. **4**, (1903), pp. 31-37.
- [HU5] E.V. Huntington, *Note on the Definitions of Abstract Groups and Fields by Sets of Independent Postulates*, AMS Trans., v. **6**, (1905), pp. 181-197.
- [HR] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, Springer, (1919).
- [KL] M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, (1972).
- [JA] N. Jacobson, *Abraham Adrian Albert*, AMS Bull., v. **80**, (1974), pp. 1075-1100.
- [LA] S.M. Lane, *Mathematics at the University of Chicago - A Brief History*, A Century of Mathematics in America, Part II, (1989), pp. 127-154.
- [MD] C.C. Mac Duffe, *Algebras's debt to Hamilton*, Scripta Math., v. **10**, (1944)pp. 23-35.
- [ME] U.C. Merzbach, *The Study of the History of Mathematics in America: a Centennial Sketch*, A Century of Mathematics in America - Part III, (1989).
- [ML1] C. Polcino Milies, *A Glance at the Early History of Group Rings*, em Groups, St. Andrews, ed. por C.M. Campbell e E.F., (1981).
- [ML2] C. Polcino Milies, *Breve Introdução à História da Teoria de Anéis*, Atas da 11ª Escola de Álgebra, v. **2**, São Paulo, (1990).
- [MM] R.C.N. Marques e C. Polcino Milies, *Leonard E. Dickson e as Álgebras com Divisão*, Anais do V Seminário Nacional de História da Matemática, (2003), pp.401-409.
- [MO1] E.H. Moore, *A Doubly-Infinite System of Simple Groups*, Math. Papers Read at the Internat. Math. Congress Held in Connection with the World's Columbian Exposition: Chicago, 1893.
- [MO2] E.H. Moore, *A Definition of Abstract Groups*, AMS Trans., v. **3**, (1902), pp. 485-492.
- [MO3] E.H. Moore, *On a Definition of Abstract Groups*, AMS Trans., v. **6**, (1905), pp. 179-180.
- [MS] C. Polcino Milies e S.K. Sehgal, *An Introduction to Groups Rings*, Dodrecht, Kluwer, (2002).
- [OH] P. Ohstrom, *W. R. Hamilton's Views of Algebra as the Science of Pure Time*, Hist. Math., v. **12**, (1985), pp. 45-55.
- [PA1] K.H. Parshal, *Historical Contours of the American Mathematical Research Community*, Anais IV Seminário Nacional de História da Matemática, pp. 42-66.

- [PA2] K.H. Parshal, *In Pursuit of the Finite Division Algebra Theorem and Beyond: Joseph H. M. Wedderburn, Leonard E. Dickson and Oswald Veblen*, Archives Internationales d'Histoire des Sciences, v. 33, (1983), pp. 274-299.
- [PA3] K.H. Parshal, *Eliakin Hastings Moore and the Founding of Mathematical Community in America, 1892-1902*, Annals of Science, v. 41, (1984), pp. 313-333.
- [PA4] K.H. Parshal, *Joseph H. M. Wedderburn and the Structure Theory of Algebras*, Archiv. Hist. Exact Sci., v. 32, (1985), pp. 223-349.
- [PA5] K.H. Parshal, *A Study in Group Theory: Leonard Eugene Dickson's Linear Groups*, The Math. Intelligencer, v. 13, n. 1, (1991), Springer-Verlag New York.
- [PE] G. Peano, *Sul Concetto di Numero*, Rivista di Matematica, v. 1, (1891), pp. 87-102.
- [PR] K.H. Parshal and D.E. Rowe, *American Mathematics Comes of Age: 1875-1900, A Century of Mathematics in America - Part III*, (1989).
- [PE] B. Peirce, *Linear Associative Algebras with Notes and Addenda by C.S. Peirce, Son of the Author*, AJM, v. 4, (1881), pp. 97-229.
- [RE] I. Reiner, *Maximal Orders*, (1975), London - New York - San Francisco: Academic Press.
- [SK] Th. Skolem, *Zu Theorie des Assoziativen Zahlensysteme*, (monografia), Skr. Norsk, Vid-Akad., Oslo 12, s. I, (1927).
- [SZA] G. Scorza, *Corpi Numerici e Algebre*, Casa Editrice Giuseppe Principato, Messina, 1921.
- [VW] O. Veblen and J.H.M. Wedderburn, *Non-Desarguesian and Non-Pascalian Geometries*, AMS Trans., v. 8, (1907), pp. 379-398.
- [WA] B.L. Van der Waerden, *Modern Algebra*, Frederick Ungar Publishing Co., (1931).
- [WA1] B.L. Van der Waerden, *Hamilton's Discovery of Quaternions*, Mathematics Magazine, v. 49, n. 5, (1976), pp. 227-234.
- [WA2] B.L. Van der Waerden, *A History of Algebra*, Springer-Verlag, Berlin Heidelberg New York Tokyo, (1980).
- [WE1] J.H.M. Wedderburn, *A Theorem on Finite Algebras*, AMS Trans., v. 6, (1905), pp. 349-352.
- [WE2] J.H.M. Wedderburn, *A Theorem in Hypercomplex Numbers*, Proc. of Royal Society of Edinburgh, v. 26, (1906).
- [WE3] J.H.M. Wedderburn, *On Hypercomplex Numbers*, LMS Proc., v. 2, s. 6, (1907), pp. 77-118.
- [WE4] J.H.M. Wedderburn, *A Type of Primitive Algebra*, AMS Trans., v. 15, (1914), pp. 162-166.
- [WE5] J.H.M. Wedderburn, *On Division Algebras*, AMS Trans., v. 22, (1921), pp. 129-135.
- [WI] A.T. Winterbourne, *Algebra and Pure Time: Hamilton's Affinity with Kant*, Hist. Math., v. 9, (1982), pp. 195-200.