

UNIVERSIDADE ESTADUAL PAULISTA
Instituto de Geociências e Ciências Exatas
Campus Rio Claro

RESOLUÇÃO DE EQUAÇÕES ALGÉBRICAS POR RADICAIS

César Ricardo P. Martins

Orientador : Prof. Dr. Marcos Vieira Teixeira

Dissertação de Mestrado elaborada
junto ao Programa de Pós-
Graduação em Educação
Matemática, Área de concentração
em Ensino e Aprendizagem da
Matemática e seus Fundamentos
filosóficos-Científicos.

Rio Claro, SP

2006

510.07 Martins, César Ricardo Peon
M386r Resolução de equações algébricas por radicais / César
Ricardo Peon Martins. – Rio Claro : [s.n.], 2006
69 f.

Dissertação (mestrado) – Universidade Estadual Paulista,
Instituto de Geociências e Ciências Exatas
Orientador: Marcos Vieira Teixeira

1. Matemática – Estudo e ensino. 2. Álgebra. I. Título.

Comissão Examinadora

Prof. Dr. Marcos Vieira Teixeira (Orientador)

Prof. Dr. Henrique Lazari

Profa. Dra. Ires Dias

Aluno: César Ricardo Peon Martins

Rio Claro, 13 de Junho de 2006

SUMÁRIO

Índice	i
Resumo	ii
Abstract	iii
Introdução	1
Um Breve Relato da História das Equações Algébricas	6
Resolução de Equações Algébricas por Radicais	30
Conclusão	64
Bibliografia	66
Anexo	69

ÍNDICE

Introdução	1
Capítulo 1. Um Breve Relato da História das Equações Algébricas	6
1.1 Preliminares	6
1.2 As Equações até o Início do Século XII	7
1.3 O Estudo das Equações na Europa Medieval	9
1.4 As Equações Cúbicas e Quárticas	10
1.5 Os Números Imaginários	14
1.6 As Equações Quínticas	19
1.7 As Condições de Solubilidade de Equações por Radicais	24
1.8 O Desenvolvimento da Álgebra após Galois	26
Capítulo 2. Resolução de Equações Algébricas por Radicais	30
2.1 Preliminares	30
2.2 A Equação Geral Cúbica	31
2.3 A Equação Geral do Quarto Grau	36
2.4 Uma Interpretação para o Artigo de Galois	43
2.5 Solução para Equações de Graus Superiores	55
Conclusão	64
Bibliografia	66
Anexo	69

RESUMO

O problema de encontrar as raízes de uma equação algébrica motiva os matemáticos desde a antiguidade. Somente resolvido por completo no início do século XIX, tal problema foi abordado de diferentes modos ao longo da História da Matemática, os quais edificaram o desenvolvimento da teoria que hoje denominamos Álgebra. Nesta dissertação propomos uma reconstrução histórica de uma parte desse desenvolvimento; mais precisamente, do período entre as descobertas, meados do século XVI, das fórmulas para exibir as soluções das equações de 3° e 4° graus e a publicação dos artigos de Evariste Galois em 1846. Em nossa reconstrução destacamos as relações entre as principais idéias de Cardano, Lagrange e Galois, que aparecem em suas tentativas de resolução de uma equação algébrica por radicais. Esta narrativa ainda tem a pretensão de que o material compilado sirva de apoio para um primeiro curso de Álgebra.

ABSTRACT

Finding the roots of an algebraic equation has challenged mathematicians since the beginning of the Mathematics knowledge, and the problem was solved only at the beginning of the 19th century. Different approaches in the search gave rise to development of what is nowadays named Algebra. Here we review a single moment in history that was precisely the middle of the 16th century, when ways to show the solutions of equations of 3rd and 4rd degrees were discovered, and the year 1846 of the publishing of Galois' works. We also point out relations among the main ideas of Cardano, Lagrange and Galois appearing in their attempt to the question. We believe that our material may be helpful in a first course of Algebra.

INTRODUÇÃO

Porque é possível exibir as soluções algébricas de equações gerais de grau menor ou igual a quatro, e o mesmo não pode ocorrer para as equações gerais de graus superiores ? É possível então estudar soluções para casos particulares ?

Essa dissertação tem como primeiro e maior objetivo, abordar a história da busca pelas soluções por radicais de equações algébricas de grau n .

Considerando sua abrangência e o caráter histórico atribuído, queremos fazer uma varredura das principais idéias sobre o tema e seus personagens, até alcançar o trabalho de Evariste Galois (1811-1832), nossa principal figura.

Para tanto, o capítulo I irá trazer um breve relato da História das Equações Algébricas, desde o século XII até o início do século XIX, com a tentativa de mostrar a evolução do tema, descrevendo suas principais passagens históricas com linguagem matemática atual. Alguns reflexos do trabalho de Galois após sua publicação também serão relatados neste capítulo.

Em seguida, no Capítulo II, vamos centrar os esforços na busca das relações entre as principais idéias matemáticas de três momentos desta História, a saber: (i) As descobertas das fórmulas para as soluções das equações gerais do terceiro e quarto graus no século XVI; (ii) A descoberta do resolvente de Lagrange no século XVIII e (iii) A publicação, no século XIX, do artigo “*Sur les conditions de résolubilité des équations par radicaux*” escrito por Evariste Galois em 1831.

O texto contido nesse Capítulo é uma exposição de fontes primária e secundária, que mostra uma das maneiras de se relacionar as três fases destacadas no parágrafo anterior, tendo como referência o texto de Galois.

O segundo objetivo desse trabalho é desenvolver um material de apoio à professores do ensino superior em Álgebra Abstrata. Este objetivo vai se apresentar através da maneira pela qual escrevemos o Capítulo II. Tal escrita

também contém um interesse pedagógico na formação de professores de matemática para o ensino médio e fundamental; professores-alunos que (também) vão começar os estudos em Álgebra Abstrata.

Querendo defender a importância da História da Matemática como recurso pedagógico para a atividade do (futuro) professor, evidenciamos nesse capítulo uma postura que (a) quer sugerir uma visão diferente para matemática abordando o tema proposto por meio da flexibilização do rigor empregado na linguagem desenvolvida atualmente no ensino superior de Álgebra para os cursos de Licenciatura em Matemática e, (b) quer mostrar a preocupação em definir uma maneira de utilizar textos históricos e textos que tratem de assuntos históricos, para introduzir os conceitos matemáticos no ensino superior.

As tentativas de inserir modelos pedagógicos em sala de aula utilizando a História da Matemática começaram a ser elaboradas junto com as discussões iniciais sobre a necessidade de buscar novos caminhos para a Educação e Formação em Matemática.

Aliados a estas tentativas foram enumerados os chamados argumentos desfavoráveis à utilização da História da Matemática como referencial para o ensino da Matemática.

Encontramos tais argumentos listados em Miguel [M1] e também em Favel & Maanen [F1]. O primeiro autor aponta, por exemplo, a ausência de literatura adequada. Fauvel & Maanen afirmam que o elemento histórico pode ser um fator complicador, ou que uma visão distorcida do contexto do passado pode prejudicar uma contextualização no presente, ou ainda que possam ser alegados fatores como falta de tempo para cumprir o programa, falta de recursos, falta de experiência, entre outros.

Em geral, tais contrapontos sempre se relacionam com a função tradicionalmente atribuída para a História da Matemática: ela é a grande fonte de inspiração para futuras descobertas em Matemática (e, portanto, não possui grandes contribuições para a Educação Matemática).

Arboleda [A2] afirma que a História da Matemática não possui nenhum compromisso com o ensino, mas sim com o desenvolvimento da própria Matemática, e esta relação passado/futuro sempre será utilizada por matemáticos, no presente, para a pesquisa e a produção científica em Matemática. Mesmo assim, ele especula possibilidades para a aplicação da História no ensino.

Foram especulações como as de Arboleda que geraram pesquisas para mostrar a existência de algumas características na História que, se bem exploradas, podem se converter em procedimentos para sala de aula.

Fauvel & Maanen [F1] relatam experiências que reforçam uma lista de argumentos favoráveis à utilização da História em sala de aula – lista que pode ser consultada também em Miguel, ou no próprio texto de Fauvel & Maanen.

Para o que pretendemos desenvolver nessa dissertação, o principal entre estes argumentos favoráveis – aquele que iremos defender e que, ao mesmo tempo, contempla a tradicional função da História – é do Desenvolvimento Histórico da Matemática.

A evolução de um determinado conceito, a partir de seu problema gerador, até a organização axiomática de uma dada teoria matemática, pode ser encarada, em nossa opinião, como um modelo a ser seguido para abordagem em sala de aula.

Observamos que a organização axiomática a que nos referimos, somente é posta em prática após tal conceito estar completamente desenvolvido e após todo o significado intuitivo deste conceito ter sido explorado.

E esse processo (histórico) pode ser reconstruído. O que propomos então é o resgate das idéias iniciais de cada teoria anterior, como meta para alcançar o próximo degrau da estrutura desse processo, aplicados em sala de aula.

Entretanto, a reconstrução de desenvolvimentos históricos somente é possível na medida em que temos informações suficientes sobre ele. E quanto maior o volume de informação à nossa disposição sobre o tema em questão, melhor poderá ser esta reconstrução.

Isto é, para viabilizar o uso da História da Matemática em sala de aula, é necessário não somente conhecer o conteúdo matemático a ser desenvolvido, mas também conhecer a História deste conteúdo.

Nobre & Baroni [N1] resumem essas últimas reflexões quando relatam: *“A História da Matemática, assim como a Análise, a Álgebra, a Topologia etc., é uma área do conhecimento matemático, um campo de investigação científica, por isso é ingênuo considerá-la como um simples instrumento metodológico. Dessa forma, é plausível dizer que tanto quanto o conteúdo matemático, há a necessidade de o professor de Matemática conhecer sua história, ou seja: A História do Conteúdo Matemático.”*

Observamos também que a pesquisa em História, por meio de sua evolução, se torna ainda mais legítima para a Educação Matemática, na medida em que podemos, como professores, identificar que algumas das dificuldades surgidas em sala de aula são as mesmas que apareceram no passado, através da abordagem que propomos.

Grabiner [G3] reforça o que acabamos de dizer: *“... a história pode ajudar o professor a compreender a dificuldade inerente a certos conceitos. Um conceito que levou centenas de anos para se desenvolver é provavelmente difícil e as dificuldades históricas bem podem se assemelhar às dificuldades dos estudantes.”*

De fato, em nossa visão, tal reconstrução que parte do intuitivo e ruma para o axiomático vai ao encontro das necessidades do público que queremos atingir, quando apontamos para as dificuldades que nascem em sala de aula, com relação aos objetivos e as habilidades próprias a serem tratadas no nível superior de ensino, no que se refere a Licenciatura em Matemática.

Nossa experiência em sala de aula mostra que o aluno nesse nível de ensino pede um amadurecimento para cumprir as exigências no nível de abstração e rigor para a linguagem matemática que encontramos hoje em qualquer curso de Licenciatura em Matemática. Esse amadurecimento, provavelmente, é o mesmo exigido ao longo do processo histórico de um conceito qualquer.

Esse é o motivo pelo qual nos preocupamos em sugerir um texto que tem o compromisso de privilegiar a flexibilização da linguagem desenvolvida atualmente no ensino superior de álgebra para os cursos de Licenciatura.

Consideramos este processo de amadurecimento do aluno em relação aos objetivos específicos a serem alcançados no ensino superior, fundamental e necessário para a formação do professor de matemática. Logo, não deve ser descartado.

Assim, nossa abordagem histórica tal como esboçada acima se reforça, considerado o trajeto intuitivo-axiomático.

Especificamente, iremos utilizar uma escrita que toma como ponto de partida exemplos numéricos. Dessa forma, o aluno pode, de maneira autônoma e segura, obter generalizações locais ao considerar outros exemplos de mesma natureza, trabalhando com o conceito de uma maneira mais intuitiva.

Daí, gradualmente, esse aluno pode obter resultados gerais próprios desse nível de ensino, isto é, definições e axiomas, juntamente com lemas, proposições e teoremas, e suas respectivas demonstrações.

CAPÍTULO 1

UM BREVE RELATO DA HISTÓRIA DAS EQUAÇÕES ALGÉBRICAS

1.1 PRELIMINARES

Podemos resumir a História das Equações Algébricas como a história da busca de métodos para exibir as soluções de uma dada equação geral de qualquer grau, por meio de radicais.

Exibir as soluções de uma equação dada por meio de radicais (isto é, encontrar as soluções algébricas) significa encontrar estas soluções por meio da manipulação de seus coeficientes através das quatro operações aritméticas e extração de raízes.

Assim, em uma equação geral do segundo grau, vamos manipular seus coeficientes por meio de operações aritméticas e extração da raiz quadrada. Se a equação for de grau três, iremos manipular seus coeficientes pelas operações aritméticas e extração das raízes cúbicas e quadradas.

A mesma idéia está fixada para as equações de grau quatro. Manipulação dos coeficientes por meio das quatro operações aritméticas e extração das raízes quárticas, cúbicas e quadradas.

Para equações de graus superiores a quatro, este procedimento se aplica à casos particulares.

Essa forma de exibir soluções para uma equação foi desenvolvida na Europa, entre os séculos XVI e XIX. Neste capítulo vamos descrever, de maneira geral, os principais conteúdos matemáticos desse período, no que se refere às equações algébricas, bem como apontar seus respectivos personagens, responsáveis por tal desenvolvimento.

1.2 AS EQUAÇÕES ATÉ O INÍCIO DO SÉCULO XII

A procura por métodos para resolver problemas de determinação de incógnitas (isto é, encontrar as soluções algébricas de uma equação) sempre foi de interesse geral para todos os povos desde a antiguidade. Os primeiros registros que temos podem ser datados a partir das civilizações egípcia e mesopotâmica. O papiro de Moscou (≈ 1850 a.C.) e o papiro Rhind (≈ 1650 a.C.) são documentos egípcios que contêm problemas matemáticos, quase todos práticos. Os babilônios usavam plaquetas (ou tabletas) de argila mole, cozidas, grafadas com um estilete. Cerca de 400 das 500.000 plaquetas já encontradas na região mesopotâmica são textos matemáticos, compostos de tábuas e listas de problemas envolvendo o que pode hoje ser chamado de aritmética, álgebra, geometria e matemática financeira. Algumas pertencem ao período em torno do ano 2000 a.C., e a maior parte vai aproximadamente do ano 600 a.C. ao ano 300 a.C.

Os chineses, apesar de isolados por sua posição geográfica, também produziram material desta natureza, e o único registro que temos conhecimento é a versão comentada no ano de 263 por Liu Hui (século III d.C.), da obra *Jiuzhang Suanshu* (“As Nove Seções da Arte da Matemática”) escrita na dinastia Han (206 a.C. – 220 d.C.) em material feito de bambu.

Euclides (*Os Elementos* datado de ≈ 300 a.C.) e principalmente Diofanto de Alexandria (provavelmente século III d.C.) foram os personagens de destaque da matemática grega que desenvolveram trabalhos que se relacionam com as equações algébricas.

As equações algébricas quadráticas têm seu destaque na Índia, através dos trabalhos dos matemáticos Āryabhata (≈ 476), Brahmagupta ($\approx 598-665$), Bhāskara I (século VI) e Bhāskara II (século XII).

Os trabalhos imediatamente posteriores a Bhaskara I sobre o desenvolvimento das equações quadráticas de que temos registro, estão relacionados à matemática árabe. A partir da morte de Maomé em 632 e da

unificação do mundo árabe através da criação de um estado independente, o conhecimento matemático foi ali centralizado pela força de domínio político, que se deu por meio de conquistas territoriais que começaram na Índia e terminaram na Península Ibérica, passando pelo norte da África. Por esse motivo, a transferência do conhecimento matemático hindu para o mundo árabe foi bastante natural.

Segundo Nobre [N3], Muhammad ibn-Musã al-Khwārizmi (780–850) é o principal nome que aparece nesta transição, pois impregna a matemática árabe com métodos hindus, através de seu trabalho “*Kitāb al-jam wal tafriḡ bi hisāb al Hind*” (Livro sobre Adição e Subtração de Acordo com os Hindus).

Sua principal obra é “*Al-kitāb al muhtasar fi hisāb al-jabr wa-l-muqābala*” (Livro Condensado de Cálculos a partir da Transposição Termo a Termo (al-jabr) e Comparação (al-muqābala)). Neste livro, ele apresenta métodos de resolução para seis formas distintas de equações quadráticas, através de exemplos numéricos. Em três destas formas al-Khwārizmi buscou justificativas geométricas para seus exemplos. Apesar de não fazer referência de suas fontes, em dois desses casos tais justificativas são idênticas às apresentadas nos *Elementos* de Euclides.

A iniciativa de justificativa geométrica contida no trabalho de al-Khwārizmi teve continuidade entre os futuros matemáticos da região, com destaque para a figura do egípcio Abu Kāmil Sogā ibn Aslam (≈ 850 –930).

É certo que os contemporâneos de al-Khwārizmi entenderam a necessidade de fundamentar suas soluções de equações nas proposições de Euclides; porém Abu Kāmil o fazia quando julgava conveniente. Ele apresentou um diferencial em seu trabalho ao utilizar de forma corrente os números irracionais para solução de equações. Esta postura, segundo Domingues [D1], teve a sua importância na transmissão dos conhecimentos matemáticos que ainda iria acontecer, desta vez passando do mundo árabe para a Europa medieval.

1.3 O ESTUDO DAS EQUAÇÕES NA EUROPA MEDIEVAL

Como dissemos, talvez o texto de Abu Kâmil, pelo diferencial relatado, tenha sido o mais influente entre os europeus medievais, mesmo que publicado três séculos depois por Leonardo de Pisa (≈ 1170 – 1250), considerado o maior matemático europeu da Idade Média.

Na verdade, o século XII é considerado o século das traduções. Em 1085 os europeus retomaram a cidade de Toledo, considerada um grande centro cultural árabe na Península Ibérica. Esta foi a oportunidade para os estudiosos desse continente providenciarem uma série de traduções de obras clássicas do grego e do árabe para o latim, maneira pela qual a Europa teve acesso (ou retomou) ao conhecimento matemático desenvolvido até então.

De todos aqueles que estudaram matemática e em particular equações algébricas, nos séculos XII e XIII, Leonardo Fibonacci de Pisa foi, de fato, o grande destaque, pois além de grande matemático, teve papel fundamental no processo de transmissão do conhecimento matemático. Filho de um mercador italiano pôde entrar em contato com a matemática árabe, pois se mudou junto com o pai para Bejaia, norte da África. Depois, realizou várias viagens pelo oriente, também como mercador, ampliando e consolidando sua formação.

De retorno a Pisa, escreveu seu principal texto *Liber abaci* (1202, 1228). Foi desta maneira que ocorreu a introdução do sistema hindu-arábico na Europa, que iria substituir o sistema romano.

Utilizando o mesmo tratamento que al-Khwārizmi, ele confirma seu papel de transmissor, ao desenvolver tal estudo por meio de casos particulares de equações quadráticas, através de exemplos próprios, mas também daqueles extraídos do mundo árabe, obviamente todos justificados geometricamente.

Também não acreditava numa solução geral algébrica para equações cúbicas, mas ao manipular números irracionais, mostrou que a equação $x^3 + 2x^2 + 10x = 20$ não possui nenhuma raiz irracional que possa ser escrita nas formas euclidianas $a \pm \sqrt{b}$, $\sqrt{a} \pm \sqrt{b}$, $\sqrt{a \pm \sqrt{b}}$, $\sqrt{\sqrt{a} \pm \sqrt{b}}$, com a , b racionais;

isto é, que nenhuma raiz da equação considerada pode ser obtida por meio de construções com régua (não graduada) e compasso.

A solução geral para as equações quadráticas iria ser consolidada por matemáticos contemporâneos dos árabes, no período posterior à Idade Média na Europa. O Renascimento Europeu teve início na Itália, em 1370, e sua filosofia perdurou até o fim do século XVI. Descobertas significativas no estudo das equações seriam alcançadas em meados do século XIV.

Entretanto, foi o trabalho dos matemáticos do século XV que consolidou o sistema de numeração hindu-arábico e o desenvolvimento da linguagem simbólica para a matemática.

Nicolas Chuquet ($\approx 1445-1500$), médico nascido em Paris, é lembrado pelo texto *Triparty en la science des nombres* (Três partes da Ciência dos Números). Na primeira parte explica o novo sistema de numeração e ensina como efetuar operações aritméticas com a estrutura desse sistema. Na terceira parte, ocupa-se das equações algébricas, onde estaria propenso a aceitar que uma equação possuísse raízes negativas, desprezando as imaginárias.

Luca Pacioli (1445–1509), padre e professor de matemática na Itália, escreveu *Summa de arithmetica, geometrica, proportioni et proportionalita* (Suma de Aritmética, Geometria, Proporções e Proporcionalidade), que foi o primeiro livro de aritmética e álgebra a ser impresso, em 1494. Em seu trabalho utilizou várias abreviações, terminando seu texto afirmando que a possibilidade de solução de uma cúbica genérica era a mesma que a da quadratura do círculo, conjectura que não demoraria a cair.

1.4 AS EQUAÇÕES CÚBICAS E QUÁRTICAS

Considerando que a equação do 2º grau já não mais representava um problema a ser resolvido, a pesquisa dos matemáticos, a partir do século XVI, se volta para equações de grau maior ou igual a 3.

Os procedimentos para a resolução das equações cúbicas $ax^3 + bx^2 + cx + d = 0$ e quárticas $ax^4 + bx^3 + cx^2 + dx + e = 0$ se devem aos italianos algebristas do século XVI. Girolamo Cardano (1501-1576), Niccolò ‘Tartaglia’ Fontana (1500-1557), Scipione Del Ferro (1465-1526) e Ludovico Ferrari (1522 – 1565) foram os principais personagens responsáveis pela descoberta das fórmulas gerais, em meio a disputas, brigas e traições. Elas foram publicadas em 1545 no ARS MAGNA, por Girolamo Cardano.

Segundo Rigatelli [R1], Cardano foi considerado um dos personagens mais extraordinários da História da Matemática. Nasceu em Pávia, era filho ilegítimo de um jurista, vindo sua personalidade a se revelar contraditória e arrebatada. Foi médico, mas paralelamente começou a dedicar-se à matemática. Renunciou à sua cadeira na Universidade de Bolonha, tornou-se astrólogo, inclusive do papa. Segundo Eves [E2], Cardano colocou fim à sua própria vida porque fez previsão do dia de sua morte. Deixou uma vasta obra englobando aritmética, astronomia, física, medicina e outros assuntos; entre estas publicações, a ARS MAGNA.

Como referido acima, ele não estava trabalhando sozinho nas fórmulas gerais da solução por radicais das equações algébricas: Ferrari, Del Ferro e Tartaglia compartilharam de sua descoberta. Em particular, Cardano também foi responsável pelo método que permite eliminar o termo de segundo grau de toda equação cúbica completa.

Nessa época tais matemáticos também analisavam estas equações em casos distintos, pois ainda não utilizavam números negativos, e o zero não era considerado número.

Entre aquelas livres do termo de segundo grau, foram analisadas as seguintes:

$$\begin{cases} ax^3 + c = bx \\ ax^3 = bx + c \end{cases}$$

Tartaglia encontrou as soluções para essas duas últimas equações em 1535, depois que Del Ferro já tinha feito, porém Tartaglia protestou ter encontrado independentemente.

Niccoló ‘Tartaglia’ Fontana quando criança foi ferido no rosto, o que acarretou uma gagueira permanente, que lhe valeu este apelido (gago, em italiano) e Scipione Del Ferro foi professor da Universidade de Bolonha e sua biografia é pouco conhecida. Rigatelli [R1] informa que existem manuscritos atribuídos a Del Ferro, que datam de 1554 à 1558, descobertos por P. Bolognetti da Universidade de Bolonha, onde é feita a referência ao método de resolver equações do tipo $ax^3 + bx = c$.

Antes de morrer, Del Ferro ensinou este seu método a dois discípulos, Annibale della Nave, seu futuro genro e sucessor na cátedra de Bolonha – e Antonio Maria Fior.

Em 1535, houve uma disputa matemática entre Fior e Tartaglia, com um prêmio de trinta banquetes. Frequentes na época, tais confrontos intelectuais podiam garantir, muitas vezes, a permanência de um matemático numa cátedra.

Tartaglia preparou questões variadas, e conseguiu resolver todas as equações propostas por Fior, já com Fior não aconteceu o mesmo, pois teria posse apenas de soluções de equações do tipo $x^3 + ax = b$. Tartaglia renunciou aos banquetes.

A notícia do triunfo de Tartaglia espalhou-se rapidamente, chegando nos ouvidos de Girolamo Cardano, que estava ocupando uma cadeira de medicina na Universidade de Pavia.

Na época da descoberta de Tartaglia, Cardano gozava de boa posição em Milão e o convidou a sua casa, para apresentá-lo ao comandante militar da cidade, uma vez que Tartaglia tinha feito também algumas descobertas sobre tiro e fortificações. Com muita insistência Cardano conseguiu que lhe fosse revelado o segredo da resolução das equações do terceiro grau. Tartaglia consentiu em lhe ensinar a regra de resolução (embora não lhe ensinasse a

demonstração da mesma), sob forma de versos, fazendo Cardano jurar que jamais publicaria este segredo.

Conhecendo o método de resolução, Cardano achou uma demonstração que a justificasse e estimulou seu discípulo Ludovico (Luigi) Ferrari a trabalhar a equação de quarto grau. Ferrari encontrou o correspondente método de resolução para esta equação, com a devida demonstração.

Ferrari, nascido em Bolonha no ano de 1522, chegou à casa de Cardano com quatorze anos para tornar-se um criado. Porém, quando Cardano descobriu que o rapaz sabia ler e escrever, o isentou de tarefas servis, designou-o como seu secretário e decidiu ensinar-lhe matemática.

Ferrari reembolsou seu mestre ajudando-o com seus manuscritos. Com a idade de dezoito anos, tornou-se um conferencista público em geometria, quando Cardano renunciou em seu favor o posto que ocupava na Fundação de Piatti em Milão em 1540.

Seu método, que também foi incluído no ARS MAGNA junto com uma lista de 20 tipos diferentes de equações quárticas, foi ilustrado pela equação $x^4 + x^2 + 36 = 60x$. Tal método consiste em completar os quadrados dos dois lados da equação.

De posse de ambas soluções, Cardano ficou tentado a publicá-las. Daí em 1544, mestre e discípulo realizaram uma viagem à Bologna, onde viram um manuscrito de Del Ferro que continha a famosa regra de Tartaglia (manuscrito este que ainda se conserva, como dito). Ao saber que a fórmula de Tartaglia já existia há trinta anos, Cardano se sentiu à vontade para publicá-la na famosa ARS MAGNA.

Ele não deixou de fazer as devidas atribuições aos respectivos descobridores.

No ARS MAGNA, Cardano analisou todo caso distinto da equação cúbica completa, transformando cada equação em uma sem o termo de segundo grau, dando um exemplo numérico em cada caso, e provando geometricamente a validade das soluções. Ele sempre resolveu os problemas propostos, mesmo quando o resultado implicaria em calcular a raiz de um número negativo, isto é,

um número complexo. “Esqueça a tortura mental que isto representa e faça as contas”.

Esta iniciativa impulsionou a descoberta dos números complexos.

1.5 OS NÚMEROS IMAGINÁRIOS

Rafael Bombelli (1526-1572) foi quem analisou completamente os tipos particulares de equação cúbica, em seu trabalho *Álgebra* (1572).

A partir da descoberta do método para a solução da cúbica por Cardano, os matemáticos buscaram as exatas relações entre os números complexos e as equações algébricas. O trabalho de Bombelli foi o ponto de partida para estabelecer tais relações.

Inicialmente ele fez um exame detalhado do que nós chamamos de o “Campo Numérico” que contém irracionais quadráticos e cúbicos, estabelecendo as leis para as operações aritméticas destes ‘novos’ números, através de vários exemplos. Segundo Katz [K1], parece ser claro que ele desenvolveu estas regras pela analogia às conhecidas regras operatórias dos números naturais.

Em linguagem moderna, vamos ilustrar o procedimento que Bombelli utilizou para a multiplicação e divisão entre pares de complexos, nos seguintes exemplos:

(a) para encontrar o produto $\sqrt[3]{2 + \sqrt{-3}} \cdot \sqrt[3]{2 + \sqrt{-3}}$, ele separa as operações entre a parte real e a imaginária:

$$\left\{ \begin{array}{l} \text{parte real} \\ \left\{ \begin{array}{l} \sqrt{-3} \cdot \sqrt{-3} = -3 \\ 2 \cdot 2 = 4 \end{array} \right. \Rightarrow \sqrt{-3} \cdot \sqrt{-3} + 2 \cdot 2 = -3 + 4 = 1 \\ \\ \text{parte imaginária:} \\ 2 \cdot (2\sqrt{-3}) = 2\sqrt{-12} = \sqrt{-48} \end{array} \right.$$

$$\sqrt[3]{2 + \sqrt{-3}} \cdot \sqrt[3]{2 + \sqrt{-3}} = \sqrt[3]{1 + \sqrt{-48}}$$

(b) para fazer a divisão entre 1000 e $2 + 11\sqrt{-1}$ por exemplo, fez

$$\frac{1000}{2 + 11\sqrt{-1}} \cdot \frac{2 - 11\sqrt{-1}}{2 - 11\sqrt{-1}} = \frac{1000(2 - 11\sqrt{-1})}{125} = 8(2 - 11\sqrt{-1}) = 16 - 88\sqrt{-1}$$

Após estabelecer as regras formais do cálculo para números imaginários, ele verificou que a adição de irracionais quadráticos é suficiente para resolver equações quadráticas, enquanto que a adição de irracionais cúbicos serve para resolver equações cúbicas.

Bombelli mostrou o porque de não existir nenhum número real capaz de representar a raiz quadrada de números negativos, sendo que é necessário adicionar algum outro irracional particular para representar estes números.

Foi por esse caminho que ele buscou a resposta para validar o método de Cardano para uma dada equação cúbica com, pelo menos, uma raiz racional:

Vamos tomar a equação $x^3 = 6x + 40$ como exemplo, onde $x = 4$ é uma das raízes da equação. Pelo método de Cardano temos que $x = \sqrt[3]{20 + \sqrt{392}} + \sqrt[3]{20 - \sqrt{392}}$.

$$\text{Bombelli 'mostra' que } x = \sqrt[3]{20 + \sqrt{392}} + \sqrt[3]{20 - \sqrt{392}} = 4.$$

$$\text{Pondo } \begin{cases} \sqrt[3]{20 - \sqrt{392}} = a - \sqrt{b} & (I) \\ e \\ \sqrt[3]{20 + \sqrt{392}} = a + \sqrt{b} & (II) \end{cases}, \text{ e fazendo } \begin{cases} (I,II) \\ (I)^3 + (II)^3 \end{cases},$$

$$\text{podemos montar o sistema } \begin{cases} a^2 - b = 2 \\ a^3 + 3ab = 20 \end{cases}$$

Bombelli não sabia resolver este sistema. Entretanto notou que o valor de a se encontra entre $a^2 > 2$ e $a^3 < 20$. E o único inteiro que satisfaz tais desigualdades é $a = 2$.

Daí, se $a = 2$ então $b = 2$.

$$\text{Portanto } x = \sqrt[3]{20 + \sqrt{392}} + \sqrt[3]{20 - \sqrt{392}} = (a + \sqrt{b}) + (a - \sqrt{b}) = 4$$

O trabalho de Bombelli, frisamos, foi de grande importância, pois a partir dele, os números complexos começaram a ser utilizados, considerando sua serventia à resolução de equações algébricas. Contudo, as relações entre estes e as soluções de equações algébricas permaneciam pendentes, uma vez que seu procedimento acima não é válido no caso geral.

Na seqüência dos acontecimentos, em particular respeito à notação para tais números, Albert Girard (1595-1632) introduziu o símbolo $\sqrt{-1}$; René Descartes (1596-1650) foi responsável pelo termo *imaginário*. Leonhard Euler (1707-1783) usou i para $\sqrt{-1}$, e Carl Friedrich Gauss (1777-1855) introduziu em 1832 o termo *número complexo*.

Junto com as modificações para sua notação, ocorreram as tentativas geométricas de validação de tais números como campo numérico. Jean Robert Argand (1786-1822) em 1806 e Gauss (1832) foram os principais colaboradores para a compreensão dos complexos através de representação gráfica. Eles são considerados os responsáveis pelo chamado *plano de Gauss-Argand*, útil para visualizar um número complexo, na medida em que podemos associar a

solução única de Cardano-Tartaglia a uma expressão trigonométrica, atualmente chamada de a *forma polar* de um número complexo.

A legitimação dos números complexos não somente seria importante para estabelecer as relações que viabilizam as soluções de equações, como também para sua própria caracterização como campo numérico. Segundo Milies [M3], Bombelli assumiu que a raiz cúbica de um número complexo é outro número complexo. Por conta disto, Milies [M3], embasado em M. Kline, afirma ainda que “no começo do século XVIII, a maioria dos matemáticos acreditava que raízes de diferentes ordens de números complexos levariam a diferentes tipos de complexos”.

Foi, enfim, por meio do famoso resultado de Abraham de Moivre (1667-1754): $(\cos x + i \operatorname{sen} x)^n = \cos nx + i \operatorname{sen} nx$, demonstrado e generalizado por Euler, que a existência de raízes de equações algébricas no campo dos números complexos ficou estabelecida.

Por exemplo, tomando a equação $x^3 - 6x - 4 = 0$, temos que sua raiz pelo método de Cardano é $x = \sqrt[3]{2 + 2\sqrt{-1}} + \sqrt[3]{2 - 2\sqrt{-1}}$.

Segue que, utilizando $v^3 = 2 + 2\sqrt{-1}$ em sua forma polar temos $2 + 2i = \sqrt{8}(\cos \frac{\pi}{4} + i \operatorname{sen} \frac{\pi}{4})$. Isto é, o plano de Gauss-Argand mostra que $\rho = \sqrt{8}$ e $\alpha = \frac{\pi}{4}$.

E por de Moivre
$$v = (\sqrt{8})^{\frac{1}{3}} \left[\cos \left(\frac{\pi}{12} + \frac{2k\pi}{3} \right) + i \operatorname{sen} \left(\frac{\pi}{12} + \frac{2k\pi}{3} \right) \right].$$

analogamente
$$u = (\sqrt{8})^{\frac{1}{3}} \left[\cos \left(\frac{\pi}{12} + \frac{2k\pi}{3} \right) - i \operatorname{sen} \left(\frac{\pi}{12} + \frac{2k\pi}{3} \right) \right],$$

de maneira que
$$x = u + v = 2(\sqrt{2}) \left[\cos \left(\frac{\pi}{12} + \frac{2k\pi}{3} \right) \right]$$

onde, para $k = 0, 3, 6, \dots \Rightarrow v = 2\sqrt{2} \cdot \cos \left(\frac{\pi}{12} \right) \Rightarrow x_1 = 1 + \sqrt{3}$

$$k = 1, 4, 7, \dots \quad \Rightarrow \quad v = 2\sqrt{2} \cdot \cos\left(\frac{\pi}{12} + \frac{2\pi}{3}\right) \quad \Rightarrow \quad x_2 = -2$$

$$k = 2, 5, 8, \dots \quad \Rightarrow \quad v = 2\sqrt{2} \cdot \cos\left(\frac{\pi}{12} + \frac{4\pi}{3}\right) \quad \Rightarrow \quad x_3 = 1 - \sqrt{3}$$

A utilização dos números complexos na resolução das equações algébricas também iria gerar as discussões acerca daquele que seria chamado o Teorema Fundamental da Álgebra:

‘Todo polinômio com coeficientes reais admite ao menos uma raiz complexa’

As várias tentativas em se encontrar as soluções de uma equação algébrica, levaram a idéia de que tais equações podem ser completamente fatoradas em valores lineares reais ou termos quadráticos em x .

A importância deste resultado foi discutida, em primeiro lugar, segundo Katz [K1], por Albert Girard (1595-1632) que produziu tal afirmação sem provar.

Riagatelli [R1] afirma que Etienne Bézout (1730-1783), em 1779 tentou formular uma demonstração sem sucesso; enquanto outros como Jean d’Alembert (1717-1783) em 1746 e Euler, utilizaram variáveis complexas e integrais que eram pouco desenvolvidas.

Com o desenvolvimento do Cálculo de Variáveis Complexas, o primeiro maior contribuinte foi Carl Friedrich Gauss (1777-1855), que produziu quatro provas entre 1799 e 1850. As duas primeiras não eram precisas, mas suas sucessoras, que usaram integrais de variáveis complexas eram mais rigorosas e fixaram o padrão para as provas mais recentes.

1.6 AS EQUAÇÕES QUÍNTICAS

Ao final do século XVI, uma vez que tinham sido encontrados os métodos de resolver as equações gerais cúbicas e quárticas, foi natural aparecer o problema de se resolver a equação geral quártica.

Este método, seguindo os exemplos conhecidos até então, fazia uso de um número finito de operações racionais e extração de raízes nos coeficientes das equações, as chamadas soluções por radicais, ou algébricas. Era costume dos algebristas desse período reexaminar os métodos conhecidos e buscar soluções diferentes das de Cardano e Ferrari para resolver equações cúbicas e quárticas.

Entre eles, podemos destacar o algebrista francês François Viète (1540-1603). Nascido em Fontenay-le Comte se formou advogado e trabalhou para o parlamento da Bretania em Rennes. Quando foi banido destas atividades, por sua postura política de oposição, dedicou-se ao estudo da matemática, e na obra *In artem analyticem isagoge* (1591), construiu seu tratamento às equações algébricas. Porém sua grande contribuição foi dada na evolução do simbolismo algébrico.

Segundo Milies [M3], foi através das leituras dos trabalhos de Diophanto, Cardano, Tartaglia, Bombelli e Simon Stevin (1548-1620), que Viète teve a idéia de utilizar letras para representar quantidades. Ele usava consoantes para representar quantidades conhecidas e vogais para as incógnitas.

Também descobriu um novo método de resolver equações cúbicas e um método particularmente elegante para resolver equações quárticas do tipo $x^4 + 2ax^2 = c - bx$.

E ainda, estabeleceu uma maneira de generalizar o conhecido procedimento para solução da equação quadrática através da fórmula de Cardano.

A procura do método para resolver a equação geral quártica usando radicais tornou-se infrutífera entre tais matemáticos, entretanto conduziu a

alguns resultados interessantes. Entre eles o de Ehrenfried von Tschirnhaus (1651-1708). Este matemático teve lições particulares de matemática enquanto ainda na escola. Entrou na Universidade em 1668 e lá estudou matemática, filosofia e medicina. Durante algum tempo teve o objetivo de obter uma boa posição na Académie Royale des Ciências em Paris.

Tschirnhaus descobriu a transformação que elimina alguns dos termos intermediários de uma equação algébrica, observando que poderia usar esta transformação para desenvolver um algoritmo capaz de reduzir uma equação geral de grau n para uma equação binomial, obviamente de grau n : uma equação na qual contém apenas o termo de grau n e de grau zero, e então resolvidas por radicais.

Entretanto, ele somente conseguiu reduzir a equação cúbica para a forma binomial, e quártica para uma do tipo $ax^4 + bx^2 + c = 0$. Usando estas transformações também demonstrou que uma equação de grau $n > 2$ pode ser reduzida para uma forma onde os coeficientes dos termos de grau $n-1$ e $n-2$ são ambos zero.

Este procedimento foi utilizado pelo inglês George Birch Jerrard (1804-1863), que mostrou que a equação geral de grau $n = 5$, poderia ser reduzida para a forma $x^5 + x + a = 0$. Tal procedimento também foi utilizado em 1786 pelo matemático sueco Erland Samuel Bring (1736-1798) que demonstrou ser possível encontrar uma transformação (por Tschirnhaus) que reduz a equação quártica para a forma $y^5 + py + q = 0$, porém este procedimento não conduz a sua resolução.

A forma $x^5 + x + a = 0$ é a chamada forma de Bring&Jerrard.

Um único método para resolver as equações dos primeiros quatro graus foi proposto por Leonard Euler em 1732. Ele sempre supôs que qualquer equação algébrica de grau n poderia admitir uma redução de seu grau para $n-1$, como acontece de fato com as equações de segundo, terceiro e quarto graus. Então propôs, para as raízes da equação de grau n , a forma $x = \sqrt[n]{A_1} + \sqrt[n]{A_2} + \dots + \sqrt[n]{A_{n-1}}$, onde os A_i são as raízes do chamado resolvente da

equação (expressão construída em função das raízes da equação dada), embora nunca tenha feito os cálculos para $n = 5$.

Foi Joseph Louis Lagrange (1736-1813) quem fez um exame cuidadoso acerca desta questão em seu trabalho *“Réflexions sur la résolution algébrique des équations”*, publicado em 1770.

Segundo Rigatelli [R1], a História normalmente considera Lagrange como um matemático francês, mas há fontes que se referem a ele como um matemático italiano. O pai de Lagrange era o Tesoureiro do Escritório de Trabalhos Públicos e Fortificações em Turim, enquanto sua mãe era a única filha de um médico de Cambiano, perto de Turim. Lagrange era o primogênito de 11 crianças. Seu interesse por matemática começou quando ele leu uma cópia, em 1693, do trabalho de Halley, no uso de álgebra em ótica. Também foi atraído para a física pelo excelente ensino na Faculdade de Turim, mas se decidiu em fazer carreira em matemática. Talvez o mundo da matemática tenha que agradecer à condição financeira de seu pai, pois segundo o próprio Lagrange: – *“Se eu tivesse sido rico, eu provavelmente não teria me dedicado a matemática”*.

Como iremos discutir adiante, em seu referido trabalho ele se fixou em criar equações auxiliares (agora conhecidas como resolvente, mas a qual ele chamou de equações reduzidas), onde as raízes da equação dada seriam expressões racionais de raízes de determinadas equações e das raízes da unidade.

Ele demonstrou que, para uma equação de grau n , o grau da equação resolvente é $n!$, e que para $n = 3$ e 4 , tal expressão racional das raízes pode ser escolhida de forma a construirmos equações resolventes de graus 6 e 24 respectivamente. As propriedades inerentes a essas equações construídas, permitem ainda a redução de seu grau para $n - 1$. Isto é, para grau $n = 3$ e 4 da equação dada, reduzimos o grau da equação resolvente para 2 e 3 respectivamente.

Entretanto, para $n = 5$, o grau de qualquer resolvente suposto por Lagrange $n = 5! = 120$, sempre foi reduzido para 6 ($n + 1$), e não para 4 ($n - 1$)

como ele poderia ter desejado. E por esse motivo, ele ficou inseguro para fazer qualquer outra redução, pois não estava habilitado a provar a não existência de tal resolvente.

Essas reflexões o conduziram a pesquisar um único método de resolver equações dos primeiros quatro graus.

Ele verificou que, para uma dada equação de grau $n \leq 4$, com raízes x_i , com $1 \leq i \leq 4$, temos: $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = (x - x_1)(x - x_2)\dots(x - x_n)$ (1)

de maneira que ao operar o lado direito da igualdade, obtemos:

$$a_n = (-1)^n x_1 x_2 \dots x_n$$

$$a_1 = -(x_1 + x_2 + \dots + x_n)$$

onde a_1 e a_n seriam funções (permutações) das raízes x_1, x_2, \dots, x_n .

Verificando que essas funções não se alteram para quaisquer permutações de x_1, x_2, \dots, x_n , desde que o lado direito de (1) não se altere por tais permutações, Lagrange teria descoberto um novo caminho para a pesquisa de soluções por radicais para equações algébricas de qualquer grau, uma vez que seu trabalho serviu de base para Paolo Ruffini (1765-1822) e Abel (1802-1829) mostrarem a insolubilidade das equações de grau maior ou igual que 5, utilizando o conceito acima de funções simétricas; e para Evariste Galois (1811-1832) desenvolver o trabalho que estabelece as condições de solubilidade para uma equação.

De fato, foi Ruffini quem primeiro destruiu a convicção dos estudiosos de álgebra quando demonstrou em 1799 a não existência de um resolvente que reduzisse o grau de equações de grau 5. Logo, também demonstrou indiretamente que as equações de quinto e maiores graus, não eram solúveis por radicais. Estes resultados estão contidos numa longa memória intitulada *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generale di grado superiore al quarto*.

Rigatelli [R1] afirma que o trabalho de Ruffini mostra de forma implícita, alguns conceitos que Evarist Galois usaria depois. O que mais tarde viria ser

chamado de grupo de permutação, Ruffini chamou apenas de permutação, e a palavra no singular, significava o grupo de todas as permutações para os quais uma função permaneceu inalterada.

Segundo Rigatelli [R1], em seu trabalho *Riflessione intorno allá soluzione delle equazioni algebrache generali* de 1813, Ruffini deu uma demonstração diferente de seu teorema, que aparece nos mais recentes trabalhos da álgebra clássica, chamado a modificação de “Wantzel’ do teorema de Abel, porém esta modificação é dada por Ruffini.

De toda forma, foi de fato o matemático norueguês Niels Abel quem, em 1824 demonstrou a impossibilidade de resolver a equação geral de grau $n \geq 5$ por meio de radicais.

Devido a um de seus professores, Bernt Holmboe, Abel começou a estudar textos de matemática em nível universitário, lendo os trabalhos de Euler, Isaac Newton (1643-1727), Joseph Jérôme Lalande (1732-1807) e Jean D'Alembert (1717-1783). Com a morte de seu pai, ele teve a responsabilidade de apoiar a mãe e família, sem recursos extras que o permitissem completar sua educação escolar e iniciar uma universidade.

Com uma bolsa de estudos permaneceu na escola e pôde entrar na Universidade de Christiania em 1821, formando-se em 1822. Trabalhou na solução das equações quínticas e enviou seu artigo a vários matemáticos inclusive Gauss, o qual pretendia visitar em uma viagem usando uma bolsa do governo norueguês.

Porém, com a reação negativa de Gauss a seu trabalho, decidiu se fixar em Paris. Lá continuou produzindo uma matemática de alta qualidade, porém com sua saúde comprometida. Abel morre sem conseguir um cargo numa universidade, que daria sustento a ele e a sua família.

A importância particular do trabalho de Abel “*Memoire sur une classe particulière d'equations résolubles algébricament*”(1829), está na demonstração de que, nas equações resolúveis por radicais, todas as raízes podiam ser expressas por funções radicais de qualquer outra raiz, e que estas funções eram permutáveis com respeito às quatro operações aritméticas.

1.7 AS CONDIÇÕES DE SOLUBILIDADE DE EQUAÇÕES POR RADICAIS

Evariste Galois, depois de analisar os trabalhos de Lagrange, Ruffini, Cauchy, Abel e Gauss, iria mostrar quais as condições para que uma equação algébrica de grau qualquer possa ser resolvida por meio de radicais.

Estas condições foram estabelecidas em 1831 no trabalho “*Sur les conditions de résolubilité des équations par radicaux*”.

Rebelde na escola, gênio incompreendido pelos colegas e professores e pelos próprios matemáticos de seu tempo, republicano revolucionário perseguido pelo sistema, morreu aos 20 anos em um duelo, durante as tumultuadas tentativas de restauração da monarquia na França, logo após a derrota de Napoleão.

Evariste Galois nasceu em 25 de Outubro de 1811, filho de Nicholas Gabriel Galois e Adelaide Marie Demante. A mãe de Galois foi sua única professora até a idade de 12 anos. Ela lhe ensinou grego, latim e religião. Seu pai era um homem importante na comunidade e 1815 foi eleito o prefeito da cidade Bourg-la-Reine, sua cidade natal.

Em 1823, ingressou no Liceu Louis-le-Grand, em Paris, onde pôde estudar o *Géométrie* de Legendre e os tratados de Lagrange. Em 1828, fez o exame para o ingresso para a principal Universidade de Paris, a École Polytechnique. Entretanto, foi reprovado. Ainda em Louis-le-Grand matriculou-se na classe de matemática de Louis Paul Emile Richard (1795-1849). Esse professor reconheceu o talento de Galois ao entender seu trabalho. Com o apoio de Richard, Galois publica seu primeiro artigo, “*Démonstration d’un théorème sur les fractions continues periodiques*”, em Abril de 1829.

Neste mesmo ano, Galois submeteu sua pesquisa sobre solução de equações algébricas para a Académie des Sciences. Cauchy foi designado revisor deste artigo. Kiernan [K2] afirma que Cauchy teria perdido duas versões deste primeiro trabalho. Entretanto, Belhoste [B2] informa que quando Cauchy

estava pronto para apresentar seu parecer do trabalho, Galois optou por uma revisão desses registros.

No dia 2 de Julho 1829, seu pai cometeu suicídio devido a dificuldades políticas. Galois ficou profundamente afetado pela morte de seu pai e esse fato influenciou fortemente o estilo de vida que iria levar.

Alguns semanas depois da morte de seu pai, Galois apresentou-se para o exame de ingresso para a École Polytechnique e falhou mais uma vez. Ele resignou-se em entrar na École Normale, que era um anexo do Liceu Louis-le-Grand, e fazer os exames de Bacharelado, algo que ele poderia ter evitado entrando na École Polytechnique.

No início de 1830, Galois publica três artigos no principal jornal científico da França daquele tempo, *Bulletin de sciences mathématiques physiques et chimiques*, popularmente conhecido como *Bulletin de Ferussac*. Foram eles: “*Analyse d’un Mémoire sur la résolution algébrique des équations*”, “*Note sur la résolution des équations numériques*” e “*Sur la théorie des nombres*”.

Em fevereiro de 1830 submeteu uma nova versão de suas investigações sobre a solubilidade das equações algébricas à Academia, sendo Jean Baptiste Joseph Fourier designado revisor, que morreu antes de ler tal trabalho. Essa versão também foi perdida.

Em dezembro desse ano, Galois foi expulso da École Normale por divergências políticas com o diretor da instituição. No mesmo período, ele submete uma nova versão de suas investigações à Academia. Somente em julho de 1831, foi deliberado o parecer. Assinado por Lacroix e Poisson, o trabalho foi rejeitado por falta de clareza nos argumentos.

A partir de Maio de 1831, Galois foi preso duas vezes por confrontos políticos com a polícia e permaneceu na prisão até Março de 1832. Em Maio desse ano, Galois foi desafiado para um duelo, o qual não saiu vencedor e veio a falecer na manhã seguinte.

Galois é considerado o fundador da Álgebra Moderna, pois foi o primeiro a introduzir a condição abstrata de associar objetos a outros que possuem completamente ou em parte, a propriedade que o primeiro quer

estudar. Isto fica claro em seu artigo, pois ele expressou a condição de resolução por radicais em termos das propriedades do que ele definiu como *grupo e grupo parcial* das permutações das raízes da equação dada.

Ele também foi o primeiro a expressar claramente a idéia de grupo de permutações, fechado em relação a uma operação, pois em suas memórias afirmou que: “*Quando queremos agrupar algumas permutações levaremos tudo para uma permutação simples ... se em tal grupo há permutações S e T , haverá também a permutação ST* ”.

Este método de investigação – associar objetos de várias ordens a outros que traduzem, completamente ou em parte, a propriedade que o primeiro quer estudar – é típico da álgebra moderna.

Galois usou, sem definir, conceitos atualmente chamados de grupo de permutação, subgrupo, sub-grupo normal, grupo quociente e a idéia de Estrutura de Corpo.

1.8 O DESENVOLVIMENTO DA ÁLGEBRA APÓS GALOIS

A publicação e o conseqüente reconhecimento dos trabalhos e das idéias de Galois ocorreram por meio das edições de Outubro e Novembro de 1846 no *Journal de Mathématique pures et appliquées*, de Joseph Liouville (1809-1882), quinze anos após a sua morte. Esta demora se deve, em parte, pelos sucessivos pareceres desfavoráveis da Academia Francesa de Ciências a estes trabalhos, pois, como já dissemos, seus principais revisores Sylvestre François Lacroix (1765-1843) e Siméon Denis Poisson (1781-1840) não encontraram clareza nas afirmações e demonstrações apresentadas. Para eles seu trabalho era mera repetição do de Abel.

Ainda vivo nesta ocasião, Galois afirmou que o trabalho de Abel era mais restrito que o seu, e que sua idéia era fazer um trabalho enxuto, com o mínimo necessário para o entendimento da leitura, sem repetições de definições e de demonstrações de teoremas já conhecidos.

Na realidade, seu trabalho estava em contraste com o de Abel por ter um espírito mais abstrato e por não ser extremamente computacional, maneira pela qual se lidava com a matemática nesta época.

O primeiro texto publicado sobre os trabalhos de Galois foi o de Enrico Betti (1823-1892) em 1852: “*Sulla risoluzione delle equazioni algebriche*”, único avanço na Teoria de Galois até 1870. Betti trabalhou as noções de subgrupo normal e grupo quociente.

Arthur Cayley publica em Janeiro de 1854, “*On the Theory of Groups, as depending on the symbolic Equation $\theta^n = 1$* ”, que aborda pela primeira vez o conceito abstrato de grupo junto com as idéias de grupos conjugados e subgrupos normais, colaborando assim para o desenvolvimento da Teoria de Grupos.

Joseph Alfred Serret (1819-1885), contribuiu para o desenvolvimento da notação das Teorias de Galois e de Grupo. Seu pupilo, Camille Jordan (1838-1922), publica em 1870 o *Traité des substitutions et des équations algébriques*. Segundo Kiernan, Jordan foi o primeiro algebrista a obter uma formulação original da Teoria de Galois, apresentando o conceito de torre de grupos (o grupo da equação é gerado por uma seqüência ordenada de permutações tal que, para cada permutação na seqüência, a última potência positiva da permutação que está no grupo gerado por todas as permutações precedentes tem expoente primo).

Quase que em paralelo ao desenvolvimento abstrato do conceito de Grupo, Richard Dedekind (1831-1916) introduziu o conceito de Corpo: “Qualquer sistema real ou complexo que satisfaz a propriedade fundamental do fechamento será chamado Corpo”.

Dedekind publica seus resultados no *Zahlentheorie*, em sociedade com Peter Gustav Lejeune Dirichlet (1805-1859), nas edições de 1863, 1871, 1879 e 1894, apresentando desenvolvimentos significativos em teoria dos números, teoria dos ideais e teoria de corpos finitos. Na edição de 1894, desenvolve a teoria de extensão de corpos, isto é, Dedekind faz referência a Galois no

conceito de adjunção de elementos para o conjunto de coeficientes de uma equação.

Com uma linha de pensamento matemático diferente, Leopold Kronecker (1823-1891) introduz o conceito *Domínio de Racionalidade*, apresentado em seu trabalho de 1882, “*Grundzüge einer arithmetischen Theorie der algebraischen Größen*”, onde mostra que toda raiz de uma equação algébrica irredutível sobre o domínio de racionalidade pertence a uma extensão algébrica criada pela adjunção. Isto é, qualquer expressão algébrica que represente uma das raízes da equação dada pode ser adjuntada para o domínio, criando um novo domínio de racionalidade.

Enquanto Kronecker estava preocupado com os elementos que formam um corpo, Dedekind estudou as propriedades dos conjuntos de tais elementos, e de certa forma a definição de extensão algébrica de Dedekind coincide com a definição de domínio de integridade de Kronecker.

Com o conceito de extensão, é Dedekind que desenvolve a idéia de isomorfismo e automorfismo de corpos, que iriam gerar os conceitos de dependência e independência linear, base e gerador e espaço vetorial, associando o número de elementos da base do espaço vetorial (dimensão) ao grau da equação dada (ao grau da extensão). Estas idéias seriam utilizadas por Emil Artin (1898-1962) em sua reformulação da Teoria de Galois. Para Dedekind estas idéias eram óbvias e, portanto ele não as provou. Artin publica *Foundations of Galois Theory* em 1938 e *Galois Theory* em 1942 com uma abordagem quase idêntica a de Dedekind, completa aquela exposição.

Um pouco antes, no final do século XIX, uma moderna exposição da Teoria de Galois foi produzida por Heinrich Weber (1842-1913) em dois artigos: “*Die allgemeinen Grundlagen der Galois’schen Gleichungstheorie*” de 1893 e “*Lehrbuch der Algebra*” de 1895.

Utilizando os conceitos de corpo de Dedekind, desenvolve a teoria sem referência a qualquer interpretação numérica dos elementos usados, isto é, assumindo uma abstração total e definindo o conceito de Grupo por meio de

elementos que são “*coisas*” (*Digen*), de forma que grupos de permutação e grupos finitos, em geral, são casos especiais, particulares.

Segundo Kiernan, o desenvolvimento de Weber é certamente o primeiro tratamento moderno da Teoria de Galois, pois não está restrito ao corpo dos racionais, mas a um corpo arbitrário. Preocupada somente com as extensões e os grupos de automorfismos dessas extensões, estuda a natureza da solução e deixando em segundo plano o processo de solução.

Estes trabalhos estavam a frente de seu tempo e podem ser considerados como antecessores do trabalho de Artin, 40 anos mais tarde, último tratamento desta Teoria.

CAPÍTULO 2

RESOLUÇÃO DE EQUAÇÕES ALGÉBRICAS POR RADICAIS

2.1 PRELIMINARES

O objetivo nesse capítulo é mostrar nossa análise do artigo de Evariste Galois (1811-1832), *Mémoire sur les conditions de résolubilité des équations par radicaux*, levando em consideração as relações existentes entre as principais idéias matemáticas levantadas por Joseph Lagrange (1736-1813), no que diz respeito a solubilidade de equações algébricas por meio de radicais.

Como ponto de partida, exibimos por meio de exemplos numéricos os métodos de Gerolamo Cardano (1501-1576) e Ludovico Ferrari (1522-1565) para a resolução das equações cúbicas e quárticas respectivamente, estendendo tal análise para equações algébricas de graus superiores, dentro da abordagem proposta na introdução deste trabalho. Como iremos mostrar, a idéia central nestes métodos é trocar a equação dada de grau n para uma equação equivalente, de grau $n-1$. Se soubermos resolver essa nova equação nosso problema estará resolvido. Se não, é necessário obter sucessivas reduções dos graus, até onde for necessário.

Em cada passagem destes métodos, vamos identificar os principais elementos do trabalho de Lagrange (entre eles, o resolvente da equação). Logo após, a partir dos conceitos definidos por Lagrange, explicitamos as idéias de Galois, com o objetivo de responder as questões propostas.

O artigo de Galois será nossa principal fonte de análise, e os textos de Victor Katz [K1], Harold M. Edwards [E1], serão as referências para os trabalhos dos outros personagens aqui citados.

Os termos permutação e substituição, utilizados em nossa escrita, são os que estão presentes no trabalho de Galois, e o resolvente de Lagrange utilizado é o mesmo sugerido em Edwards [E1].

2.2 A EQUAÇÃO GERAL CÚBICA

Considere a cúbica $x^3 - 3x^2 + 39x + 55 = 0$.

Vamos obter sua transformada tomando $x = y + h$ num primeiro momento, e depois, fazendo $h = 1$.

Com isto, obtemos $y^3 + 36y + 92 = 0$.

Se $y = u + v$,

$$\begin{cases} y^3 = -36(u+v) - 92 \\ y^3 = u^3 + v^3 + 3uv(u+v) \end{cases} \quad \text{e tomando - se} \quad \begin{cases} u^3 + v^3 = -92 \\ \text{e} \\ uv = -12 \end{cases}$$

$$\text{obtemos} \quad u = -\frac{12}{v} \quad \Rightarrow \quad \left(-\frac{12}{v}\right)^3 + v^3 = -92$$

$$\Leftrightarrow v^6 + 92v^3 - 1728 = 0 \quad \underset{(z=v^3)}{\Rightarrow} \quad z^2 + 92z - 1728 = 0, \quad \text{obtemos} \quad \begin{cases} z = -108 \\ z = 16 \end{cases}$$

logo,

$$\begin{cases} v^3 = -108 & \text{e} & u^3 = 16 \\ & \text{ou} & \\ v^3 = 16 & \text{e} & u^3 = -108 \end{cases} \quad \therefore \quad y = 2\sqrt[3]{2} - 3\sqrt[3]{4} \quad \text{e} \quad \therefore \quad x_1 = 1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}$$

Observe que a escolha dos valores u e v é arbitrária, pois eles assumem valores simétricos.

Esse método, de maneira geral, é a contribuição de Cardano/Tartaglia para a solução das cúbicas. Sua idéia geral é reduzir o grau da equação. Isto é, se a equação dada for de grau 3, precisamos reduzi-lo para grau 2.

Mas, a importância do *Ars Magna* também se encontra nas dúvidas e discussões geradas posteriormente à sua publicação.

Por exemplo, em cúbicas como $x^3 - 6x - 4 = 0$, o método de Cardano/Tartaglia apresenta a solução $x = \sqrt[3]{2 + 2\sqrt{-1}} + \sqrt[3]{2 - 2\sqrt{-1}}$.

Uma pergunta natural seria: porque a única solução inteira desta equação, $x = -2$, não está explicitada por este método ?

Uma cúbica possui três soluções. De que maneira se apresentam as outras duas ? Qual o papel dos números negativos e imaginários, não utilizados e fundamentados naquela época ?

Entre esses questionamentos, queremos discutir a maneira pela qual podemos encontrar as outras duas soluções de uma cúbica, considerando o método acima exposto. Este foi um dos esforços de Lagrange.

Observe na resolução (ou procedimento) acima que se $v^3 = -108$, então $v = \sqrt[3]{-108} = \sqrt[3]{-108\alpha^3}$, desde que $\alpha^3 = 1$.

Se interpretarmos α como a raiz complexa da unidade, isto é, α é raiz da equação $x^3 - 1 = 0$, temos que $v = \alpha \sqrt[3]{-108}$, e também $v = \alpha^2 \sqrt[3]{-108}$, pois $v = \sqrt[3]{-108\alpha^6} = \alpha^2 \sqrt[3]{-108}$, onde $\alpha^6 = (\alpha^3)^2 = 1$.

Dessa maneira, as raízes $1, \alpha, \alpha^2$ da equação auxiliar $x^3 - 1 = 0$, nos dão a opção de substituir os valores $v = \sqrt[3]{-108}$ e $u = \sqrt[3]{16}$ por $v = \alpha \sqrt[3]{-108}$, ou $v = \alpha^2 \sqrt[3]{-108}$ e por $u = \alpha \sqrt[3]{16}$, ou $u = \alpha^2 \sqrt[3]{16}$ respectivamente, desde que a condição $uv = -12$ seja satisfeita, naquele procedimento.

Isto é, ao fazer o que chamamos a adjunção das raízes da unidade aos valores $v = \sqrt[3]{-108}$ e $u = \sqrt[3]{16}$, é necessário que $uv = -12$.

Temos nove possibilidades:

$$u.v = \sqrt[3]{-108} \cdot \sqrt[3]{16} = -12$$

$$u.v = \alpha \sqrt[3]{-108} \cdot \sqrt[3]{16} = -12\alpha$$

$$u.v = \alpha^2 \sqrt[3]{-108} \cdot \sqrt[3]{16} = -12\alpha^2$$

$$u.v = \sqrt[3]{-108} \cdot \alpha \sqrt[3]{16} = -12\alpha$$

$$u.v = \alpha \sqrt[3]{-108} \cdot \alpha \sqrt[3]{16} = -12\alpha^2$$

$$u.v = \alpha^2 \sqrt[3]{-108} \cdot \alpha \sqrt[3]{16} = -12$$

$$u.v = \sqrt[3]{-108} \cdot \alpha^2 \cdot \sqrt[3]{16} = -12\alpha^2$$

$$u.v = \alpha \cdot \sqrt[3]{-108} \cdot \alpha^2 \cdot \sqrt[3]{16} = -12$$

$$u.v = \alpha^2 \cdot \sqrt[3]{-108} \cdot \alpha^2 \cdot \sqrt[3]{16} = -12\alpha^4 = -12\alpha^3 \cdot \alpha = -12\alpha$$

E como estamos interessados nas substituições que fixam o valor do produto entre u e v em -12 , quando substituimos $u = \sqrt[3]{-108}$ por $u = \alpha^2 \cdot \sqrt[3]{-108}$ é necessário que $v = \sqrt[3]{16}$ seja substituído por $v = \alpha \cdot \sqrt[3]{16}$.

Logo, a segunda raiz da equação dada é $x_2 = 1 + 2\alpha \cdot \sqrt[3]{2} - 3\alpha^2 \cdot \sqrt[3]{4}$.

Seguindo o mesmo raciocínio, a terceira raiz da equação é expressa por $x_3 = 1 + 2\alpha^2 \cdot \sqrt[3]{2} - 3\alpha \cdot \sqrt[3]{4}$.

Lembrando a simetria existente entre u e v no método acima, é necessário ressaltar que, por esse motivo, temos duas possibilidades para obter cada uma das três raízes, num total de seis valores. De fato, acima escolhemos $v^3 = -108$ e $u^3 = 16$ para adjuntarmos $\alpha^3 = 1$ em $v = \sqrt[3]{-108}$. Se tomássemos $v^3 = 16$ e $u^3 = -108$ para tal procedimento, iríamos obter as mesmas (três) raízes acima exibidas, num total de seis valores. Este é um ponto importante para a discussão que propomos a seguir.

Veja que as raízes da unidade são cíclicas, isto é $\alpha^3 = 1$, $\alpha^4 = \alpha$, $\alpha^5 = \alpha^2$, $\alpha^6 = 1$, ... Tal característica permitiu a Lagrange considerar quantidades definidas por meio das raízes da equação, como veremos adiante. Ele utilizou a quantidade $t = \frac{1}{3}(x_1 + \alpha \cdot x_2 + \alpha^2 \cdot x_3)$.

Tal como faz Edwards [E1], vamos utilizar, em geral, a quantidade $t = x_1 + \alpha \cdot x_2 + \alpha^2 \cdot x_3 + \dots + \alpha^{n-1} x_n$ onde $x_1, x_2, x_3, \dots, x_n$ são as raízes da equação dada, e $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ são as raízes da unidade, equação auxiliar $x^n - 1 = 0$.

Considere então a quantidade $t = x_1 + \alpha \cdot x_2 + \alpha^2 \cdot x_3$, onde x_1, x_2, x_3 são as raízes de uma equação cúbica. Por meio das permutações das raízes x_1, x_2 e x_3

em t , Lagrange descobriu que a quantidade t , o qual ele chamou o *resolvente* da equação, revela uma maneira diferente de olhar o procedimento descrito acima.

Pelas permutações das raízes x_1 , x_2 e x_3 em t , encontramos seis valores:

$$\begin{aligned} t_1 &= x_1 + \alpha \cdot x_2 + \alpha^2 \cdot x_3 & t_4 &= x_2 + \alpha \cdot x_1 + \alpha^2 \cdot x_3 \\ t_2 &= x_3 + \alpha \cdot x_1 + \alpha^2 \cdot x_2 = \alpha \cdot t_1 & t_5 &= x_3 + \alpha \cdot x_2 + \alpha^2 \cdot x_1 = \alpha \cdot t_4 \\ t_3 &= x_2 + \alpha \cdot x_3 + \alpha^2 \cdot x_1 = \alpha^2 \cdot t_1 & t_6 &= x_1 + \alpha \cdot x_3 + \alpha^2 \cdot x_2 = \alpha^2 \cdot t_4 \end{aligned}$$

Devemos interpretar essas seis quantidades, como as duas possibilidades de obter as três raízes da equação pelo método de Cardano/Tartaglia.

Lagrange elevou a terceira potência cada uma dessas permutações, e os resultados revelaram apenas duas expressões diferentes. Isto é, ele conseguiu, como iremos ver, reduzir o grau da equação dada de três para dois.

Iremos tomar um caminho mais prático para esta redução. De maneira equivalente, vamos fazer as contas com as raízes de nosso exemplo.

Podemos verificar que:

$$\begin{aligned} t_1 &= x_1 + \alpha x_2 + \alpha^2 x_3 \\ &= (1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}) + \alpha(1 + 2\alpha\sqrt[3]{2} - 3\alpha^2\sqrt[3]{4}) + \alpha^2(1 + 2\alpha^2\sqrt[3]{2} - 3\alpha\sqrt[3]{4}) \\ &= (1 + \alpha + \alpha^2) + 2\sqrt[3]{2}(1 + \alpha^2 + \alpha) - 3\sqrt[3]{4}(1 + 1 + 1) = 3 \cdot (-3\sqrt[3]{4}) = 3v \end{aligned}$$

pois $(1 + \alpha + \alpha^2) = 0$,

$$\begin{aligned} t_2 &= x_3 + \alpha \cdot x_1 + \alpha^2 \cdot x_2 \\ &= (1 + 2\alpha^2\sqrt[3]{2} - 3\alpha\sqrt[3]{4}) + \alpha(1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}) + \alpha^2(1 + 2\alpha\sqrt[3]{2} - 3\alpha^2\sqrt[3]{4}) \\ &= (1 + \alpha + \alpha^2) + 2\sqrt[3]{2}(\alpha^2 + \alpha + 1) - 3\sqrt[3]{4}(\alpha + \alpha + \alpha) = 3\alpha \cdot (-3\sqrt[3]{4}) = 3\alpha \cdot v = \alpha \cdot t_1 \end{aligned}$$

$$\begin{aligned} t_3 &= x_2 + \alpha \cdot x_3 + \alpha^2 \cdot x_1 \\ &= (1 + 2\alpha\sqrt[3]{2} - 3\alpha^2\sqrt[3]{4}) + \alpha(1 + 2\alpha^2\sqrt[3]{2} - 3\alpha\sqrt[3]{4}) + \alpha^2(1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}) \\ &= (1 + \alpha + \alpha^2) + 2\sqrt[3]{2}(\alpha + 1 + \alpha^2) - 3\sqrt[3]{4}(\alpha^2 + \alpha^2 + \alpha^2) = 3\alpha^2 \cdot (-3\sqrt[3]{4}) = 3\alpha^2 \cdot v = \alpha^2 \cdot t_1 \end{aligned}$$

$$t_4 = \dots = 3u \quad t_5 = \dots = 3\alpha.u = \alpha.t_4 \quad t_6 = \dots = 3\alpha^2.u = \alpha^2.t_4$$

Essas expressões mostram a relação entre as quantidades t, u, v e as substituições em u, v por $\alpha.u, \alpha^2.u$ e $\alpha.v, \alpha^2.v$, respectivamente.

Devido a isso, podemos estabelecer uma relação entre estes seis valores que t assume através das permutações das raízes, e a equação de sexto grau, resolvente da equação dada, através do procedimento de Cardano:

$$\begin{aligned} \text{se} \quad g(x) &= (x-t_1)(x-t_2)(x-t_3)(x-t_4)(x-t_5)(x-t_6), \\ \text{então} \quad g(x) &= (x-t_1)(x-\alpha.t_1)(x-\alpha^2.t_1)(x-t_4)(x-\alpha.t_4)(x-\alpha^2.t_4) \\ &= (x^3-t_1^3)(x^3-t_4^3) = x^6 - (t_1^3+t_4^3)x^3 + t_1^3.t_4^3 \end{aligned}$$

com isso encontramos a relação entre esta última equação e a equação $v^6 + 92v^3 - 1728 = 0$, resolvente do método de Cardano/Tartaglia (ver pág 34).

$$\text{isto é, } \begin{cases} -\frac{t_1^3+t_4^3}{3^3} = -92 = (u^3+v^3) \\ \frac{t_1^3.t_4^3}{3^3} = 1728 = 12^3 = -(u.v)^3 \end{cases}$$

$$\text{pois } \begin{cases} t_1^3 = (x_1 + \alpha.x_2 + \alpha^2.x_3)^3 = (3v)^3 \\ t_4^3 = (x_2 + \alpha.x_1 + \alpha^2.x_3)^3 = (3u)^3 \end{cases}$$

Portanto, tal como fez Lagrange, descobrimos que apenas duas das quantidades t_i^3 são diferentes. Isto é, reduzimos o grau da equação dada de 3 para 2 por intermédio da equação resolvente.

E essas relações mostram que podemos expressar cada raiz de uma equação cúbica em função delas próprias e de quantidades conhecidas. Assim podemos escrever:

$$x_1 = \frac{1}{3} \left[(x_1 + x_2 + x_3) + \sqrt[3]{t_1^3} + \sqrt[3]{t_4^3} \right]$$

$$x_2 = \frac{1}{3} \left[(x_1 + x_2 + x_3) + \alpha \sqrt[3]{t_2^3} + \alpha^2 \sqrt[3]{t_4^3} \right]$$

$$x_3 = \frac{1}{3} \left[(x_1 + x_2 + x_3) + \alpha^2 \sqrt[3]{t_1^3} + \alpha \sqrt[3]{t_4^3} \right],$$

pois
$$\begin{aligned} x_1 &= \frac{1}{3} \left[(x_1 + x_2 + x_3) + \sqrt[3]{t_1^3} + \sqrt[3]{t_4^3} \right] \\ &= \frac{1}{3} \left[(x_1 + x_2 + x_3) + (x_1 + \alpha x_2 + \alpha^2 x_3) + (x_2 + \alpha x_1 + \alpha^2 x_3) \right] \\ &= \frac{1}{3} \left[3x_1 + (1 + \alpha + \alpha^2)x_2 + (1 + \alpha + \alpha^2)x_3 \right] \end{aligned}$$

onde $1 + \alpha + \alpha^2 = 0$.

Procedemos da mesma maneira para os outros dois valores x_2, x_3 .

2.3 A EQUAÇÃO GERAL DO QUARTO GRAU

Aqui, vamos expor o método de Ferrari para a solução da equação quártica $x^4 + ax^3 + bx^2 + cx + d = 0$.

Para tanto, é necessário eliminar o termo ax^3 . Podemos fazer isso utilizando o mesmo procedimento que eliminou o termo da segunda potência, na solução da cúbica. Ou seja, fazemos $x = y + h$, escolhendo um h conveniente.

Como exemplo, considere a equação $16x^4 - 64x^3 + 72x^2 + 16x - 19 = 0$. Sua reduzida, para $h = 1$, é $16y^4 - 24y^2 + 32y + 21 = 0$.

Essa equação é equivalente a $y^4 - \frac{3}{2}y^2 = -2y - \frac{21}{16}$.

Precisamos completar o quadrado na equação acima, e para isso, vamos inserir a expressão $\gamma \cdot y^2 + \beta$ em ambos os lados da igualdade. Isto é,

$$y^4 - \frac{3}{2}y^2 + \gamma \cdot y^2 + \beta = \gamma \cdot y^2 - 2y + \left(\beta - \frac{21}{16}\right)$$

de tal forma que ela seja equivalente à equação:

$$(y^2 + \sqrt{\beta})^2 = \left(\sqrt{\gamma} \cdot y - \sqrt{\beta - \frac{21}{16}}\right)^2$$

Se conseguirmos isso, reduzimos a equação dada em uma equação do segundo grau.

Para tanto, é necessário que

$$\begin{cases} 2\sqrt{\beta} = \gamma - \frac{3}{2} \\ \sqrt{\gamma \cdot \left(\beta - \frac{21}{16}\right)} = 1 \end{cases}$$

$$\Leftrightarrow \begin{cases} 4\beta = \gamma^2 - 3\gamma + \frac{9}{4} \\ \gamma \cdot \left(\beta - \frac{21}{16}\right) = 1 \end{cases} \Leftrightarrow \begin{cases} \beta = \frac{\gamma^2}{4} - 3\frac{\gamma}{4} + \frac{9}{16} & (I) \\ \gamma \cdot \left(\beta - \frac{21}{16}\right) = 1 & (II) \end{cases}$$

substituindo (I) em (II), expressões do sistema acima, recaímos na cúbica:

$$\gamma \cdot \left(\frac{\gamma^2}{4} - 3\frac{\gamma}{4} + \frac{9}{16} - \frac{21}{16}\right) = 1 \quad \Leftrightarrow \quad \gamma^3 - 3\gamma^2 - 3\gamma - 4 = 0 \quad [1]$$

e se $1, \alpha, \alpha^2$ são as raízes da unidade, as soluções desta cúbica, por

Cardano/Lagrange são:

$$\begin{cases} \gamma_1 = 4 \\ \gamma_2 = 1 + 2\alpha + 2\alpha^2, \\ \gamma_3 = 1 + 2\alpha^2 + 2\alpha \end{cases}$$

utilizando $\gamma_1 = 4 \Rightarrow \sqrt{4\left(\beta - \frac{21}{16}\right)} = 1 \Rightarrow \beta = \frac{25}{16}$

de maneira que $\left(y^2 + \sqrt{\frac{25}{16}}\right)^2 = \left(2y - \sqrt{\frac{4}{16}}\right)^2 \Leftrightarrow y^2 + \frac{5}{4} = \pm\left(2y - \frac{1}{2}\right)$

fornecendo as quatro raízes da equação reduzida:

$$y_{1,2} = \frac{2 \pm \sqrt{-3}}{2}, y_3 = -\frac{1}{2}, y_4 = -\frac{3}{2}$$

Entretanto, se utilizarmos γ_2 ou γ_3 ao invés de γ_1 , quando do cálculo do valor de β , iremos obter as mesmas quatro raízes obtidas acima.

E considerando a simetria em u, v na solução da cúbica $\gamma^3 - 3\gamma^2 - 3\gamma - 4 = 0$, pelo método de Cardano, encontramos as mesmas quatro raízes, por outras três vezes.

Temos assim, seis possibilidades de encontrar as quatro raízes desta equação, em um total de 24 valores.

Por sua vez, Lagrange pôde analisar a resolução da quártica, partindo da mesma idéia que utilizou na análise da cúbica; isto é, utilizando um resolvente para validar o método de solução. Ele utilizou $t = x_1x_2 + x_3x_4$, encontrando 24 valores. Elevando cada um dos 24 valores à quarta potência, encontrou 3 valores diferentes, trocando a equação dada de grau quatro por outra de grau três, equivalente à primeira, por meio do resolvente definido.

Com isto, tal como fez na solução para cúbicas, Lagrange pôde escrever as quatro raízes da quártica em função das quantidades t_i :

$$\begin{aligned}
x_1 &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \sqrt[4]{t_i^4} + \sqrt[4]{t_j^4} + \sqrt[4]{t_k^4} \right] \\
x_2 &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \alpha \sqrt[4]{t_i^4} + \alpha^2 \sqrt[4]{t_j^4} + \alpha^3 \sqrt[4]{t_k^4} \right] \\
x_3 &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \alpha^3 \sqrt[4]{t_i^4} + \alpha \sqrt[4]{t_j^4} + \alpha^2 \sqrt[4]{t_k^4} \right] \\
x_4 &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \alpha^2 \sqrt[4]{t_i^4} + \alpha^3 \sqrt[4]{t_j^4} + \alpha \sqrt[4]{t_k^4} \right]
\end{aligned}$$

Vamos verificar de que maneira conquistamos estes resultados, de modo análogo ao que fizemos para a cúbica na seção anterior. Logo, não é necessário elevar as quantidades t_i , agora, a quarta potência, se construirmos um polinômio g .

Tal como em Edwards [E1], assuma a quantidade:

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4,$$

onde x_1, x_2, x_3, x_4 são as raízes da quártica, que se permutam em t ; e $1, \alpha, \alpha^2, \alpha^3$ são as raízes da equação auxiliar $x^4 - 1 = 0$.

Pondo $\alpha = -1$ no lugar de $\alpha = i$, para utilizar a simetria induzida por essa adjunção, encontraremos vinte e quatro valores,

$$\begin{aligned}
t_1 &= x_1 - x_2 + x_3 - x_4 & t_5 &= x_1 - x_2 + x_4 - x_3 \\
t_2 &= x_4 - x_1 + x_2 - x_3 = -t_1 & t_6 &= x_3 - x_1 + x_2 - x_4 = -t_5 \\
t_3 &= x_3 - x_4 + x_1 - x_2 = t_1 & t_7 &= x_4 - x_3 + x_1 - x_2 = t_5 \\
t_4 &= x_2 - x_3 + x_4 - x_1 = -t_1 & t_8 &= x_2 - x_4 + x_3 - x_1 = -t_5 \\
\\ \\
t_9 &= x_1 - x_3 + x_2 - x_4 & t_{13} &= x_1 - x_3 + x_4 - x_2 \\
t_{10} &= x_4 - x_1 + x_3 - x_2 = -t_9 & t_{14} &= x_2 - x_1 + x_3 - x_4 = -t_{13} \\
t_{11} &= x_2 - x_4 + x_1 - x_3 = t_9 & t_{15} &= x_4 - x_2 + x_1 - x_3 = t_{13} \\
t_{12} &= x_3 - x_2 + x_4 - x_1 = -t_9 & t_{16} &= x_3 - x_4 + x_2 - x_1 = -t_{13}
\end{aligned}$$

$$t_{17} = x_1 - x_4 + x_2 - x_3$$

$$t_{21} = x_1 - x_4 + x_3 - x_2$$

$$t_{18} = x_3 - x_1 + x_4 - x_2 = -t_{17}$$

$$t_{22} = x_2 - x_1 + x_4 - x_3 = -t_{21}$$

$$t_{19} = x_2 - x_3 + x_1 - x_4 = t_{17}$$

$$t_{23} = x_3 - x_2 + x_1 - x_4 = t_{21}$$

$$t_{20} = x_4 - x_2 + x_3 - x_1 = -t_{17}$$

$$t_{24} = x_4 - x_3 + x_2 - x_1 = -t_{21}$$

Esses vinte e quatro valores devem ser interpretados como as seis possibilidades de se encontrar as quatro raízes pelo método acima. Isto se torna mais evidente quando escrevemos o polinômio g para este caso e realizamos as substituições t_i em g , $1 \leq i \leq 24$:

$$\begin{aligned} g(x) &= (x-t_1)(x-t_2)(x-t_3)(x-t_4)(x-t_5)\dots(x-t_{23})(x-t_{24}) \\ &= (x-t_1)(x+t_1)(x-t_1)(x+t_1)(x-t_5)(x+t_5)\dots(x-t_{21})(x+t_{21}) \\ &= (x-t_1)^2 \cdot (x+t_1)^2 \cdot (x-t_5)^2 \cdot (x+t_5)^2 \cdot (x-t_9)^2 \cdot (x+t_9)^2 \cdot \\ &\quad (x-t_{13})^2 \cdot (x+t_{13})^2 \cdot (x-t_{17})^2 \cdot (x+t_{17})^2 \cdot (x-t_{21})^2 \cdot (x+t_{21})^2 \end{aligned}$$

mas $t_1 = t_{21}$, $t_5 = t_{13}$, $t_9 = t_{17}$.

Logo,

$$\begin{aligned} g(x) &= (x-t_1)^4 \cdot (x+t_1)^4 \cdot (x-t_5)^4 \cdot (x+t_5)^4 \cdot (x-t_9)^4 \cdot (x+t_9)^4 \\ &= (x^2 - t_1^2)^4 \cdot (x^2 - t_5^2)^4 \cdot (x^2 - t_9^2)^4 \end{aligned}$$

Observe que, de fato, utilizar $\alpha = -1$ ao invés de $\alpha = i$, é mais prático. Observe ainda que a penúltima expressão equivalente de $g(x)$ mostra as seis possibilidades de encontrarmos as quatro raízes.

Se tomarmos $g(x) = f(x)^4$, definimos então a relação entre a cúbica $\gamma^3 - 3\gamma^2 - 3\gamma - 4 = 0$ [1], equação presente no procedimento de Ferrari, com $f(x) = (x^2 - t_1^2) \cdot (x^2 - t_5^2) \cdot (x^2 - t_9^2)$.

$$\begin{aligned} f(x) &= (x^2 - t_1^2) \cdot (x^2 - t_5^2) \cdot (x^2 - t_9^2) \\ &= x^6 - (t_1^2 + t_5^2 + t_9^2)x^4 + (t_1^2 \cdot t_5^2 + t_1^2 \cdot t_9^2 + t_5^2 \cdot t_9^2)x^2 - (t_1^2 \cdot t_5^2 \cdot t_9^2) \end{aligned}$$

Esse polinômio $f(x)$ é de grau seis, e representa a equação resolvente da cúbica, onde t_1^2, t_5^2, t_9^2 representam suas três soluções, quando tomamos $\gamma = x^2$.

De fato, fazendo $\gamma = x^2$ em $f(x)$, temos

$$f(\gamma) = \gamma^3 - (t_1^2 + t_5^2 + t_9^2)\gamma^2 + (t_1^2 \cdot t_5^2 + t_1^2 \cdot t_9^2 + t_5^2 \cdot t_9^2)\gamma - (t_1^2 \cdot t_5^2 \cdot t_9^2)$$

onde $\gamma_1, \gamma_2, \gamma_3$ são as raízes da equação [1] em função dos t_i .

Isto é, podemos estabelecer uma relação entre as quantidades t_1, t_5, t_9 e os coeficientes de [1]:

$$\begin{cases} t_1^2 + t_5^2 + t_9^2 = 3 \\ t_1^2 \cdot t_5^2 + t_1^2 \cdot t_9^2 + t_5^2 \cdot t_9^2 = -3 \\ t_1^2 \cdot t_5^2 \cdot t_9^2 = 4 \end{cases}$$

Cada função dessa gera uma raiz para a cúbica [1]. E cada raiz de [1] gera as quatro raízes da equação dada (lembramos Ferrari).

Ou seja, conseguimos reduzir o grau da equação dada de quatro para três. Depois vamos reduzir o grau de três para dois. E portanto, essa análise também nos permite definir as raízes da quártica por meio dos valores $\pm t_1, \pm t_5, \pm t_9$,

$$x_1 = \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \sqrt[4]{t_1^4} + \sqrt[4]{t_5^4} + \sqrt[4]{t_9^4} \right]$$

$$x_2 = \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) - \sqrt[4]{t_1^4} - \sqrt[4]{t_5^4} + \sqrt[4]{t_9^4} \right]$$

$$x_3 = \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \sqrt[4]{t_1^4} - \sqrt[4]{t_5^4} - \sqrt[4]{t_9^4} \right]$$

$$x_4 = \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) - \sqrt[4]{t_1^4} + \sqrt[4]{t_5^4} - \sqrt[4]{t_9^4} \right]$$

Se chamarmos as permutações t_i acima de um *grupo* de vinte e quatro permutações das raízes, e chamarmos de um *grupo parcial* cada coluna com 4 permutações $(t_i, t_{i+1}, t_{i+2}, t_{i+3} ; i = 1+k, \dots, 4+k ; k = 0, 4, \dots, 20)$, podemos dizer que cada uma dessas 4 permutações de cada grupo parcial é uma escolha que podemos fazer para obter as raízes x_1, x_2, x_3, x_4 definidas como acima.

De fato, se as quantidades t_i são cíclicas, isto é, se

$$t_1 = \alpha.t_2 = \alpha^2.t_3 = \alpha^3.t_4 = \alpha^4.t_1 = \dots$$

$$t_5 = \alpha.t_6 = \alpha^2.t_7 = \alpha^3.t_8 = \alpha^4.t_5 = \dots$$

$$t_9 = \alpha.t_{10} = \alpha^2.t_{11} = \alpha^3.t_{12} = \alpha^4.t_9 = \dots$$

então podemos optar em tomar qualquer t_i de cada grupo parcial e obter as raízes da equação dada.

Por exemplo, é fácil verificar a possibilidade de utilizar a quantidade t_2 e t_{22} no lugar de t_1 e t_{21} , em $g(x)$:

$$\begin{aligned} g(x) &= (x-t_1)(x-t_2)(x-t_3)(x-t_4)(x-t_5)\dots(x-t_{23})(x-t_{24}) \\ &= (x+t_2)(x-t_2)(x+t_2)(x-t_2)(x-t_5)(x+t_5)\dots(x-t_{21})(x+t_{21}) \end{aligned}$$

E com tais escolhas, iremos escrever as raízes da equação quártica em função de t_2, t_5, t_9 .

Poderíamos também optar em utilizar t_6 ao invés de t_5 , por exemplo. Nesse caso escrevemos as raízes da equação em função de t_1, t_6, t_9 .

De fato, quando representadas em função de t_i, t_{i+4}, t_{i+8} , com i variando como estabelecido acima, as raízes da equação quártica ficam bem definidas, e são chamadas *invariantes* por estas substituições. Isto é, podemos escolher as substituições t_i em $g(x)$, conforme o critério obtido para as permutações acima, que seus valores não serão alterados.

Esta escolha também aparece quando optamos em analisar as soluções pelo procedimento de Ferrari. Ali estaremos fazendo tal escolha quando utilizamos γ_1, γ_2 ou γ_3 . Lembremos que podemos obter as mesmas quatro raízes utilizando qualquer γ naquele procedimento.

Se retornarmos à discussão da resolução das cúbicas, vamos notar que esta escolha também ocorre em Cardano e Lagrange quando optamos em usar um dos valores atribuídos para u ou para v , devido a simetria existente entre tais valores.

A idéia de construção de grupos e grupos parciais foi introduzida, na realidade, por Galois em seu artigo já mencionado, *Mémoire sur les conditions de résolubilité des équations par radicaux*. Neste trabalho ele estabelece as propriedades que regem a construção dos grupos, estabelecendo as condições de solubilidade por radicais para uma equação algébrica.

2.4 UMA INTERPRETAÇÃO PARA O ARTIGO DE GALOIS

Nessa seção apresentaremos os conceitos propostos por Galois contidos no artigo *Mémoire sur les conditions de résolubilité des équations par radicaux*.

Nosso maior objetivo é o de estabelecer relações destes conceitos com as idéias de Lagrange, associando os polinômios g e f , introduzidos por Lagrange e descritos nas seções anteriores para as análises das soluções das equações cúbicas e quárticas, com as propriedades do que Galois, para estabelecer em que condições uma equação algébrica irreduzível é solúvel por radicais, chamou de grupos e grupos parciais.

Podemos dividir o trabalho de Galois em três partes: (a) as *definições*, que contêm definições e conceitos estabelecidos em trabalhos anteriores ao seu artigo; (b) os *lemas*, que fundamentam, por meio de uma função definida por

Galois, a construção do grupo da equação e do polinômio associado; e (c) as *proposições*, responsáveis por estabelecer como construir e reduzir o grupo da equação e de seu polinômio associado.

Galois inicia sua memória introduzindo os conceitos de equação *reduzível*, *irreduzível*, *divisor racional*, *adjunção* e *substituição*.

Destacamos os conceitos de *adjunção* e *racional*, e a relação entre eles. Pelo termo *racional* Galois entende, de maneira geral, as quantidades que possam ser expressas como uma *função racional*¹ dos coeficientes da equação dada, sejam eles números racionais ou não. Ou seja, mesmo que a equação a ser resolvida se apresente com coeficientes não racionais basta supormos tais coeficientes como quantidades conhecidas, a priori, para interpretarmos como uma *quantidade racional*, toda expressão escrita como uma função racional destes coeficientes.

E quando assumimos tais quantidades como *quantidades racionais*, obviamente devemos, quando necessário, ampliar o campo numérico² o qual realizamos as chamadas operações racionais de soma, subtração, multiplicação e divisão.

Por exemplo, a quantidade $t = \frac{1}{3}(x_1 + \alpha \cdot x_2 + \alpha^2 \cdot x_3)$ utilizada por Lagrange para a análise da solubilidade da equação cúbica (pág 34) é uma quantidade *racional* em x_1, x_2, x_3 (raízes da equação dada) e α, α^2 (raízes da equação auxiliar), pela definição de Galois. Aquela equação dada possui coeficientes racionais. Por outro lado, essa quantidade está contida em um campo numérico que deve agregar todos os números racionais e ainda os números α, α^2 . Definir tal campo é a maneira pela qual tornaremos possível executar as operações racionais – adição, subtração, divisão e produto – entre dois números desse campo, e assim dizer que tais números são *racionalmente conhecidos*.

¹ Função Racional é uma expressão na qual podemos efetuar operações racionais, isto é, soma, subtração, multiplicação e divisão entre quaisquer duas quantidades dessa natureza.

² Daremos preferência ao termo campo numérico quando nos referirmos a corpo e extensão de corpo, considerando que tais conceitos foram estabelecidos após e por consequência do trabalho de Galois.

Dizemos que as quantidades α , α^2 estendem o campo numérico dos coeficientes da equação dada, para resolvê-la. Esse procedimento é denominado *adjunção*. No exemplo acima, estamos adjuntando sobre o campo numérico dos racionais as quantidades α , α^2 .

Vejamos outro exemplo: o número $\sqrt{\frac{-5 + \sqrt{13}}{2}}$ é uma raiz da equação $x^4 + 5x^2 + 3 = 0$. Este número não é uma *quantidade racional* sobre os coeficientes da equação dada, isto é, não pertence ao conjunto Q dos racionais; contudo será assim considerada se o campo numérico dos racionais for estendido de forma a agregar as quantidades $\sqrt{13}$ e $\sqrt{\frac{-5 + \sqrt{13}}{2}}$.

Isto é, por essa raiz não estar contida em Q (campo numérico dos coeficientes da equação) será necessário obter um processo de adjunção. O primeiro passo é adjuntar o número $\sqrt{13}$ em Q . Com isto, nos habilitamos a efetuar operações racionais ao campo numérico que contém todos os números racionais mais os elementos da forma $a + b\sqrt{13}$, com $a, b \in Q$. Denotemos este campo por $Q(\sqrt{13})$

Uma segunda adjunção deve estender $Q(\sqrt{13})$ de maneira que nos seja permitido executar operações racionais com quantidades da forma $c + d\sqrt{a + b\sqrt{13}}$ com $a, b, c, d \in Q$, e assim exibir a raiz acima.

Podemos executar este procedimento de adjunção quantas vezes forem necessárias para exibir uma raiz de uma equação irredutível.

Ainda na parte (a) de seu trabalho, Galois chama nossa atenção para o termo *substituição*, que foi definido por ele como a passagem de uma permutação para outra. Entendemos este termo como a aplicação que leva uma permutação na outra.

Logo após a essas definições preliminares Galois afirmou, por meio do Lema II, que existe uma função que, quando associada a um polinômio, exibirá as raízes da equação dada: “*Dada qualquer equação com raízes distintas a, b, c, \dots* ”

podemos sempre construir uma função V das raízes, tal que nenhum entre dois dos valores obtidos pela permutação das raízes nessa função são iguais”.

Como exemplo, ele sugere tomarmos a função $V = Aa + Bb + Cc + Dd + \dots$, onde A, B, C, D, \dots são números inteiros, e a, b, c, d, \dots são as raízes da equação dada.

O polinômio associado à função acima definida foi construído quando da demonstração do Lema III: “*Quando a função V é escolhida como indicada acima, ela irá ter a propriedade que todas as raízes da equação dada podem ser expressas como funções racionais de V ”.*

Na demonstração do Lema acima, Galois toma $V = \phi(a, b, c, d, \dots)$ ou $V - \phi(a, b, c, d, \dots) = 0$ e mostra que basta multiplicar entre si todas as equações semelhantes a essa, obtidas pelas permutações definidas³ por ϕ_i em V , deixando somente uma letra fixa. Se, por exemplo, fixarmos a letra a , temos:

$$(V - \phi(a, b, c, d, \dots)) (V - \phi(a, c, b, d, \dots)) (V - \phi(a, b, d, c, \dots)) \dots$$

para obter uma equação da forma $F(V, a) = 0$ ou $a = f(V)$ e, dela poder obter o valor de a .

Se ao invés da letra a fixarmos a letra b , vamos construir uma equação da forma $F(V, b) = 0$, obtendo o valor de b e assim por diante para todas as outras letras, raízes da equação dada, isto é, “*as raízes da equação dada podem ser expressas como funções racionais de V ”.*

Para uma equação de grau n , podemos afirmar que $F(V, a)$ possui no máximo $(n - 1)!$ fatores, pois fixamos uma letra e permutamos todas as outras. O mesmo número de fatores define $F(V, b)$ ou qualquer outro polinômio dessa natureza, para uma mesma equação dada.

³ Em uma dada equação de grau quatro, de raízes a, b, c, d , suponha $V = a + b$. Vamos chamar de ϕ as aplicações (substituições) que calculam V . Então $\phi(a, b, c, d) = a + b$, ao passo que $\phi(a, c, d, d) = a + c$ e assim por diante, isto é ϕ calcula V .

Tal característica para $F(V, a)$ (ou qualquer um dos outros polinômios assim definidos) nos leva a sugerir a existência de uma relação entre esse(s) polinômio(s) e o polinômio $g(x)$, apresentado nas seções anteriores. Se compararmos o exposto acima com o que fizemos naquelas seções, podemos verificar que Galois tentava preservar a idéia básica de Cardano, Ferrari e Lagrange: para resolver uma equação dada de grau n temos que trocar tal equação por uma equação resolvente de grau $n!$ e reduzir seu grau para $(n-1)!$. Isto é, Galois construiu um polinômio $(F(V, a))$ com o objetivo de reduzir o grau da equação resolvente para no máximo $(n-1)!$, dado que o grau da equação a ser resolvida seja n .

Se aplicarmos os Lemas II e III ao estudo da solubilidade da equação irreduzível de grau quatro, por exemplo, teremos então $V = \phi(a, b, c, d)$, de forma que quando permutamos todas as letras deixando a letra a fixa, temos:

$$\begin{aligned}
 F(V, a) = & \\
 = & (V - \phi(a, b, c, d))(V - \phi(a, d, b, c))(V - \phi(a, c, d, b)) \\
 & \cdot (V - \phi(a, c, b, d))(V - \phi(a, d, c, b))(V - \phi(a, b, d, c))
 \end{aligned}$$

O Lema III nos diz que, com esse polinômio – veremos isto, de fato, ao final dessa seção – obtemos o valor de a , uma raiz da equação de quarto grau.

Observemos que $F(V, a)$ está definido com 6 fatores. Lembremos que no decorrer dos métodos de solução de Ferrari e Lagrange obtemos equações de grau 6, que são reduzidas para o grau 3, equação cúbica intermediária desses procedimentos, dadas diretamente (Ferrari) ou por meio do polinômio $g(x)$ (Lagrange). Por este motivo, podemos sugerir a possibilidade de reduzir tal polinômio resolvente $F(V, a)$ para o grau 3, identificando esse polinômio com aquelas equações do grau 6 e do grau 3.

E se, de fato, houver tal possibilidade de reduzir $F(V, a)$ para o grau 3, com fatores $(V - \phi_i)(V - \phi_j)(V - \phi_k)$, por exemplo, as quantidades racionais ϕ_i, ϕ_j, ϕ_k serão tomadas para escrevermos

$$a = \frac{1}{4} \left[(a + b + c + d) + \sqrt[4]{\phi_i^4} + \sqrt[4]{\phi_j^4} + \sqrt[4]{\phi_k^4} \right],$$

tal como fizemos ao final da seção anterior, com a última redução em $g(x)$. Isto é, obter o valor de a .

Poderemos também, identificar, quando possível, a função V com o resolvente de Lagrange, $t = x_1 + \alpha x_2 + \alpha^2 x_3 + \dots + \alpha^{n-1} x_n$. Isto é, fazer $V \equiv t$.

Para tanto continuemos com o exemplo da equação do quarto grau. Vimos na seção anterior que o grupo para essa equação é gerado por meio das permutações das raízes x_1, x_2, x_3, x_4 da equação dada, na expressão racional $t = x_1 - x_2 + x_3 - x_4$ (o resolvente de Lagrange).

Galois utiliza as letras a, b, c, \dots para se referir as raízes da equação, e a letra ϕ para as aplicações (substituições) que calculam as permutações em V (Lema III), que podem se identificar com as permutações t_i . Utilizando estas letras, podemos apresentar o que Galois chamou de o *grupo* (de permutações) da equação de grau quatro, na disposição que ele sugeriu:

$\phi_1 = abcd$	$\phi_5 = acdb$	$\phi_9 = adbc$	$\phi_{13} = abdc$	$\phi_{17} = acbd$	$\phi_{21} = adcb$
$\phi_2 = badc$	$\phi_6 = cabd$	$\phi_{10} = dacb$	$\phi_{14} = bacd$	$\phi_{18} = cadb$	$\phi_{22} = dabc$
$\phi_3 = cdab$	$\phi_7 = dbac$	$\phi_{11} = bcad$	$\phi_{15} = dcab$	$\phi_{19} = bdac$	$\phi_{23} = cbad$
$\phi_4 = dcba$	$\phi_8 = bdca$	$\phi_{12} = cbda$	$\phi_{16} = cdba$	$\phi_{20} = dbca$	$\phi_{24} = bcda$

Onde, quando escrevemos $abcd$ estaremos nos referindo a quantidade $\phi_1 \equiv t_1 = x_1 - x_2 + x_3 - x_4$. Para nos referirmos a quantidade $\phi_2 \equiv t_2 = x_4 - x_1 + x_2 - x_3$ iremos escrever $dabc$, e assim por diante para os 24 valores $\phi_i = t_i$, $1 \leq i \leq 24$ ($4! = 24$ permutações da expressão $t = x_1 - x_2 + x_3 - x_4$).

Observemos que o *grupo* acima contém as mesmas 24 permutações t_i apresentadas na seção anterior, entretanto, elas estão agora dispostas de maneira como Galois sugeriu. Observemos também que letra a está fixada em cada uma das linhas apresentadas, com as outras letras permutando. Logo, tal

disposição satisfaz o Lema III, pois as 6 permutações de cada linha se identificam com os 6 fatores de $F(V, a)$.

Galois demonstra por meio de suas Proposições I, II e III que as 4 linhas do grupo acima são equivalentes. Isto significa que podemos construir 4 versões diferentes para o polinômio $F(V, a)$. Construção que nos leva novamente ao encontro dos métodos de Ferrari e Lagrange para a solução da equação de quarto grau. Logo, poderemos fazer a identificação $V \equiv t$ para construir o grupo acima, bem como fazer a relação de $F(V, a)$ com o polinômio $g(x)$ e suas respectivas reduções.

Usando ϕ para denotar cada permutação em t podemos reescrever $g(x)$:

$$g(x) = (x - \phi_1)(x - \phi_2)(x - \phi_3)(x - \phi_4)(x - \phi_5) \dots (x - \phi_{23})(x - \phi_{24})$$

Vimos nas seções anteriores que a redução dos fatores de g ocorrem através das equivalências em t_i (ou em ϕ_i). Tais equivalências reduzem não somente o grau do polinômio $g(x)$, gerando o polinômio reduzido $F(V, a)$, como também o número de permutações do grupo da equação, associando as reduções do grupo com às do polinômio.

As Proposições I, II e III não somente fundamentam as relações entre as reduções em g , que fizemos nas seções anteriores, com reduções no grupo, que iremos fazer nessa seção, como também estabelecem os critérios para obter a construção de tal grupo (com a disposição apresentada acima), associando cada uma das sucessivas reduções desse grupo com cada uma das sucessivas reduções para os fatores do polinômio $g(x)$.

Na demonstração da Proposição I, ele esclarece que as equivalências em ϕ_i ocorrem, necessariamente, entre aquelas permutações que estão fixadas entre as linhas, para cada coluna, devido a natureza cíclica destas quantidades. A redução ocorre porque tais equivalências deixam inalterado o grupo da equação.

Proposição I: “Seja a equação de raízes a, b, c, \dots . Existirá sempre um grupo de permutações das letras a, b, c, \dots que terá a seguinte propriedade:

1. que cada função invariante sobre as substituições de seu grupo será conhecida racionalmente.
2. reciprocamente, que toda função das raízes que podem ser determinadas racionalmente serão invariantes sobre essas substituições.”

Por outro lado, as equivalências em ϕ_i que reduzem o grupo (e reduzem $g(x)$), obedecem, ainda, a dupla propriedade descrita a seguir, nas proposições II e III:

“O grupo da equação deve se decompor em p grupos parciais, quando adjuntamos as raízes da equação auxiliar na equação dada, sendo que passamos de um grupo parcial para o outro por uma substituição simples, e que cada grupo parcial deve conter as mesmas substituições” (proposições⁴ II e III, em resumo pelo próprio Galois, na proposição V).

Vejamos então como decompor o grupo acima em p grupos parciais, onde p é um número primo, ao mesmo tempo que reduzimos o grau de $g(x)$. Para tanto, Galois nos diz que devemos seguir os passos da solução da equação dada. Nossa referência para isto é o método de Ferrari para resolver a equação de grau 4. Nesse método, é necessário, em primeiro lugar, extrair uma raiz quadrada, para recairmos em uma equação cúbica. Após a extração da raiz cúbica, fazemos a extração da raiz quadrada duas vezes. Isto é, “O grupo da equação deve se decompor em p grupos parciais, quando adjuntamos as raízes da equação auxiliar na equação dada”.

⁴ Proposição II: “Se adjuntarmos para uma dada equação as raízes r de uma equação auxiliar irredutível:

(i) uma das duas coisas acontecerá: ou o grupo da equação não mudará; ou ele será particionado em p grupos, cada um pertencendo a dada equação respectivamente quando adjuntarmos cada uma das raízes da equação auxiliar;

(ii) esses grupos terão a propriedade que um passará para outro aplicando a mesma substituição das letras para todas as permutações do primeiro”.

Proposição III: “Se adjuntarmos a uma equação todas as raízes de uma equação auxiliar, os grupos no Teorema II terão a propriedade que cada grupo contém as mesmas substituições”.

De acordo com a seqüência para a solução de Ferrari, a extração da raiz quadrada é a primeira adjunção das raízes de uma equação auxiliar que devemos fazer. Então essa adjunção deve dividir o grupo de 24 elementos em $p = 2$ grupos parciais com o mesmo número de elementos.

Depois, vamos dividir este grupo parcial de 12 elementos, resultante da primeira redução, em $p = 3$ grupos de quatro elementos. E esse é o próximo passo na seqüência do procedimento de Ferrari: resolver a equação cúbica oriunda da extração da primeira raiz. Nesse caso, fazemos a segunda adjunção das raízes da equação auxiliar, de grau 3.

E pelas duas extrações consecutivas da raiz quadrada, ou seja, adjuntando pela terceira e quarta vez as raízes de uma equação auxiliar de grau 2, reduzimos o grupo parcial de 4 para 2, e de 2 para 1.

Portanto decompos as $4! = 24$ permutações do grupo total em $24 = 2.3.2.2$.

Por outro lado, “... *passamos de um grupo parcial para o outro por uma substituição simples, e ... cada grupo parcial deve conter as mesmas substituições*”.

Para cumprir esta exigência, temos que definir as *substituições* de maneira a dividir o grupo. Estas substituições são aplicações que serão definidas tomando como referência, as posições das letras, e não as letras.

Vamos então fixar as posições das letras, a partir da permutação identidade $abcd$:

$$\begin{cases} a = 1 & b = 2 \\ c = 3 & d = 4 \end{cases}$$

Assim, podemos ver que:

(i) a substituição (ou a aplicação) $(3 \rightarrow 4, 4 \rightarrow 3)$ divide⁵ o grupo em 2 grupos parciais

⁵ Se $c = 3, d = 4$ então $(3 \rightarrow 4, 4 \rightarrow 3)$ leva c para a posição de d , e vice-versa, isto é, inverte as posições das letras c e d para os 12 elementos a esquerda, em relação a cada um dos 12 elementos a direita, no grupo acima. Logo, qualquer um dos grupos parciais de 12 permutações fica invariante sobre suas permutações, de maneira a optarmos entre um dos grupos. Fazemos o mesmo com relação às aplicações em (ii), (iii) e (iv).

<i>abcd</i>	<i>acdb</i>	<i>adbc</i>	<i>abdc</i>	<i>acbd</i>	<i>adcb</i>
<i>badc</i>	<i>cabd</i>	<i>dacb</i>	<i>bacd</i>	<i>cadb</i>	<i>dabc</i>
<i>cdab</i>	<i>dbac</i>	<i>bcad</i>	<i>dcab</i>	<i>bdac</i>	<i>cbad</i>
<i>dcba</i>	<i>bdca</i>	<i>cbda</i>	<i>cdba</i>	<i>dbca</i>	<i>bcda</i>

Em $g(x)$ devemos ter:

$$g(x) = (x - \phi_1)(x - \phi_2)(x - \phi_3)(x - \phi_4)(x - \phi_5) \dots (x - \phi_{23})(x - \phi_{24}) =$$

$$= (x - \phi_1)^2 (x - \phi_2)^2 (x - \phi_3)^2 (x - \phi_4)^2 (x - \phi_5)^2 (x - \phi_6)^2 \dots (x - \phi_{11})^2 (x - \phi_{12})^2$$

pois $\phi_i \equiv \phi_{12+i}$, $i = 1, \dots, 12$ são equivalências que deixam invariante o grupo da equação e cada grupo parcial contém a mesma substituição. Isto é, $g(x) = (h_1)^2$.

(ii) a substituição $(2 \rightarrow 4, 4 \rightarrow 3, 3 \rightarrow 2)$ define a divisão de cada um dos grupos parciais de 12 elementos, em 3 grupos parciais de 4 elementos;

<i>abcd</i>	<i>acdb</i>	<i>adbc</i>
<i>badc</i>	<i>cabd</i>	<i>dacb</i>
<i>cdab</i>	<i>dbac</i>	<i>bcad</i>
<i>dcba</i>	<i>bdca</i>	<i>cbda</i>

E em $h(x)$ teremos:

$$h_1(x) = (x - \phi_1)(x - \phi_2)(x - \phi_3)(x - \phi_4)(x - \phi_5)(x - \phi_6) \dots (x - \phi_{11})(x - \phi_{12})$$

$$= (x - \phi_1)^3 (x - \phi_2)^3 (x - \phi_3)^3 (x - \phi_4)^3 ,$$

para definirmos $(h_2)^3 = h_1(x)$, considerando que $\phi_i \equiv \phi_{i+4} \equiv \phi_{i+9}$, $i = 1, 2, 3, 4$ são as equivalências que deixam o grupo inalterado e que cada grupo parcial contém as mesmas 4 substituições.

(iii) a substituição $(1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 4, 4 \rightarrow 3)$ define a divisão de cada um dos grupos de 4 elementos, em 2 grupos de 2 elementos;

<i>abcd</i>	<i>cdab</i>
<i>badc</i>	<i>dcba</i>

isto é, $\phi_1 \equiv \phi_3$ e $\phi_2 \equiv \phi_4$. Estas equivalências definem $(h_2)^2 = h_3(x) = (x - \phi_1)(x - \phi_2)$

(iv) a substituição identidade define a última divisão do grupo e o polinômio

$$(h_3)^2 = h_4(x) = (x - \phi_1);$$

de maneira que, frisamos, “... passamos de um grupo parcial para o outro por uma substituição simples, e ... cada grupo parcial deve conter as mesmas substituições”.

Podemos então afirmar que as reduções do grupo e do seu polinômio associado se completam quando definimos o grupo da equação dada pelos critérios acima. O grupo total, disposto como abaixo, ainda revela o polinômio $F(V, a) = (x - \phi_1)(x - \phi_2)(x - \phi_3)$, pois, quando tomamos qualquer permutação contida na primeira coluna, por exemplo $\theta = abcd$, e as aplicações descritas em (i), (ii) e (iii) acima para construção do grupo da equação, temos:

<i>abcd</i>	<i>acdb</i>	<i>adbc</i>	<i>abdc</i>	<i>acbd</i>	<i>adcb</i>
<i>badc</i>	<i>cabd</i>	<i>dacb</i>	<i>bacd</i>	<i>cadb</i>	<i>dabc</i>
<i>cdab</i>	<i>dbac</i>	<i>bcad</i>	<i>dcab</i>	<i>bdac</i>	<i>cbad</i>
<i>dcba</i>	<i>bdca</i>	<i>cbda</i>	<i>cdba</i>	<i>dbca</i>	<i>bcda</i>

(i) aplicando $2 \rightarrow 4, 4 \rightarrow 3, 3 \rightarrow 2$ para θ , obtemos $\theta_1 = acdb$.

(ii) aplicando $2 \rightarrow 4, 4 \rightarrow 3, 3 \rightarrow 2$ para θ_1 , temos $\theta_2 = adbc$.

(iii) e ainda $\theta_3 = \theta$, pela mesma aplicação.

Obedecendo a condição que θ é aplicada em uma das permutações que está no grupo, e não está no grupo parcial.

Galois afirma sem demonstrar⁶ que esta construção faz com que a expressão $(\theta + \alpha\theta_1 + \alpha^2\theta_2)^3$ seja invariante por todas as substituições do grupo total.

⁶Uma demonstração pode ser encontrada em Edwards [E1], Proposição 46, pags 61-64.

Quando extraímos a raiz cúbica dessa expressão, isto é quando temos $\left(\sqrt[3]{(\theta + \alpha\theta_1 + \alpha^2\theta_2)^3}\right)$, obtemos a parte final das quatro raízes expressas por Lagrange em função das quantidades t_i exibidas nas pág 40 e 43 da seção anterior, de forma que:

$$\begin{aligned} x &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \sqrt[4]{t_i^4} + \sqrt[4]{t_j^4} + \sqrt[4]{t_k^4} \right] \\ &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \theta + \alpha\theta_1 + \alpha^2\theta_2 \right] \end{aligned}$$

onde $\theta = t_1 = \phi_1$, $\theta_1 = t_5 = \phi_5$, $\theta_2 = t_9 = \phi_9$ e $F(V, a) = (x - \theta)(x - \theta_1)(x - \theta_2)$.

Repetindo tal procedimento para cada uma das 3 permutações restantes na primeira coluna, vamos obter o mesmo resultado, isto é, definimos as quatro raízes da equação de grau quatro como acima, considerando a equivalência entre as permutações de cada coluna.

Vendo isto pelo método de Ferrari, temos a mesma idéia: cada raiz da equação cúbica, inerente ao processo (divisão do grupo de 12 elementos em 3 grupos de 4 elementos), fornece as mesmas 4 raízes para a equação dada (as permutações dispostas na mesma coluna são equivalentes, pois são cíclicas).

De maneira geral, Galois mostra que uma equação geral de grau n será solúvel por radicais quando, ao definirmos uma função V das raízes dessa equação, construímos um polinômio $F(V, a)$, que deverá conter $(n-1)!$ fatores, obtidos quando permutamos todas as raízes na função V , com a raiz a fixa. Por meio desse polinômio, podemos extrair o valor de a , uma raiz da equação dada. Para tanto, é necessário, através de todas as permutações da função V , construir e reduzir o grupo desta equação e seu polinômio associado $g(x)$, tal que esse grupo satisfaça a dupla propriedade acima, descrita na Proposição V, de maneira que a expressão $(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \dots + \alpha^{p-1}\theta_{p-1})^p$ seja invariante por

todas as substituições do grupo total; e portanto, quando extrairmos a p -ésima raiz desta expressão iremos obter as n raízes da equação dada.

Vamos agora verificar como esta teoria se aplica a equações de grau maior que 4.

2.5 SOLUÇÃO PARA EQUAÇÕES DE GRAUS SUPERIORES

Vamos, por um instante, retomar as idéias de Lagrange.

Tal como fez para a cúbica e quártica, ele pesquisou um resolvente t para a equação quártica dada (que em nosso padrão computacional é $t = x_1 + \alpha.x_2 + \alpha^2.x_3 + \alpha^3.x_4 + \alpha^4.x_5$, onde x_1, x_2, x_3, x_4, x_5 são as raízes da equação de grau cinco $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$; e $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ são as raízes da equação auxiliar $x^5 - 1 = 0$, ou raízes da unidade) e elevou cada uma das expressões obtidas pelas permutações das raízes a quinta potência.

Entretanto, como afirma Kiernan [K2](pág 57), ao contrário do que poderia ter desejado, Lagrange sempre encontrou seis expressões diferentes para qualquer resolvente suposto, e não quatro.

Em resumo, seu procedimento troca a equação dada de grau cinco, para uma outra de grau seis. Isto é, o grau da equação resolvente não fica menor do que o grau da equação dada. E portanto, não é possível encontrar valores t_1, t_2, t_3, t_4 , por exemplo, para escrevermos

$$x_1 = \frac{1}{5}[(x_1 + x_2 + x_3 + x_4 + x_5) + t_1 + t_2 + t_3 + t_4].$$

De fato, Lagrange não conseguiu provar que não existe uma equação resolvente de grau 4, que possa exibir as soluções de uma equação de quinto grau. Ruffini e Abel foram responsáveis por esta prova e pela conseqüente demonstração da insolubilidade, por radicais, de equações gerais de grau maior ou igual a 5.

Ruffini estudou e classificou as permutações provando que não existe um resolvente para a equação geral quártica que assuma menos de 5 valores distintos. Foi Abel quem apresentou uma prova definitiva para a insolubilidade por radicais de equações de grau igual a 5, utilizando um resultado de Augustin-Louis Cauchy (1789-1847).

Cauchy não esteve diretamente relacionado com o problema da solubilidade de equações, mas em 1815 desenvolveu um trabalho sobre teoria das permutações, “*Mémoire sur le nombre des valeurs qu’une fonction peut acquérir, lorsqu’on y permute de toutes les manières possibles les quantités qu’elle renferme*”.

Neste artigo ele mostra que:

se uma expressão de n quantidades assume um número r de diferentes valores, então r não pode ser menor que o maior número primo p , menor ou igual a n , ao menos que seja no máximo 2.

Por sua vez, Abel buscava um formato padrão para expressar os resolventes das equações de grau primo (tal como em nosso padrão computacional). Ele propôs a função

$$x = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \dots + q_{n-1} p^{\frac{p(n-1)}{n}}$$

onde n é primo e $p, q_0, q_2, \dots, q_{n-1}$ são expressões racionais nos coeficientes da equação dada (aqui Abel utiliza o termo *racional* tal como fez depois Galois – pags 46-48). Estabelecendo isso, ele tomou a hipótese de que se uma equação é solúvel por radicais, então cada raiz da equação dada pode ser escrita por uma expressão que é racional nessas raízes.

Adjuntando as raízes da unidade (isto é, as raízes complexas de $x^n - 1 = 0$) para a expressão acima, aplicou o resultado de Cauchy em uma destas, considerando a equação dada de grau $n = 5$, e demonstrou que $p^{\frac{1}{n}}$ não

pode ser escrito em função das raízes da equação dada, assumindo $n = 5$ ou $n = 2$; isto é tomando $p^{1/5}$ e $p^{1/2}$, recaiu em contradição para cada caso⁷.

Por sua vez Galois, contemporâneo de Lagrange e Cauchy, estava interessado em saber quando é possível resolver por radicais uma equação de qualquer grau. Ele também explora o resultado de Cauchy estabelecendo que as divisões dos grupos parciais ocorrem quando $r = p$.

De fato, como vimos na seção anterior, o resolvente para a equação quártica assume um grupo de $4! = 24$ valores, que se divide sucessivamente em $p = 2, 3, 2, 2$ grupos parciais. O mesmo ocorre com o resolvente da cúbica, que assume um grupo de $3! = 6$ valores, que é dividido sucessivamente em $p = 2, 3$.

Por essas considerações, podemos continuar nossa análise para equações de graus superiores a 4, explorando apenas casos particulares (ou equações incompletas).

E, neste sentido, as pesquisas de Lagrange, Ruffini e Abel vão ao encontro das conclusões de Galois.

Podemos fazer tal afirmação considerando que Galois ainda abordou em seu artigo o estudo da solubilidade de equações irredutíveis do tipo $x^p - B = 0$, p primo.

Para tais equações, Galois afirma que o número de elementos do grupo será $p \cdot (p-1)$, devido a natureza cíclica de suas raízes.

Na demonstração da Proposição VII: “*se uma equação irredutível de grau primo é solúvel por radicais então o grupo dessa equação somente pode conter substituições da forma*

$$x_k \quad x_{ak+b}$$

com a, b constantes.”, Galois observa que:

⁷ Podemos apreciar a prova de Abel por meio de seu artigo contido em Smith [S1] págs 261-266.

(i) o grupo imediatamente anterior a última redução será aquele em que cada permutação é gerada por uma substituição (aplicação) cíclica e conterà exatamente p permutações.

Como exemplo, tomemos uma equação de grau 5, $x^5 - B = 0$. O grupo dessa equação será da forma

abcde
bcdea
cdeab
deabc
eabcd

para equação de grau 7, teremos:

abcdefg
bcdefga
cdefgab
defgabc
efgabcd
fgabcde
gabcdef

de maneira que a próxima redução gera o grupo que contém somente a permutação identidade.

(ii) o grupo que imediatamente precede qualquer um desses acima, na seqüência das decomposições, deve ser tomado com um certo número de grupos parciais com as mesmas (e únicas) substituições, de forma que cada coluna (tal como fizemos para a primeira) seja formada por uma substituição cíclica.

Tomemos como exemplo novamente o caso $x^5 - B = 0$, com $B \in \mathbb{Z}$. Observando que a posição da letra a em cada linha deve estar fixa enquanto todas as outras letras se permutam (pelo Lema III, e porque cada coluna deve ser gerada por uma substituição cíclica), o grupo da equação deverá ser

<i>abcde</i>	<i>acebd</i>	<i>aedcb</i>	<i>adbec</i>
<i>bcdea</i>	<i>cebda</i>	<i>edcba</i>	<i>dbeca</i>
<i>cdeab</i>	<i>ebdac</i>	<i>dcbae</i>	<i>becad</i>
<i>deabc</i>	<i>bdace</i>	<i>cbaed</i>	<i>ecadb</i>
<i>eabcd</i>	<i>daceb</i>	<i>baedc</i>	<i>cadbe</i>

onde a mesma (e única) substituição $(2 \rightarrow 4, 4 \rightarrow 5, 5 \rightarrow 3, 3 \rightarrow 2)$ define os grupos parciais acima. E, desse modo, o número de substituições do grupo é $p(p-1)$.

Com essa substituição, acima apresentada, sintetizamos a condição estabelecida na proposição: *o grupo dessa equação somente pode conter substituições da forma x_k, x_{ak+b}* . De fato, ainda na demonstração dessa proposição, Galois define a função $f(k) = ak + b \pmod{n}$ para calcular as posições das letras a, b, c, d, e em cada permutação do grupo.

Nessa abordagem, ele chamou as raízes da equação dada de x_0, x_1, x_2, x_3, x_4 em lugar de a, b, c, d, e respectivamente, onde os índices $0, 1, 2, 3, 4$ são os valores assumidos por $k, ak + b$ em x_k, x_{ak+b} . Julgamos que esta mudança se deve a utilização da função f , considerando que ela manipula os índices de x_k, x_{ak+b} .

Vamos exemplificar esses cálculos:

Em primeiro lugar, observemos que se a letra $a = x_0$ está fixa no grupo acima, então é necessário que $f(0) = 0$ quando $k = 0$, porque a letra a é levada para as próximas colunas na mesma posição que ocupa na primeira (Lema III). Isto é, a imagem de x_0 é o próprio x_0 .

Por este motivo $b = 0$ em $ak + b$. Portanto, para esse grupo, $f(k) = ak \pmod{n}$.

Com essa última função vamos definir as permutações das próximas colunas, a partir da primeira. Em primeiro lugar, se $a = 1$, então $f(k) = k$ é a função identidade, que define a primeira coluna.

Se $a = 2$, então $f(k) = 2k \pmod{5}$ é a função que define a segunda coluna a partir da primeira. Para tanto, basta tomar $k = 1, 2, 3, 4$ índices para x_k (uma vez que a letra a – onde x_k tem índice 0 – está fixa). Aplicando cada um desses valores para k em f , vamos definir as próximas posições das letras b, c, d, e no grupo. Podemos representar isso da seguinte maneira:

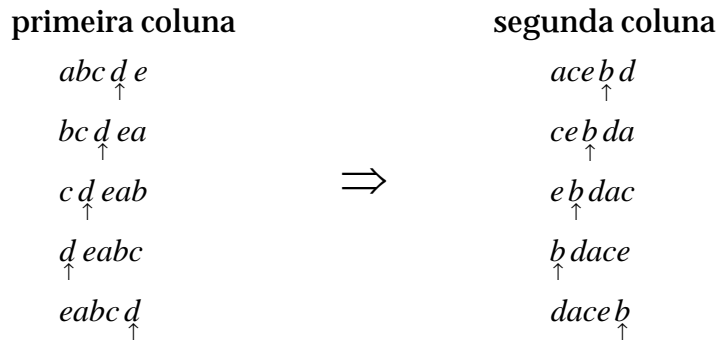
primeira coluna		segunda coluna
<i>abcde</i>		<i>acebd</i>
<i>bcdea</i>	$\xrightarrow{a=2}$	<i>cebda</i>
<i>cdeab</i>	$\xrightarrow{f(k)=2k \pmod{5}}$	<i>ebdac</i>
<i>deabc</i>		<i>bdace</i>
<i>eabcd</i>		<i>daceb</i>

De forma que, quando $k = 1$, por exemplo, temos $f(1) = 2$.

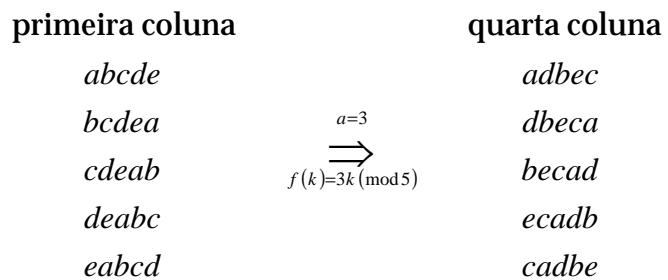
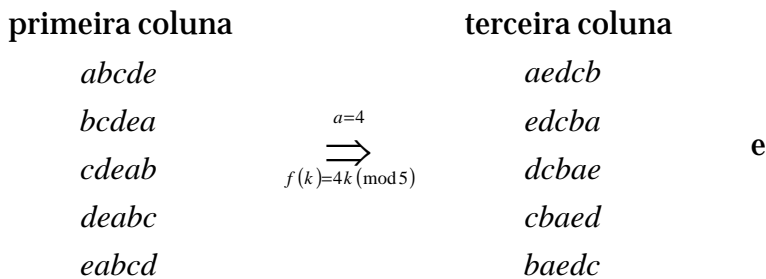
Esse resultado nos diz que a imagem de x_1 será $x_2 = c$. Logo, a letra c ocupará, na segunda coluna, a posição que a letra b ocupa na primeira:

primeira coluna		segunda coluna
<i>a</i> ↑ <i>b</i> <i>cde</i>		<i>a</i> ↑ <i>c</i> <i>ebd</i>
<i>b</i> ↑ <i>c</i> <i>de</i> <i>a</i>	\Rightarrow	<i>c</i> ↑ <i>e</i> <i>b</i> <i>d</i> <i>a</i>
<i>c</i> ↑ <i>d</i> <i>e</i> <i>a</i> <i>b</i>		<i>e</i> ↑ <i>b</i> <i>d</i> <i>a</i> <i>c</i>
<i>d</i> ↑ <i>e</i> <i>a</i> <i>b</i> <i>c</i>		<i>b</i> ↑ <i>d</i> <i>a</i> <i>c</i> <i>e</i>
<i>e</i> ↑ <i>a</i> <i>b</i> <i>c</i> <i>d</i>		<i>d</i> ↑ <i>a</i> <i>c</i> <i>e</i> <i>b</i>

Se tomarmos $k = 3$, então $f(3) = 6 \pmod{5} = 1$. Ou seja, a imagem de x_3 será x_1 . Então, a letra b ocupará, na segunda coluna, a posição que a letra d ocupa na primeira:



Os exemplos que fizemos acima induzem não somente a construção da segunda coluna, mas todo o processo de construção das quatro colunas. Quando $a = 4$, temos $f(k) = 4k \pmod{5}$, para construirmos a terceira coluna a partir da primeira. E quando $a = 3$, temos $f(k) = 3k \pmod{5}$ que constrói da quarta coluna a partir da primeira. Podemos representar tais substituições, respectivamente, como abaixo:



Observamos ainda que todo esse processo constrói cada uma das colunas com permutações cíclicas, isto é tal processo também satisfaz a primeira das duas condições descritas acima.

Para concluirmos este tratamento, vamos estabelecer que cada coluna desse grupo se inicia com as permutações ϕ_{5j+1} , $j=0, 1, 2, 3$ para, tal como fizemos nas seções anteriores, pelos Lemas II e III, poderemos construir uma função V , tomando, por exemplo, as quantidades $\phi_1, \phi_6, \phi_{11}, \phi_{16}$ (associadas ao polinômio $F(V, a) = (V - \phi_1)(V - \phi_6)(V - \phi_{11})(V - \phi_{16})$), para obtermos o valor de a :

$$\frac{1}{5}[(a + b + c + d + e) + \phi_1 + \phi_6 + \phi_{11} + \phi_{16}] = a$$

O polinômio g associado ao grupo da equação será reduzido como abaixo:

$$\begin{aligned} g(x) &= (x - \phi_1) \cdot (x - \phi_2) \cdot \dots \cdot (x - \phi_{20}) = \\ &= (x - \phi_1)^5 (x - \phi_6)^5 (x - \phi_{11})^5 (x - \phi_{16})^5 \end{aligned}$$

Onde a multiplicidade 5 de cada fator de $g(x)$, define os 4 grupos parciais (cada uma das colunas com 5 elementos do grupo total), considerandos as equivalências entre estas substituições (pois são cíclicas), de forma que:

$$g(x) = (h(x))^5 \quad \text{e} \quad h(x) \equiv F(V, a) = (x - \phi_1) \cdot (x - \phi_6) \cdot (x - \phi_{11}) \cdot (x - \phi_{16})$$

Após fundamentar as condições de solubilidade para essas equações em acordo com sua teoria geral, Galois por fim, propõe um método direto para exhibir as raízes de equações dessa natureza.

Proposição VIII: “*Para que uma equação irreduzível de grau primo seja solúvel por radicais, é necessário e suficiente que pelo menos duas de suas raízes sejam conhecidas para que as outras sejam deduzidas racionalmente das primeiras*”.

Vejam como aplicar essa proposição, utilizando novamente o exemplo da equação do quinto grau. Tomemos a equação $x^5 - B = 0$.

Isolando a indeterminada x , obtemos:

$$x^5 - B = 0 \quad \Leftrightarrow \quad x^5 = B \quad \Leftrightarrow \quad x = \sqrt[5]{B}$$

que pela Proposição acima é uma das duas quantidades que admitiremos como *racionalmente conhecida* para, a partir delas, deduzirmos as demais. Pelo processo de adjunção das raízes complexas da equação auxiliar $x^5 - 1 = 0$, podemos obter racionalmente a outra raiz, necessária ao processo.

Isto é, como $x = \sqrt[5]{B} = \sqrt[5]{\alpha^5 \cdot B}$, onde α é uma das raízes complexas da equação $x^5 - 1 = 0$, então $x_2 = \alpha \cdot \sqrt[5]{B}$ é a outra raiz conhecida.

Dessas duas, concluímos que as raízes da equação dada são:

$$x_1 = \sqrt[5]{B}, \quad x_2 = \alpha \cdot \sqrt[5]{B}, \quad x_3 = \alpha^2 \cdot \sqrt[5]{B}, \quad x_4 = \alpha^3 \cdot \sqrt[5]{B}, \quad x_5 = \alpha^4 \cdot \sqrt[5]{B}$$

CONCLUSÃO

Na nossa opinião, a teoria matemática na qual nos envolvemos, conhecida como Álgebra, está fundamentada em um processo de modificação e de construção de conceitos, mais do que na simples acumulação de definições, teoremas e símbolos.

Nesta dissertação procuramos compilar um material que exemplifique parte desse processo. Em outras palavras, procuramos reconstruir, com a nossa visão, uma pequena parte do processo histórico de desenvolvimento dessa teoria matemática.

As descobertas das fórmulas para a solução das equações cúbicas e quárticas, e a procura infrutífera por um método de solução da equação do quinto grau motivaram o início de um tratamento completamente diferente para o problema da resolução das equações algébricas por radicais.

Lagrange, após estudar os métodos de solução para equações de grau 2, 3 e 4, pesquisou uma maneira de unificá-los, criando o procedimento que descrevemos nas seções 2.2 e 2.3. Entretanto, a originalidade de Lagrange ao substituir uma equação por outra, exibindo as raízes da primeira em função da segunda, percebendo que propriedades importantes da primeira equação poderiam ser deduzidas examinando o efeito produzido na equação e na equação auxiliar, pela permutação das raízes, não permitiu-lhe provar a não existência de uma equação auxiliar para o caso geral de uma equação de grau qualquer. Por outro lado, a atenção dada por Lagrange no efeito das permutações nessas equações levaram-no a demonstrar que a ordem de um subgrupo de um grupo simétrico divide a ordem do grupo, fato importante, hoje, na teoria dos grupos.

Galois foi influenciado pela idéias de Lagrange mas, sua abordagem constituiu numa ruptura com a de Lagrange, considerando que ele não se fixou em desenvolver métodos computacionais para exibir raízes de equações, mas em estabelecer condições necessárias e suficientes para que uma equação seja

solúvel por radicais. Utilizando substituições (funções) trocou a equação dada por um grupo de permutações, decidindo se a equação é solúvel por radicais ou não apenas utilizando-se das propriedades desse grupo.

Por esse motivo, a abordagem sugerida por Galois foi de fundamental importância para o desenvolvimento posterior da Álgebra, considerando a mudança de foco para o ataque em diversos problemas sugeridos. Após o trabalho de Galois, os algebristas não mais se preocupam com os elementos que formam um determinado campo ou conjunto numérico, mas sim com as propriedades dos conjuntos de tais elementos.

Foi com essa visão que a Álgebra passou a ser desenvolvida. Por meio dos trabalhos dos matemáticos alemães no século XIX e início do século XX (veja Capítulo 1, págs 28-30), o conceito de grupo foi aos poucos se desprendendo do estudo das equações algébricas, tornando-se um conceito muito mais abstrato e abrangente. Nasce, da Teoria de Galois, a chamada Teoria de Grupos, onde o grupo de permutações passa a ser apenas um caso particular a ser estudado.

A noção de grupo é uma das mais importantes idéias unificadoras da matemática, na medida em que trata da noção geral de composição de funções¹. Pela Teoria de Grupos é possível, por exemplo, descrever algebricamente o grupo de simetrias do triângulo, do quadrado ou dos poliedros regulares, ou ainda descrever o grupo das matrizes das transformações lineares.

Galois foi assim o precursor de uma das mais importantes idéias matemáticas. Seu nome para sempre será lembrado, (até) mesmo como um mero tópico (um capítulo sobre a Teoria de Galois) de um livro didático de Álgebra Moderna.

¹ Galois diz que se as aplicações S e T pertencem ao grupo, então a aplicação ST também pertence. De fato, podemos assumir que cada permutação do grupo é uma substituição. E assim teremos um grupo de substituições.

BIBLIOGRAFIA

[A1] Anglin, W.S. & Lambek, J. (1995). “*The Heritage of Thales*”. New York: Springer-Verlag. Undergraduate Texts in Mathematics.

[A2] Araujo, O. (1999), “Apuntes sobre la evolucion histórica de la teoría de Galois.”, in Paques, A. *Teoría de Galois sobre Anillos Conmutativos*. Mérida, Venezuela. 1º Edição. p 89-154.

[A2] Arboleda, L. C. (1983). “*Historia y Enseñanza de Las Matemáticas*”. Bogotá.

[B1] Baumgart, J.K. (1989). “*Historical Topics for the Mathematics Classroom*”. NCTM. 2º Ed.

[B2] Belhoste, B. (1985). “*Cauchy, Um Mathématicien Légitimiste au XIX Siècle*”. Librairie Classique Eugène Belin.

[B3] Botazzini, U. (1994). “Solving higher-degree equations”, in Grattan-Guinness, I. *Companion Encyclopedia of History and Philosophy of the Mathematical Sciences*. London & New York. Routledge, vol 1.4.11 p 567-572.

[D1] Domingues, Hygino H. (2000). “*Síntese da História das Equações Algébricas*”. São José do Rio Preto, SP: SBEM.

[E1] Edwards, H. M. (1984). “*Galois Theory*”. New York: Springer-Verlag. Graduate Texts in Mathematics 101.

[E2] Eves, H. (1995). “*Introdução à História da Matemática*”. Trad Hygino H. Domingues. Campinas. Ed da Unicamp.

[F1] Fauvel, J & van Maanen, J. (org) (2000). “*History in Mathematics Education. An ICMI Study*”. Amsterdam: Kluwer Academic Publishers.

[G1] Galois, E. (1984). “*Sur lês conditions de résolubilité des équations par radicaux*”. Trad. Harold M. Edwards, in *Galois Theory*. New York: Springer-Verlag.

[G2] Gonçalves, A. (2001). “*Introdução à Álgebra*”. Rio de Janeiro: IMPA.

[G3] Grabner, J. V. (1975). “The Mathematician, The Historian, and The History of Mathematics”, in *Historia Mathematica 2* p 439-447.

[K1] Katz, V. J. (1993). “*A History of Mathematics – an introduction*”. New York: Harper College Publishers.

[K2] Kiernan, B. M. (1971). “The Development of Galois Theory from Lagrange to Artin” in *Arch. Hist. Exact. Sci*, 8 p 40-154.

[L1] Lins, R. C. & Gimenez, J. (1997). “*Perspectivas em Aritmética e Álgebra para o Século XXI*”. Campinas: Papirus.

[M1] Miguel, A. (1997). “As Potencialidades Pedagógicas da História da Matemática em Questão: Argumentos Reforçadores e Questionadores” in *Zetetiké Vol 5 n° 8* p 73-105.

[M2] Miguel A., Miorim M. A. (2004) “*História na Educação Matemática – propostas e desafios*”. Belo Horizonte. Autêntica.

[M3] Milies, C. P. (2004) “*Breve História da Álgebra Abstrata*”. II Bienal da Sociedade Brasileira de Matemática (www.bienasbm.ufba.br/M18.pdf).

[M4] Moreira, P. C. & David, M. M. S. (2005). “*A formação matemática do professor – Licenciatura e prática docente escolar*”. Belo Horizonte: Autêntica.

[N1] Nobre, S.R. & Baroni, R. L. S.(1999). “A pesquisa em História da Matemática e suas relações com a Educação Matemática” in *Pesquisa em Educação Matemática: concepções & perspectivas*. cap. 7 p 129-136. São Paulo: Editora Unesp..

[N2] Nobre S. R. & Teixeira, M. V. & Baroni, R. L. S. (2004). “A Investigação Científica em História da Matemática e suas Relações com o Programa de Pós-Graduação em Educação Matemática” in Bicudo, M. A. V. & Borba, M. C. (org) *Educação matemática : pesquisa em movimento* p 164-185. São Paulo: Cortez Editora

[N3] Nobre, S. R. (2003). “*História da Resolução da Equação de 2º Grau: Uma Abordagem Pedagógica*”. Coleção História da Matemática para Professores. Rio Claro: SBHMat.

[R1] Rigatelli, L. T. (1994). “The theory of equations from Cardano to Galois” in Grattan-Guinness, I. *Companion Encyclopedia of History and Philosophy of the Mathematical Sciences*. London & New York. Routledge, vol 1.6.1 p 713-721.

[S1] Smith, D. E. (1959). “*A Source Book in Mathematics*”. Dover Publications: New York.

[S2] Stillwell, J.(1989). “*Mathematics and Its History*”. Springer-Verlag: New York. Undergraduate Texts in Mathematics.

[S3] Stillwell, J.(1994). “*Elements of Algebra*”. Springer-Verlag: New York. Undergraduate Texts in Mathematics.

ANEXO

O artigo "*Sur les conditions de résolubilité des équations par radicaux*", por Evariste Galois