

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

Uma Análise da “Parte Primeira” da Obra
“Sulla Risoluzione Delle Equazioni Algebriche”, de Enrico Betti.

César Ricardo P. Martins

Orientador : Prof. Dr. Marcos Vieira Teixeira

Tese de Doutorado, 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
2012

512 Martins, Cesar Ricardo Peon
M379a Uma análise da "Parte Primeira" da obra "Sulla
Risoluzione Delle Equazioni Algebriche", de Enrico Betti. /
Cesar Ricardo Peon Martins. - Rio Claro : [s.n.], 2012
74 f. : il.

Tese (doutorado) - Universidade Estadual Paulista,
Instituto de Geociências e Ciências Exatas
Orientador: Marcos Vieira Teixeira

1. Álgebra. 2. Gallois. 3. Equações. 4. Grupos. 5.
Permutações. I. Título.

Comissão Examinadora

Prof. Dr. Marcos Vieira Teixeira (Orientador)

Prof. Dr. Ubiratan D'Ambrósio

Profa. Dra. Iris Dias

Prof. Dr. Henrique Lazari

Prof. Dr. Fábio Maia Bertato

Aluno: Cesar Ricardo Peon Martins

Rio Claro, 26 de Abril de 2012

ÍNDICE

Introdução	1
Capítulo 1. Uma Biografia de Enrico Betti.	2
1.1 Sobre a Vida Acadêmica e Profissional	2
1.2 Sobre o Trabalho Científico	9
Capítulo 2. Um Breve Histórico sobre a Teoria das Equações Algébricas e sobre as Origens da Teoria de Grupos.	13
2.1 A Teoria das Equações.	13
2.2 As Origens da Teoria de Grupos e das Estruturas Algébricas.	18
2.3 Algumas Relações Matemáticas entre os Principais Conceitos Desenvolvidos por Cardano e Lagrange	21
2.4 As Ideias de Galois	28
Capítulo 3. “ <i>Sulla Risoluzione Delle Equazioni Algebriche</i> ”.	35
3.1 Preliminares	35
3.2 Parte Primeira	36
3.2.1 Capítulo Primeiro	36
3.2.2 Capítulo Segundo	46
3.2.3 Capítulo Terceiro	57
Considerações Finais.	69
Bibliografia	71
Anexo – A obra <i>Sulla Risoluzione Delle Equazioni Algebriche</i> .	

Resumo

No presente trabalho apresentamos uma análise da a “Parte Primeira” da obra “*Sulla Risoluzione Delle Equazioni Algebriche*” (1852), de Enrico Betti (1823–1892). Com foco na Teoria das Equações Algébricas, ela pode também ser elencada como as obras que pertencem à fase embrionária da Teoria de Grupos, uma vez que a parte citada contempla a então chamada Teoria das Substituições, que envolve os conceitos de permutação, grupo de permutação, sub-grupo e sub-grupo normal, entre outros. Iremos apresentar seu conteúdo matemático, relacionando-o com a forma com que hoje é estudado, como também, os fatos históricos e os resultados matemáticos anteriores aos abordados pela obra citada, principalmente aos que se referem à vida e obra de Evariste Galois (1811-1832).

Abstract

We present an analysis of the “First Part” of the work “*Sulla Risoluzione Delle Equazioni Algebriche*” (1852), Enrico Betti (1823–1892). Focusing on the Theory of Algebraic Equations, it can also be classified as works belonging to the early stage of the Theory of Groups, since the portion cited includes the so-called Theory of substitutions, which involves the concepts of permutation, permutation group, sub-group or sub-normal group, among others. We will present its mathematical content, linking it with the way today is studied, as well as the historical facts and mathematical results covered by the previous work cited, especially those that relate to the life and work of Evariste Galois (1811 -1832).

INTRODUÇÃO.

O presente trabalho tem como objetivo utilizar as concepções e as propriedades da História da Matemática como objeto de pesquisa em Educação Matemática, na análise e interpretação da “Parte Primeira” da obra “*Sulla Risoluzione Delle Equazioni Algebriche*” (1852), de Enrico Betti (1823–1892).

Essa obra, cujo foco está na Teoria das Equações Algébricas, pode também ser elencada como as que pertencem à fase embrionária da Teoria de Grupos, uma vez que a parte citada contempla a então chamada Teoria das Substituições, que envolve os conceitos de permutação, grupo de permutação, sub-grupo e sub-grupo normal, entre outros.

Priorizando a apresentação do conteúdo matemático desenvolvido e dos fatos históricos relacionados com o período de sua publicação, nosso trabalho está inserido na perspectiva do chamado desenvolvimento histórico de uma teoria, uma vez que a relacionamos tanto com os fatos históricos e resultados matemáticos anteriores aos abordados pela obra citada – principalmente no que se refere à vida e obra de Évariste Galois – quanto com a forma com que trabalhamos esses conceitos atualmente.

No primeiro capítulo fazemos um breve histórico da vida e obra de Enrico Betti. No segundo capítulo exibimos uma descrição geral da História da Teoria das Equações Algébricas, elencando seus principais personagens, e destacando aquelas que consideramos as relações matemáticas fundamentais para o seu desenvolvimento. Faremos isso por meio de sínteses e recortes de nossa dissertação de mestrado [M1]. No terceiro capítulo, propomos uma análise do texto acima citado, que trazemos em anexo a partir da página 75.

CAPÍTULO 1. Uma Biografia de Enrico Betti.

1.1 Sobre a vida acadêmica e profissional.

Enrico Betti nasceu em 21 de Outubro de 1823, em Pistoia, no então Grão-ducado da Toscana (atualmente, comuna italiana da região do Lácio, província de Viterbo; localizada no centro-oeste do país, ao norte de Roma). Morreu em 11 de Agosto de 1892, em Soiana, Pisa – Reino da Itália.

O pai de Enrico Betti, Matteo Betti, morreu quando ele ainda era muito jovem e sua mãe, Francesca Dei, teve de educá-lo por conta própria. Betti estudou Matemática e Física na Universidade de Pisa, graduando-se em Matemática em 1846. Em seguida, foi nomeado professor assistente nessa Universidade e enquanto lá permaneceu, foi orientado por Ottaviano Fabrizio Mossotti (Novara, 1791 – Pisa, 1863), matemático, físico e astrônomo; junto com Betti, um dos fundadores da *Scuola Normale Superiore* de Pisa, dedicada à formação de professores.

Alcançou pleno reconhecimento por sua dedicação à Matemática, como também conciliou ciência e política em vários períodos de sua vida – aspecto característico nos cientistas italianos à época, que tinham por preocupação estruturar e organizar a ciência e a educação da Itália como país em formação – participando, primeiro de levantes revolucionários e depois, de contribuições à administração pública.

Já em 1848, ainda que empenhado em alcançar um posto em uma universidade e talvez por influência de seu orientador, participou efetivamente de um evento militar, que teve por objetivo a unificação da Itália como país.

Na realidade, desde 1815, militantes dessa causa se organizaram e, enquanto Betti se graduava, até sua formatura, tais eventos – que faziam parte do movimento conhecido como *Risorgimento* – foram se intensificando. O *Risorgimento* buscou entre 1815 e 1870 unificar a Itália, que era apenas uma coleção de pequenos Estados submetidos a potências estrangeiras, impostos pelo Congresso de Viena (1814–1815), devido à anexação desse território por Napoleão Bonaparte, desde 1796.

Pode-se dividir tal movimento em duas fases distintas. Na primeira, até 1849, desenvolveram-se vários levantes revolucionários, bem como a chamada primeira guerra de independência italiana, contra o Império Austríaco, com início em 1848, e vitória austríaca. A segunda fase, completada em 1870 com a anexação de Roma, teve seu apogeu no período 1859-1860 com o desenrolar de uma segunda guerra que culminou na criação do Reino da Itália, em 17 de Março de 1861, sem a inclusão das cidades de Roma e Veneza (essa última, anexada em 1866).

Mossotti, desde sempre, ativista dessa causa (chegou a se exilar entre 1825 e 1839), apoiou fortemente a luta pela independência liderando, na primeira guerra, o batalhão da Universidade da Toscana. Betti uniu-se a esse batalhão e lutou na batalha de *Curtatone e Montanara*, em 29 de Maio de 1848. Essa é considerada a maior expressão da participação dos cientistas no *Risorgimento*.

Após esse envolvimento – o único dessa natureza – Betti retornou à sua cidade natal, Pistoia, tornando-se, em 1849, professor de matemática do ensino secundário. Em 1854, assumiu uma cadeira no departamento de ensino superior do novo Liceu de Firenze. Depois de um ano de estudo preparatório, realizou o exame de Bacharel, primeiro título conquistado, que o habilitou a trabalhar tanto na Universidade quanto no Liceu Fiorentino, pois o programa adotado era o mesmo nas duas instituições, e em 1857, assume a cadeira de Álgebra Superior da Universidade de Pisa.

No que diz respeito a sua atuação como pesquisador, entre 1853 e 1857, Betti realizou algumas publicações no periódico *Annali di Scienze Matematiche e Fisiche*, fundado em 1850 por Barnaba Tortolini (1808-1874), sendo essa revista a principal referência para a matemática italiana.

Por outro lado, esse periódico não acompanhava as principais descobertas matemáticas num âmbito europeu, nem tão pouco a matemática italiana desenvolvida nessa época, considerando o momento de construção do país, era reconhecida no estrangeiro. Em parte, essa característica ocorria devido a uma centralização de Tortolini na direção e editoração da revista, uma vez que seria necessário um maior número de colaboradores para essa função. Preocupado com essa situação, o matemático Francesco Brioschi (1824-1897) decide assumir, em 1857,

a redação da revista, tendo como coadjuvantes Betti e Angelo Genocchi (1817–1889), solicitando à Tortoloni uma direção compartilhada.

Consciente das necessidades de, em primeiro lugar, apresentar o trabalho matemático produzido na Itália, e também de promover esse desenvolvimento em um contexto internacional, em Setembro de 1858 visitou centros matemáticos na Europa, junto com Francesco Brioschi e Felice Casorati (1835–1890); e esse feito, com referência aos três matemáticos, realmente simboliza o ingresso da matemática italiana na comunidade científica européia.

A primeira parada foi em Paris, onde encontraram Charles Hermite (1822–1901) e Joseph Louis François Bertrand (1822–1900). Em seguida, foram a Berlim, contatando Karl Theodor Wilhelm Weierstrass (1815–1897), Leopold Kronecker (1823–1891) e Ernst Eduard Kummer (1810–1893); e por último, se dirigiram à Göttingen, estabelecendo amizade com Johann Peter Gustav Lejeune Dirichlet (1805–1859), Julius Wilhelm Richard Dedekind (1831–1916) e Georg Friedrich Bernhard Riemann (1826–1866). Em particular, Betti ficou amigo de Riemann, que o influenciou em futuras pesquisas, iniciadas em 1863.

Tal viagem também transformou a atitude dos três matemáticos italianos. Ao retornarem, em 1859, viram-se estimulados a prosseguir suas pesquisas naquela direção de desenvolvimento da matemática inserida em um contexto europeu; e esse aspecto se deu tanto no campo do desenvolvimento científico pessoal, quanto no que diz respeito à iniciação de uma nova geração de matemáticos, que agora se titulavam inseridos nesse contexto.

Betti, em retorno à Universidade de Pisa, ocupou a cadeira de Análise e Geometria Superior. Essa instituição se revelou rica em atrair jovens com perfis apropriados à pesquisa em matemática e, assim, Betti se tornou a referência para toda essa nova geração, sendo o propulsor da pesquisa na Itália, nesse período.

Por outro lado, após a ocorrência da Segunda Guerra de Independência, as atividades políticas se voltaram para a discussão da estrutura governamental do novo país, e Betti se tornou membro do Parlamento desse novo país em 1862.

Em paralelo a essa nova atividade, e por influência de sua amizade com Riemann que se instalou em Pisa entre 1863 e 1865, começa a dedicar-se à Física-

Matemática, mudando sua linha de pesquisa de tal maneira que, por seu trabalho de 1871, é considerado um dos fundadores da topologia. Foi reitor da Universidade de Pisa e em 1864 tornou-se diretor da *Scuola Normale Superiore*, onde permaneceu até sua morte. Sob sua liderança, essa instituição se tornou o principal centro para pesquisas em Matemática e Educação Matemática, considerando o interesse pelo tema, trazido pela criação do país.

O'Connor e Robertson [C1] citam a descrição de Ettore Carruccio (1908–1980), sobre como Betti concebe o ensino de Matemática:

– ... *gostando de cultura clássica patrocinou, junto com Brioschi, o retorno do ensino de Euclides no ensino secundário, por considerarem esse trabalho um modelo de disciplina e beleza.*

Eles aprofundaram esse objetivo traduzindo *Os Elementos*. E sozinho, Betti traduziu o *Traité élémentaire d'algèbre* (1850), um dos livros didáticos de Bertrand.

Ainda em 1864, Betti sucedeu Mossotti, nomeado para a cadeira de Física-Matemática. Em 1870, trocou a cadeira de Mecânica Celeste pela de Análise e Geometria. Apesar desses movimentos acadêmicos, continuou desempenhando um papel político no desenvolvimento do país, atuando como Secretário Geral do Ministério da Instrução Pública, de Outubro de 1874 à Março de 1876, e em 1884, foi uma vez mais, senador no parlamento italiano.

À título de complemento, segue seu obituário, elaborado por Ulisse Dini (1845–1918), um de seus ex-estudantes:

“Il giorno 11 agosto del decorso anno 1892 fu giorno di grave lutto per la Università nostra, per la scienza, per la Patria.

Enrico Betti che tanto aveva contribuito al progresso della Scienza e a portare in alto il nome della nostra facoltà matematica, in quel giorno, quieto come sempre visse, quasi improvvisamente moriva nella sua villa di Sojana.

Di lui, della bontà dell'animo suo, del suo affetto alla scienza che coltivò con tanto successo, dell'amore che poneva nell'istruire i giovani di questa Università, nell'eccitarli allo studio, e nell'invogliarli a contribuire un giorno essi pure al progresso scientifico, male può dirsi

adeguatamente nelle poche pagine che in questo annuario possono riserbarsi al ricordo di un collega, sia pur questo un collega amatissimo. I colleghi, e primi fra essi quelli che lo ebbero a maestro ben tutto questo di lui ricordano; in tutti poi l'immagine cara e venerata di lui, il ricordo delle sue tante virtù restano ancora e resteranno scolpite per sempre.

Enrico Betti nacque nei pressi di Pistoia il 21 ottobre 1823 da Matteo Betti e Francesca Dei. Mortogli il padre mentre era ancor bambino, restò insieme alle sorelle Luisa e Laura che morirono la prima ancor nubile, e l'altra in ancor giovane età, affidato alle cure della madre, la quale col meschino reddito di due casupole in Pistoia, e col suo lavoro attese alla educazione dei figli. Così poté giungere a compiere gli studii classici nel Liceo Forteguerri di Pistoia, e essere poi mandato a Pisa alla Università, dove soltanto con un posto di studio che i brillanti esami da lui sostenuti gli permisero di conseguire, e col meschino retribuito di lezioni private che dava poté procacciarsi i mezzi per campare modestamente la vita. Fino d'allora tanto potevano in lui l'ingegno, l'amore allo studio e la ferrea volontà; qualità queste che dovevano tanto e poi sì efficacemente manifestarsi in lui nell'avvenire!

Laureato in matematiche pure e, applicate nel 1846, e subito dopo ajuto a una cattedra universitaria, attese sempre più a perfezionare la sua cultura scientifica; e certo fin d'allora la Scienza avrebbe avuto da registrare qualche importante lavoro di lui se le vicende politiche di quel tempo non ne lo avessero distolto. Erano gli anni che precedevano i fortunosi eventi del 1848, ed egli, nell'ambiente universitario, caldo come tanti altri del suo tempo per amore di patria e di libertà, non poteva non lasciarsi trascinare anche dall'affetto per queste. Corse perciò cogli altri nel 1848 nel Battaglione Universitario sui campi di Lombardia dove prese parte alla memoranda giornata di Curtatone, dopo di ché, volte malauguratamente in peggio le sorti della patria, tornò agli studii prediletti; e può dirsi che da quell'epoca incominciò quella sua vita scientifica che tanto doveva portare in alto il suo nome, e che durò fino a poco tempo prima della sua morte.

Il bisogno di procurarsi di che vivere lo costrinse ad accettare un posto d'insegnante di matematiche nel Liceo di Pistoia, retribuito dapprima col meschino stipendio di £. 756 all'anno che fu poi portato a £. 1008 nell'anno successivo quando fu nominato titolare; ma, malgrado le strettezze della vita, sue sole cure furono anche allora l'insegnamento e il culto della scienza.

I lavori di Abel e di Galois sulle equazioni, da questi geometri lasciati incompiuti, e in parte non ché sviluppati soltanto enunciati, attrassero pei primi l'attenzione di lui; e i risultati dei suoi studi delle sue ricerche profonde, consegnati in tante memorie negli annali di scienze fisiche e matematiche del prof. Tortolini, ben presto lo fecero conoscere, fra noi e fuori, come uno dei primi matematici dei nostri tempi.

Non poteva perciò il giovane matematico restare lungamente nell'umile posto da lui occupato nel Liceo di Pistoia, e lo troviamo quindi nel 1854 professore nel Liceo di Firenze, e nel 1857 professore di Algebra superiore in questa Università. Passò poi nell'anno 1859 all'Analisi e geometria superiore, e nel 1863 dopo morto il Mossotti anche alla cattedra di Fisica matematica che conservò finché visse, mentre nel 1870 lasciò l'insegnamento dell'Analisi e geometria superiore per sostituirvi quello della Meccanica celeste che prese allora in seguito alla morte del prof. Lavagna; e così dal 1857 in poi dettò non interrotte le sue lezioni su varii rami della scienza matematica in questa Università fino a tutto l'anno scolastico 1890-91.

Avrebbe voluto continuarle anche nell'anno decorso, ma la lenta paralisi che già fino dal novembre 1890 si era disgraziatamente manifestata in lui pur troppo non glielo permise.

I suoi 34 anni d'insegnamento universitario misero in chiara luce sempre più quale alto ingegno matematico egli si fosse, perocché in ogni parte dei varii rami della scienza dei quali ebbe ad occuparsi per l'insegnamento si trovano tracce di lui, del suo alto sapere delle sue profonde investigazioni. I suoi lavori sulle equazioni per l'algebra; quelli sulle funzioni ellittiche, sulle funzioni algebriche di una variabile complessa, sugli spazii a più dimensioni ecc. per l'analisi e per le applicazioni di questa alla geometria; i tanti lavori di fisica matematica e di meccanica celeste sulla teorica delle forze newtoniane, sul calore, sulla elettricità, sul magnetismo, sulla elasticità, sulla capillarità, sulla idrodinamica, sui moti di sistemi di punti, sulla estensione dei principii della dinamica ecc. mostrano tutti come, sol che si dedicasse allo studio di una parte qualsiasi delle scienze matematiche, egli rinveniva o un nuovo vero da scoprire o una nuova via da aprire al progresso scientifico. Bene a ragione quindi l'Accademia dei Lincei che lo ebbe per tanti anni fra i suoi membri più illustri volle di tutti i suoi lavori riuniti decretare la ristampa.

Tutto dedicato alle matematiche, a svilupparle ogni giorno di più, a infonderne l'amore ai giovani studiosi, non dimenticò però gli studii letterarii e filosofici, e ad essi pure dedicava sempre qualche ora del giorno; per modo che fu versatissimo anche in questo genere di studii. Né lasciò di attendere a tutto quello che attiene alla pubblica istruzione, tantoché poté sedere nel Consiglio superiore di P.I. da quando questo fu ricostituito nel 1867 fino a pochi mesi avanti la sua morte; fu sempre chiamato dal Governo a far parte delle commissioni più importanti per lo studio di cose relative ai varii rami dell'insegnamento; fu segretario generale del Ministero di Pubblica Istruzione dall'ottobre 1874 al marzo 1876; e oltre a insegnare nella Università diresse dal 1865 in poi la nostra Scuola normale superiore che, sotto di lui poté venire in tanto onore, e dare tanti dei migliori insegnanti attuali non solo alle nostre scuole secondarie, ma anche alle Università, sì per le lettere che per le scienze.

Salito in tanta fama pei suoi lavori scientifici, venne nominato socio o corrispondente delle varie accademie o Società italiane, come di molte straniere, fra le quali sono a citarsi quelle di Berlino, Gottinga, Londra, Stoccolma, ecc., e fu decorato del merito civile di Savoia. Conosciuto da tutti oltre che pei suoi lavori, anche per la sua rettitudine, e pel suo amore alla patria e alla libertà, fu per varie volte chiamato da uno dei Collegi della sua città natale a rappresentarlo in Parlamento, subito dopo la costituzione del Regno d'Italia; e fu poi nominato senatore del Regno nel 1884.

La paralisi che negli ultimi 18 o 20 mesi della sua vita lo andava lentamente consumando pose fine a tanta operosità scientifica, e tolse poi alla scienza e alla patria un uomo che tanto l'aveva illustrata, e che più avrebbe certamente potuto illustrarla se fosse ancora vissuto. La sua morte avvenne quando, essendo chiusa l'Università, la maggior parte dei Professori e degli studenti erano assenti; ma malgrado questo, le onoranze che gli furono rese furono ancora solenni, perocché il Municipio nostro volle decretargli onorata sepoltura nel suo celebre camposanto urbano, e oltre ai colleghi e agli scolari presenti buon numero di cittadini vollero prendere parte alla funebre cerimonia dell'accompagnamento della sua salma, tutti compresi di dolore per la dipartita dal mondo di lui che tanto avevano amato e stimato in vita.

Ed ora Enrico Betti non è più; ma il ricordo delle sue belle qualità di mente e di cuore vive e vivrà perenne in tutti e specialmente in coloro che lo ebbero a collega o maestro amatissimo, e in tutti quelli che hanno il culto della Scienza. Il monumento che a cura della nostra Facoltà di matematiche e di tanti scienziati e amici e ammiratori di lui gli sarà eretto nel nostro Camposanto varrà a ricordarlo anche ai pisani; ma più di ogni altra cosa, e qui non solo, ma in tutto il mondo scientifico, e anche in epoche da noi lontane, varranno a ricordarlo i suoi lavori che senza dubbio lasceranno tracce incancellabili nella Scienza”.

ULISSE DINI

Da: Annuario della R. Università di Pisa per l'anno accademico 1891-1892

1.2 Sobre o trabalho científico.

Betti é lembrado por suas contribuições à Álgebra e à Topologia. Sua *Opere Matematiche*, [B5], é composta de 64 artigos, não somente nas áreas acima mencionadas, mas também em física-matemática e na área do ensino de matemática. Publicou em renomados periódicos científicos europeus, desde 1850 até 1889.

Mostrou ser um pesquisador nato e dedicado. Segundo Nagliati, [N1], além de se dedicar à leitura de diversas obras e de se empenhar em assumir uma cadeira universitária, (o primeiro cargo por ele assumido em 1854 no Liceu de Firenze também lhe ajudou nessa prática), seus relacionamentos permitiram-lhe manter-se atualizado no campo científico.

Com efeito, Betti mantinha correspondência com diversos matemáticos e cientistas de sua época. Num total de 1.535 cartas, elencamos os nomes mais presentes: Giuseppe Battaglini (1826–1894) (33 cartas.), Giusto Bellavitis (1803–1880) (11 cartas), Eugenio Beltrami (1835–1900) (11 cartas), Pietro Blaserna (5 cartas), Francesco Brioschi (1824–1897) (61 cartas), Luigi Cremona (1830–1903) (25 cartas), Ulisse Dini (1845–1918) (22 cartas), Riccardo Felici (48 cartas), Angelo Forti (7 cartas), Angelo Genocchi (1817–1889) (51 cartas), Francesco Magni (9 cartas), Luigi Pacinotti (18 cartas), Placido Tardy (1816–1859) (48 cartas), Barnaba Tortolini (1808–1874) (48 cartas). Ocorreram ainda importantes contatos com os matemáticos Kronecker e James Joseph Sylvester (1814–1897).

Em particular, a correspondência com seu orientador, Mossotti (entre 1847 e 1857) foi fundamental para o desenvolvimento de sua primeira pesquisa realizada sem vínculo burocrático com a academia, qual seja, a Teoria das Equações Algébricas, em particular, sobre os resultados de Evariste Galois (1811–1832).

Após publicar uma memória isolada em 1850 sobre física-matemática, *Sopra la determinazione analitica dell'efflusso dei liquidi per una piccolissima apertura* [1850], preocupada com a Teoria Capilar, que apareceu no primeiro número do *Annali di scienze matematiche e fisiche*, o interesse de Betti realmente se voltou à resolução algébrica e analítica de equações.

As obras *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo* [1851], *Sulla risoluzione delle equazioni algebriche* [1852] e *Sopra la teorica delle sostituzioni* [1855], são as mais importantes publicadas por Betti sobre a Teoria de Galois. Nessas, Betti estendeu e deu provas relativas aos conceitos algébricos da Teoria de Galois, proporcionando uma importante contribuição na transição da álgebra clássica para a álgebra moderna, com o reconhecimento de ter sido o primeiro matemático a ter publicado observações sobre essa Teoria, com a demonstração de um teorema enunciado por Galois.

Na primeira memória, *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo* [1851], Betti demonstra, a partir das pesquisas de Lagrange [1770], Niels Abel (1802-1829) [1829] e Carl Johann Malmsten (1814-?) [1847], o teorema enunciado por Galois: “para que uma equação irredutível de grau primo seja resolúvel por radicais, é necessário e suficiente que todas as raízes sejam funções racionais de duas quaisquer entre elas”.

Como complemento a esse primeiro trabalho, publica uma breve nota, *Un teorema sulle risolventi delle equazioni risolubili per radicali* [1851], mostrando alguns resultados obtidos e demonstrando um resultado sobre o resolvente de Lagrange.

Em 1852, na memória *Sulla risoluzione delle equazioni algebriche* (que representa a contribuição mais importante entre as três acima elencadas), Betti tentou tratar de três problemas, a saber:

- (i) a determinação da condição necessária e suficiente para que uma equação irredutível seja resolúvel por radicais,
- (ii) a determinação da condição necessária e suficiente para a obtenção das raízes da equação de grau imediatamente inferior ao grau da equação proposta e,
- (iii) a determinação da equação que definiu o mais simples irracional que exprime a raiz da equação proposta, considerando resolvido completamente o problema (i), conforme os fragmentos de Galois.

Nessa memória Betti estaria preocupado em expor, como ele mesmo disse, “uma simples e fácil Teoria das Substituições”, com a intenção de realizar uma “exposição incomparavelmente mais clara” da que estava publicada sobre esse argumento.

Todavia a leitura de tal trabalho é difícil e confusa quando se trata do conceito de subgrupo e grupo quociente. Apesar de Marie Ennemond Camille Jordan (1838 – 1922), em seu *Traité des substitutions et des equations algebriques* [1870], ter creditado a Betti tanto o preenchimento de lacunas nos argumentos de Galois, quanto ter sido o primeiro a estabelecer, rigorosamente, a seqüência dos teoremas de Galois, a verdade é que seu trabalho contém erros conceituais. Mammone [M1] aponta tais erros; porém esse seu trabalho também contém erros na teoria de grupos, apontados na revisão do algebrista britânico Peter Neumann (1940). Nagliati [N1] afirma que a causa desse problema é que a memória de Betti foi recebida com dificuldade no ambiente matemático europeu.

O próprio Betti se preocupava com a difusão de sua ideia no estrangeiro, e no último mês de 1851 submeteu seu estudo à Guglielmo Libri (1803–1869), a personalidade matemática italiana que, talvez, teria a maior fama na Europa, mas que por outro lado já se encontrava inativo do ponto de vista matemático.

Em Setembro de 1854, ainda com o objetivo de buscar uma melhor recepção no ambiente matemático europeu para essa pesquisa se dispôs a analisar a avaliação de seu trabalho, feita por Sylvester, que escreveu a Mossotti em 11 de Abril de 1855, convidando Betti a publicar notas de esclarecimento em vários pontos da memória.

Betti reescreve sua Teoria de Grupo de Substituição na memória de 1855, *Sopra la teorica delle sostituzioni*, na qual faz referência a Sylvester. A memória vem escrita com uma terminologia e um sistema de notação que reflete aquele introduzido por Augustin Louis Cauchy (1789–1857) nos anos 40.

Muito provavelmente, situações como esta podem tê-lo levado a ser editor do *Annali di matematica pura ed applicata*, junto com Brioschi, Tortolini e Angelo Genocchi (1817-1899). Esse periódico substituiu, em 1857, o *Annali di Scienze matematiche e fisiche*, primeira revista italiana de matemática e física, publicada em 1850 em Roma por Tortolini, periódico que tinha por principal objetivo fazer

conhecido o trabalho italiano no estrangeiro, e de fazer conhecer na Itália as mais diferentes linhas de pesquisa da Europa.

Por outro lado, Kronecker, escreve sobre o problema levantado por Betti em 1852, qual seja de determinar “a forma efetiva das raízes da equação resolúvel”. Kronecker tinha terminado esse cálculo para a equação de grau primo e o seu trabalho foi apresentado na Academia de Berlin, de Dirichlet (1805-1859).

Betti então, com um tratamento analítico, melhorou o resultado de Kronecker, estendendo-o às equações de grau primo na memória de 1855, *Sopra la più generale funzione algebrica che può soddisfare una equazione, il grado della quale è potenza di un numero primo*.

Um pouco antes, em 1854, mostrou que a equação quártica pode ser resolvida por meio de integrais, resultando em funções elípticas; e assim pesquisou sobre Funções Elípticas e em Funções Algébricas de Variáveis Complexas entre 1860 e 1863.

Como mencionamos, devido a Riemann, mudou sua linha de pesquisa, passando a se dedicar à Física-Matemática e realizando um importante trabalho em física teórica, em particular em teoria potencial e elasticidade. Foi essa mudança para física-matemática que o conduziu Betti à herdar a cadeira de Mossotti em Pisa, como já acima mencionado, e Dini foi nomeado como seu sucessor na cadeira de Análise e Geometria Superior.

Enfim, Betti ainda é considerado um dos fundadores da topologia, dada a publicação de uma memória em 1871, no qual vem a determinar os invariantes chamados *números de Betti*, assim nomeados por Poincaré, que estudou topologia por intermédio dessa obra.

Como pesquisador, orientou os seguintes alunos: Ulisse Dini (1845–1918), Cesare Arzelà (1847–1912), Gregorio Ricci-Curbastro (1853–1925), Luigi Bianchi (1856–1928), Vito Volterra (1860–1940), Federigo Enriques (1871–1946).

CAPÍTULO 2. Um Breve Histórico sobre a Teoria das Equações Algébricas e sobre as Origens da Teoria de Grupos.

2.1 A Teoria das Equações.

Como já dissemos em [M3], podemos resumir a História das Equações Algébricas como a história da busca de métodos para exhibir as soluções de uma dada equação de qualquer grau, por meio de radicais.

Exibir as soluções uma dada equação de grau n , por meio de radicais (isto é, encontrar as suas soluções algébricas) significa encontrar estas soluções por meio da manipulação de seus coeficientes através das quatro operações aritméticas e extração de raízes. Tal procedimento aplica-se de maneira geral para quaisquer equações de graus inferiores a cinco; para aquelas com grau superior a quatro, obtemos soluções algébricas somente em casos particulares.

Entretanto, as primeiras generalizações desse procedimento somente começam a ocorrer no final do século XVI. Até meados do século XVI sabia-se, por esse método, resolver muitos ‘tipos’ de equações do segundo grau e algumas do terceiro grau, pelos trabalhos dos matemáticos árabes. Essas equações algébricas eram classificadas de modo que as raízes negativas e iguais a zero fossem evitadas. Em 1545, Girolamo Cardano (1501-1576) publica, em meio a disputas, brigas e traições, a obra “*Ars Magna*”, onde nos apresenta os procedimentos para a resolução das equações cúbicas e quárticas. Nesse trabalho, Cardano analisou cada caso distinto da equação cúbica completa (isto é, classificou as equações em ‘tipos’), transformando cada equação em uma outra do mesmo grau, sem o termo do 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. Esta iniciativa, inclusive, impulsionou a descoberta dos números complexos.

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.

Era costume dos algebristas desse período reexaminar os métodos conhecidos e buscar soluções diferentes das de Cardano para resolver equações. Entre eles, podemos destacar o algebrista francês François Viète (1540-1603), que pela obra *In artem analyticem isagoge* (1591), construiu seu tratamento às equações algébricas, apresentando um novo método de resolver equações cúbicas e um método particularmente elegante para resolver equações quárticas do tipo $x^4 + 2ax^2 = c - bx$. Porém sua grande contribuição foi dada na evolução do simbolismo algébrico e, por conta disso, estabeleceu uma maneira de generalizar o conhecido procedimento para solução da equação quadrática através da fórmula de Cardano.

Apesar da procura de um método para resolver a equação quártica usando radicais ter tornado-se infrutífera, ela conduziu a alguns resultados interessantes. Entre eles o de Ehrenfried von Tschirnhaus (1651-1708), que 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 (1707-1783) 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.

Nesse 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, 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:

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = (x - x_1)(x - x_2) \dots (x - x_n) \quad (1)$$

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 Niels Henrik 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.

Rigatelli, [R1], afirma que o trabalho de Ruffini mostra de forma implícita, alguns conceitos que Évariste 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 permanece inalterada.

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. A importância particular do trabalho de Abel "*Memoire sur une classe particulière d'equations résolubles algébriquement*" (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.

Évariste Galois, depois de analisar os trabalhos de Lagrange, Ruffini, Cauchy, Abel e Johann Carl Friedrich Gauss (1777-1855), iria mostrar, como dissemos, 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*".

Galois é considerado um dos fundadores 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 se quer estudar no primeiro. 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 ideia 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 se quer estudar no primeiro – é típico da álgebra moderna. Galois usou, sem definir, conceitos atualmente chamados de grupo de permutação, subgrupo, subgrupo normal, grupo quociente e a ideia de Estrutura de Corpo.

2.2 As Origens da Teoria de Grupos e das Estruturas Algébricas.

A publicação e o conseqüente reconhecimento dos trabalhos e das ideias 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 ideia 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.

Como já dissemos, os primeiros textos publicados sobre os trabalhos de Galois foram os de Enrico Betti e esse foi o único avanço na Teoria de Galois até 1870.

Arthur Cayley (1821-1895) 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 ideias 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, publica em 1870 o *Traité des substitutions et des équations algébriques*. Segundo Kiernan, [K2], 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 introduziu o conceito de Corpo, citado por Kiernan [K2]: “Qualquer sistema real ou complexo que satisfaz a propriedade fundamental do fechamento será chamado Corpo”.

Dedekind publica seus resultados no *Zahlentheorie*, em sociedade com Dirichelet, 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, Kronecker 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 racionalidade de Kronecker.

Com o conceito de extensão, é Dedekind que desenvolve a ideia 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 ideias seriam utilizadas por Emil Artin (1898-1962) em sua reformulação da Teoria de Galois. Para Dedekind estas ideias eram óbvias e, portanto ele não as provou. Artin publica *Foundations of Galois Theory* em 1938 e *Galois Theory* em 1942, e com uma abordagem quase idêntica a de Dedekind completa àquela 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, [K2], 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.

Esses trabalhos podem ser considerados como antecessores do trabalho de Artin, 40 anos mais tarde, último tratamento desta Teoria.

2.3 Algumas Relações Matemáticas entre os Principais Conceitos Desenvolvidos por Cardano e Lagrange.

Faremos, neste item e no próximo, a apresentação de algumas relações das ideias matemáticas elaboradas por Cardano e Lagrange, restritas as equações do 4º grau.

Suponha uma equação dada $x^4 + ax^3 + bx^2 + cx + d = 0$, de coeficientes inteiros. O chamado método de Ferrari, apresentado por Lodovico Ferrari (1522–1565) à Cardano, e que foi publicado no *Ars Magna*, como o primeiro método descoberto para a resolução desse tipo de equação, pode ser descrito tal como segue:

Fazendo a mudança de variável $x = y + h$ na equação proposta, eliminaremos o termo ax^3 , por meio de uma escolha conveniente para o valor de h .

Como exemplo, considere a equação $16x^4 - 64x^3 + 72x^2 + 16x - 19 = 0$. Para $h = 1$, obtemos a equação reduzida $y^4 - \frac{3}{2}y^2 = -2y - \frac{21}{16}$.

Nessa última versão da equação, inserimos a expressão $\gamma \cdot y^2 + \beta$ em ambos os lados da igualdade. Isto é,

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

Essa inserção nos leva à fatoração $(y^2 + \sqrt{\beta})^2 = \left(\sqrt{\gamma} \cdot y - \sqrt{\beta - \frac{21}{16}}\right)^2$, com a condição de que

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

E substituindo (I) em (II), recaímos na cúbica $\gamma^3 - 3\gamma^2 - 3\gamma - 4 = 0$ [1].

Se $1, \alpha, \alpha^2$ são as raízes da unidade, as soluções desta cúbica, por Cardano/Lagrange (procedimento descrito em [M3]) 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 $\gamma_1 = 4$ em (II), temos $\sqrt{4\left(\beta - \frac{21}{16}\right)} = 1 \Rightarrow \beta = \frac{25}{16}$

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

e portanto, as quatro raízes da equação reduzida $y^4 - \frac{3}{2}y^2 = -2y - \frac{21}{16}$ são:

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

Entretanto, a escolha por $\gamma_1 = 4$ foi arbitrária.

Poderíamos ter utilizado γ_2 ou γ_3 quando do cálculo do valor de β e, é claro, obteríamos as mesmas quatro raízes descritas acima. Ou, e assim observando esse fato de outra maneira, temos três caminhos diferentes que nos leva às quatro raízes da equação proposta. E isso se aplica em geral.

Mas, e do mesmo modo que para a equação quártica, o método de Cardano para a resolução de equações cúbicas nos leva a duas possibilidades distintas para encontrar as (três) raízes de equações desse grau (v. M[3]).

Considerando a necessidade da resolução de $\gamma^3 - 3\gamma^2 - 3\gamma - 4 = 0$ no exemplo acima, temos, enfim, no procedimento para a solução por radicais da equação do 4º grau, duas possibilidades para encontrar os três caminhos que nos leva às quatro raízes da equação. E, uma vez mais, isso se aplica em geral.

Temos, assim, vinte e quatro valores tais que somente quatro são diferentes entre si.

Verifiquemos o porquê desse resultado, por meio de uma interpretação acerca da pesquisa, nesse tema, de Lagrange.

Preocupado com a unificação e a validação dos diferentes métodos de solução para as equações de grau menor do que cinco, Lagrange propôs uma análise por meio da utilização do que chamou *resolventes* das equações.

Os resolventes foram por ele definidos como funções racionais das raízes das equações propostas. Para equações do grau três, utilizou $t = \frac{1}{3}(x_1 + \alpha.x_2 + \alpha^2.x_3)$, e do grau quatro, utilizou $t = x_1x_2 + x_3x_4$.

Permutando de todas as maneiras possíveis as raízes x_i em t , encontrou 6 expressões diferentes para a função relativa à equação do 3º grau e 24 expressões para a função relativa à equação do 4º grau.

Elevando cada um dos 6 e 24 valores à terceira e à quarta potências, respectivamente, encontrou 2 valores diferentes para o primeiro caso, e 3 valores diferentes para o segundo caso.

E assim, pôde trocar a equação proposta, de grau três ou quatro, por outra de grau dois ou três, respectivamente, redefinindo, dessa maneira alternativa, o princípio básico para a solução de equações por radicais: para resolvermos uma equação de grau n , devemos encontrar uma equação, equivalente à proposta, de grau $n - 1$.

Nessa exposição utilizaremos um resolvente padrão, definido por Betti. A quantidade $t = x_1 + \alpha.x_2 + \alpha^2.x_3 + \dots + \alpha^{n-1}.x_n$ foi chamada por Betti de o *resolvente de Lagrange*, onde $x_1, x_2, x_3, \dots, x_n$ são as raízes da equação de grau n dada, e $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ são as raízes da unidade, equação auxiliar $x^n - 1 = 0$.

Retomemos, então, a equação geral e completa do quarto grau e consideremos 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 suas raízes, que se permutam em t , e $1, \alpha, \alpha^2, \alpha^3$ são as raízes da equação auxiliar $x^4 - 1 = 0$.

Abaixo descrevemos cada uma das vinte e quatro permutações possíveis pondo, por praticidade, $\alpha = -1$ no lugar de $\alpha = i$, para utilizar a simetria induzida por essa adjunção,

$$t_1 = x_1 - x_2 + x_3 - x_4$$

$$t_5 = x_1 - x_2 + x_4 - x_3$$

$$t_2 = x_4 - x_1 + x_2 - x_3 = -t_1$$

$$t_6 = x_3 - x_1 + x_2 - x_4 = -t_5$$

$$t_3 = x_3 - x_4 + x_1 - x_2 = t_1$$

$$t_7 = x_4 - x_3 + x_1 - x_2 = t_5$$

$$t_4 = x_2 - x_3 + x_4 - x_1 = -t_1$$

$$t_8 = x_2 - x_4 + x_3 - x_1 = -t_5$$

$$t_9 = x_1 - x_3 + x_2 - x_4$$

$$t_{13} = x_1 - x_3 + x_4 - x_2$$

$$t_{10} = x_4 - x_1 + x_3 - x_2 = -t_9$$

$$t_{14} = x_2 - x_1 + x_3 - x_4 = -t_{13}$$

$$t_{11} = x_2 - x_4 + x_1 - x_3 = t_9$$

$$t_{15} = x_4 - x_2 + x_1 - x_3 = t_{13}$$

$$t_{12} = x_3 - x_2 + x_4 - x_1 = -t_9$$

$$t_{16} = x_3 - x_4 + x_2 - x_1 = -t_{13}$$

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

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

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

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

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

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

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

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

Devemos interpretar essas vinte e quatro quantidades como duas possibilidades para encontrar os três caminhos que nos leva às quatro raízes da equação, num total de vinte e quatro valores, onde somente quatro serão diferentes entre si.

E ao invés de calcularmos a quarta potência de cada uma das permutações em t , faremos tal como Edwards, [E1], construindo um polinômio g e realizando, pelas igualdades descritas, as trocas das quantidades t_i , em seus fatores, $1 \leq i \leq 24$, como segue:

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

$$= (x-t_1)^2 \cdot (x+t_1)^2 \cdot (x-t_5)^2 \cdot (x+t_5)^2 \cdot (x-t_9)^2 \cdot (x+t_9)^2 \cdot (x-t_{13})^2 \cdot (x+t_{13})^2 \cdot (x-t_{17})^2 \cdot (x+t_{17})^2 \cdot (x-t_{21})^2 \cdot (x+t_{21})^2$$

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

Logo,

$$g(x) = (x-t_1)^4 \cdot (x+t_1)^4 \cdot (x-t_5)^4 \cdot (x+t_5)^4 \cdot (x-t_9)^4 \cdot (x+t_9)^4$$

$$= (x^2 - t_1^2)^4 \cdot (x^2 - t_5^2)^4 \cdot (x^2 - t_9^2)^4$$

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

$$f(x) = (x^2 - t_1^2)(x^2 - t_5^2)(x^2 - t_9^2)$$

$$= x^6 - (t_1^2 + t_5^2 + t_9^2)x^4 + (t_1^2 t_5^2 + t_1^2 t_9^2 + t_5^2 t_9^2)x^2 - (t_1^2 t_5^2 t_9^2)$$

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

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

onde γ_1 , γ_2 , γ_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]:

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

Cada função gera uma raiz para a cúbica [1]. E cada raiz de [1] gera as quatro raízes da equação proposta.

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 nos permite definir as raízes da quártica por meio dos valores $\pm t_1, \pm t_5, \pm t_9$,

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

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

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

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

pois,

$$\begin{aligned} x_1 &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \sqrt[4]{t_1^4} + \sqrt[4]{t_5^4} + \sqrt[4]{t_9^4} \right] = \\ &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + \sqrt[4]{(x_1 - x_2 + x_3 - x_4)^4} + \right. \\ &\quad \left. + \sqrt[4]{(x_1 - x_2 + x_4 - x_3)^4} + \sqrt[4]{(x_1 - x_3 + x_2 - x_4)^4} \right] \\ &= \frac{1}{4} \left[(x_1 + x_2 + x_3 + x_4) + (x_1 - x_2 + x_3 - x_4) + \right. \\ &\quad \left. + (x_1 - x_2 + x_4 - x_3) + (x_1 - x_3 + x_2 - x_4) \right] = \frac{1}{4} \cdot 4x_1 \end{aligned}$$

Analogamente para x_2, x_3, x_4 .

Notemos que a opção na conservação das quantidades $\pm t_1, \pm t_5, \pm t_9$ em g foi tão arbitrária quanto à escolha de γ_1 , quando da resolução do exemplo acima.

Isto porque as quantidades t_i são cíclicas para $t_i, t_{i+1}, t_{i+2}, t_{i+3}; i = 1+k, \dots, 4+k; k = 0, 4, \dots, 20$, isto é,

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

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

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

então, poderemos optar em tomar qualquer t_i que obedeçam essas condições 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 $g(x)$:

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

Com tais escolhas, iríamos 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 escreveríamos as raízes da equação em função de t_1, t_6, t_9 .

E isso mostra que as quantidades $t_i, t_{i+1}, t_{i+2}, t_{i+3}; i = 1+k, \dots, 4+k, k = 0, 4, \dots, 20$, são *invariantes* entre si.

2.4 As Ideias de Galois.

A equação do grau quatro possui soluções por radicais porque obedece a condições específicas, relativas às trocas das quantidades invariantes t_i em g . E foi Galois quem estabeleceu, para uma equação algébrica de grau qualquer, tais condições, que estão diretamente associadas com as propriedades que regem a construção do que ele chamou o *grupo* da equação.

Nosso objetivo, agora, passa a ser o de estabelecer relações entre os conceitos apresentados por Galois e as ideias de Lagrange; vamos associar os polinômios g e f com as propriedades dos chamados *grupos* e *grupos parciais*, para o caso da equação do 4º grau.

Como sabemos, Galois nos diz que, em primeiro lugar, devemos tomar uma função do tipo $V = Aa + Bb + Cc + Dd$, com A, B, C, D números inteiros, e a, b, c, d raízes da equação dada, associando a essa, o polinômio $V = \phi(a, b, c, d)$ ou $V - \phi(a, b, c, d) = 0$.

Devemos multiplicar entre si todas as equações semelhantes a essa, obtidas por todas as permutações definidas por ϕ_i em V , deixando somente uma letra fixa, por exemplo, a letra a , construindo uma equação da forma $F(V, a) = 0$ ou $a = f(V)$, para dela obtermos o valor de a , raiz da equação que se quer resolver, expressada como uma função racional de V :

$$F(V, a) = (V - \phi(a, b, c, d)).(V - \phi(a, d, b, c)).(V - \phi(a, c, d, b)). \\ . (V - \phi(a, c, b, d)).(V - \phi(a, d, c, b)).(V - \phi(a, b, d, c))$$

Essa equação será associada ao grupo da equação proposta.

Antes desse próximo passo, vamos relacionar a construção dessa equação com os procedimentos de Cardano/Ferrari e de Lagrange. Em Ferrari, quando da solução da equação cúbica, obtivemos uma equação de grau 6, que foi reduzida para o grau 3, tal que tínhamos duas possibilidades de encontrar 3 raízes, num total de 6 valores, tal que cada um deles fornece as quatro raízes da equação proposta. E, no

decorrer da análise de Lagrange, o polinômio $g(x)$ é reduzido a uma versão com 6 fatores de multiplicidade 4: $g(x) = f(x)^4$.

Logo, sendo $F(V, a)$ com 6 fatores, podemos sugerir a identificação $F(V, a) \equiv f(x)$, desde que $V \equiv t$ e que exista a possibilidade de reduzir $F(V, a)$ em três fatores.

Daí, se $F(V, a)$ for composta pelos $(V - \phi_i)(V - \phi_j)(V - \phi_k)$, 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 acima, dada a última redução em $g(x)$. E, então obter, racionalmente, o valor de a .

Nesse caso, a identificação $V \equiv t$ é simples e direta. Acima, definimos t_i por meio das permutações das raízes x_1, x_2, x_3, x_4 da equação dada, na expressão racional $t = x_1 - x_2 + x_3 - x_4$. Entretanto, Galois utilizou as letras $a, b, c, \dots$ para se referir as raízes da equação, e a letra ϕ para as permutações em V . Basta adaptarmos a notação para os 24 valores $\phi_i \equiv t_i, 1 \leq i \leq 24$.

Agora, nos voltemos ao próximo passo de Galois: associar à equação $F(V, a) \equiv f(x)$, o grupo (de permutações) da equação de grau quatro, que segue:

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

Observemos que em cada linha do grupo, a letra a está fixa, tal que a primeira linha do grupo representa os fatores da equação $F(V, a)$; as demais linhas serão versões diferentes para $F(V, a)$. Portanto, a disposição das permutações no grupo mostra-nos que podemos construir 4 versões diferentes para essa equação (e

cada uma das 4 linhas do grupo acima são equivalentes entre si; o que completa a identificação $F(V, a) \equiv f(x)$.

Como sabemos, devemos decompor o grupo acima em p (p primo) grupos parciais, sendo que tal decomposição ocorrerá sempre que adjuntarmos as raízes da equação auxiliar na equação proposta.

Logo, as sucessivas reduções no grupo definem cada uma das sucessivas reduções dos fatores do polinômio $g(x)$.

Um grupo é decomposto toda vez que definirmos uma única *substituição* (operação que relaciona duas permutações) que nos faz passar de um grupo parcial para outro, sendo que cada grupo parcial construído deverá conter permutações equivalentes entre si.

Entretanto, Galois nos diz que devemos realizar as decomposições seguindo os passos da solução da equação dada.

Nossa referência é o método de Ferrari, acima exposto: 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.

De acordo com essa seqüência, 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.

O próximo passo é dividir este grupo parcial de 12 elementos, resultante da primeira redução, em $p = 3$ grupos de quatro elementos, que ocorrerá quando da resolução da 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, decomparamos as 24 permutações do grupo total em $24 = 2.3.2.2$.

As substituições que irão dividir o grupo serão definidas tomando como referência as posições das letras, e não as letras.

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

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

Assim, temos que:

(i) a substituição $(3 \rightarrow 4, 4 \rightarrow 3)$ divide¹ o grupo em 2 grupos parciais

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

Considerando a identificação $V \equiv t$, vamos usar ϕ para denotar cada permutação em t e reescrever $g(x)$:

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

Assim, devemos ter:

$$\begin{aligned} g(x) &= (x - \phi_1)(x - \phi_2)(x - \phi_3)(x - \phi_4)(x - \phi_5) \dots (x - \phi_{23})(x - \phi_{24}) = \\ &= (x - \phi_1)^2 (x - \phi_2)^2 (x - \phi_3)^2 (x - \phi_4)^2 (x - \phi_5)^2 (x - \phi_6)^2 \dots (x - \phi_{11})^2 (x - \phi_{12})^2 \end{aligned}$$

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 as mesmas permutações. 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;

¹ 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).

$abcd$	$acdb$	$adbc$
$badc$	$cabd$	$dacb$
$cdab$	$dbac$	$bcad$
$dcba$	$bdca$	$cbda$

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 permutações.

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

$abcd$	$cdab$
$badc$	$dcba$

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

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 $F(V, a) = (x - \phi_1)(x - \phi_5)(x - \phi_9)$, 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:

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

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

Galois afirma sem demonstrar² 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.

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 acima, de forma que:

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

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.

E, vendo isto pelo método de Ferrari, temos a mesma ideia: cada raiz da equação cúbica, inerente ao processo (divisão do grupo de 12 elementos em 3 grupos

²Uma demonstração pode ser encontrada em Edwards [E1], Proposição 46, pags 61-64.

de 4 elementos), fornece as mesmas 4 raízes para a equação dada (as permutações dispostas na mesma coluna são equivalentes, pois são cíclicas).

3. *“Sulla Risoluzione Delle Equazioni Algebriche”*.

3.1 Preliminares.

A obra de Betti – em anexo – está dividida em duas partes. A primeira parte está dividida em três capítulos e trata da chamada Teoria das Substituições. Como dissemos, iremos analisar a Parte Primeira dessa obra. Entendemos que nosso estilo de escrita privilegiará a maneira como a obra foi estruturada no que diz respeito à ordem dos conceitos apresentados. Betti, por vezes, apresenta tais conceitos introduzindo notações diferentes das que conhecemos; em outras situações utiliza-se de linguagem retórica. Entretanto, em momento algum ele se utiliza de exemplos. Por esse motivo, ainda traremos, na medida da necessidade e a título de esclarecer ou ilustrar tais conceitos, exemplos que ilustrarão o que está sendo introduzido.

A segunda parte, dividida em dois capítulos, se preocupa com a Teoria das Equações Algébricas, no que diz respeito às abordagens de Abel e Galois.

Na primeira parte, primeiro capítulo, Betti define os conceitos básicos relativos às substituições: as operações entre substituições e a substituição derivada. No segundo capítulo, caracteriza grupo de substituição definido como as substituições agem nas permutações de tal grupo, em particular de um grupo derivado. No terceiro capítulo, define o que chama de multiplicador e divisor de um grupo, para expor sobre a decomposição de um grupo.

Na segunda parte Betti discute as condições de resolubilidade, por radicais, das equações algébricas, com o apoio do que foi desenvolvido na primeira parte. No primeiro capítulo, aborda as condições de resolubilidade das chamadas equações auxiliares e, no capítulo dois, a resolubilidade para as equações em geral.

3.2 Parte Primeira.

3.2.1 Capítulo Primeiro.

O primeiro capítulo está dividido em duas seções. Na **seção I**, Betti estabelece os princípios para o cálculo das Substituições, e a **seção II** apresenta resultados relativos ao que chamou de *substituição derivada*.

Na **seção I**, ele começa sua exposição definindo *substituição*:

“Uma substituição é a operação mediante a qual se passa de uma para outra permutação de várias quantidades”.

Como Betti não faz qualquer referência à definição de permutação, levaremos em conta que: uma permutação é uma seqüência de n letras, ou símbolos. Por exemplo, tomemos as cinco letras a, b, c, d, e . Podemos dispô-las em 120 sequencias diferentes.

Em seguida, diz: “Usaremos uma só letra x com diversos índices i para distinguir entre eles todas as quantidades que entram nas permutações. Assim poderemos considerar que toda substituição se executa substituindo-se todos os índices i por uma função $\varphi(i)$ dos mesmos e a indicaremos pela notação

$$\begin{pmatrix} x_i \\ x_{\varphi(i)} \end{pmatrix}.$$

Sendo que a função $\varphi(i)$ deverá ter a propriedade de assumir todos os valores de i , numa ordem diferente.

Expandindo-se essa notação, o que Betti não faz, podemos escrever

$$\theta = \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_{\varphi(1)} & x_{\varphi(2)} & x_{\varphi(3)} & \dots & x_{\varphi(n)} \end{pmatrix}.$$

Vamos ilustrar essa notação para $n=5$. Consideremos as permutações $x_1x_2x_3x_4x_5$ e $x_3x_1x_2x_4x_5$. Se θ é a substituição que leva a permutação $x_1x_2x_3x_4x_5$ na permutação $x_3x_1x_2x_4x_5$, isto é

$$\theta = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_1 & x_2 & x_4 & x_5 \end{pmatrix},$$

então, $\varphi(1)=3$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=4$, $\varphi(5)=5$.

Observemos que dado o conjunto $S=\{1, 2, 3, \dots, n\} \subset Z$, o conjunto $G=\{\varphi: S \rightarrow S: \varphi \text{ bijetiva}\}$ é o chamado conjunto das permutações do conjunto S . E cada elemento φ de G , usualmente denotado por

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \varphi(1) & \varphi(2) & \varphi(3) & \dots & \varphi(n) \end{pmatrix},$$

é chamado uma permutação de S .

Assim, as definições de substituição e permutação são, atualmente, um só. Ambas se reduzem à definição de Betti, em que “... toda substituição se executa substituindo-se todos os índices i por uma função $\varphi(i)$ dos mesmos e a indicaremos pela notação $\begin{pmatrix} x_i \\ x_{\varphi(i)} \end{pmatrix}$ ”.

Por outro lado, observamos que para Betti a ordem dos símbolos que entram nas permutações é arbitrária. Isso significa que, no exemplo acima, a substituição θ pode ser indicada por

$$\theta = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_1 & x_2 & x_4 & x_5 \end{pmatrix},$$

ou por $\theta = \begin{pmatrix} x_3 & x_4 & x_2 & x_5 & x_1 \\ x_2 & x_4 & x_1 & x_5 & x_3 \end{pmatrix}$

ou ainda por quaisquer pares de permutações, desde que $\varphi(1)=3, \varphi(2)=1, \varphi(3)=2, \varphi(4)=4, \varphi(5)=5$. O que deixa Betti em acordo ainda maior com a notação moderna, a saber, a notação por ciclos, $\theta=(123)(45)=(213)(54)=\dots$.

Em exemplos futuros na análise dessa obra, por uma questão de padrão com o capítulo anterior, vamos indicar os símbolos das permutações por meio das letras do alfabeto. Por exemplo, se queremos trabalhar com a permutação $x_3x_1x_2x_4x_5$, escreveremos *cabde*.

Para explicitar as substituições, em conformidade com a natureza do exemplo, poderemos usar $\theta = \begin{pmatrix} c & d & b & e & a \\ b & d & a & e & c \end{pmatrix}$, ou $\theta(cdbea) = bdaec$.

Em seguida, Betti introduziu um sistema de índices $\varphi(i)$ dada a natureza do número n de símbolos, e somente começou a utilizá-lo a partir do capítulo terceiro de sua obra. Denotando por p um primo:

- (a) se $n = p$, tomou por índices as p raízes da congruência $i^p \equiv i \pmod{p}$;
- (b) se $n = p^\nu$, tomou por índices as p^ν raízes da congruência $i^{p^\nu} \equiv i \pmod{p}$;
- (c) e se $n = p^\nu \cdot q^\mu \cdot r^\sigma \dots$, tomou por índices as raízes das congruências $k^{p^\nu} \equiv k \pmod{p}, h^{q^\mu} \equiv h \pmod{q}, l^{r^\sigma} \equiv l \pmod{r}, \dots$.

O próximo conceito que Betti apresentou, citando Cauchy como seu introdutor, foi o de *operações sucessivas* com substituições. O resultado dessas operações será equivalente a uma única substituição φ , indicada pela notação:

$$\varphi = \theta_0 \theta_1 \theta_2 \dots \theta_{n-1}.$$

Esse conceito de operação sucessiva é o que hoje chamamos de composição de funções. Devemos observar que para Betti, a substituição $\varphi = \theta_0 \theta_1 \theta_2 \dots \theta_{n-1}$ é obtida primeiro aplicando-se θ_0 à uma permutação; em seguida, ao resultado, aplica-se θ_1 ; e assim por diante até a aplicação de θ_{n-1} .

Por exemplo, tome a substituição θ_0 , a operação que leva a permutação $abcd$ na permutação $bcad$, por meio da $\varphi_1(i)$, $0 \leq i \leq 3$, tal que $\varphi(0)=2$, $\varphi(1)=0$, $\varphi(2)=1$, $\varphi(3)=3$; e θ_1 a operação que troca, em particular, $abcd$ por $dbca$, por meio da $\varphi_2(i)$, $0 \leq i \leq 3$, tal que $\varphi(0)=3$, $\varphi(1)=1$, $\varphi(2)=2$, $\varphi(3)=0$, isto é, $\theta_0(abcd)=bcad$ e $\theta_1(abcd)=dbca$.

Temos

$$\phi(abcd) = \theta_0(abcd) \cdot \theta_1(abcd) = bcda,$$

e, portanto, ϕ é a substituição definida por $\varphi(0)=1$, $\varphi(1)=2$, $\varphi(2)=3$, $\varphi(3)=0$.

Se $\theta_0 = \theta_1 = \theta_2 = \dots = \theta_{n-1}$, então $\varphi = \underbrace{\theta \cdot \theta \cdot \theta \dots \theta}_{n \text{ vezes}}$, que será denotada por $\varphi = \theta^n$.

E se θ for uma chamada substituição circular sobre p letras, ao realizarmos essa operação p vezes, aplicando-a pela primeira vez numa dada permutação, essas p aplicações reproduzirão essa permutação inicial, isto é, teremos a mesma permutação executando θ , a ou b vezes, desde que $a \equiv b \pmod{p}$. Nessas condições, pôde Betti escrever que

$$\theta^{mp+a} = \theta^a,$$

definindo que $\theta^p = 1$.

Betti supõe, a exemplo do conceito de permutação, que o conceito de substituição circular é conhecido. Entendemos por uma substituição circular de p letras, aplicada numa permutação de n letras, com $0 \leq p \leq n$, a operação que, ciclicamente, troca de lugar as p letras, deixando fixas as $(n-p)$ letras restantes.

Por exemplo, tome $n=5$, $p=3$, tal que θ esteja definida pela $\varphi_1(i)$, $0 \leq i \leq 3$, tal que $\varphi(0)=1$, $\varphi(1)=2$, $\varphi(2)=3$, $\varphi(3)=3$, $\varphi(4)=4$, no caso dela levar a permutação $abcde$ na permutação $cabde$, isto é, $\theta(abcde) = cabde$.

Nessas condições,

$$\theta^2(abcde) = \theta(abcde).\theta(abcde) = (bcade),$$

$$\theta^3(abcde) = \theta^2.\theta = (abcde) = \theta^0 = 1,$$

$$\theta^4(abcde) = \theta^3.\theta = 1.\theta = \theta(abcde) \quad \text{e}$$

$$\theta^5 = \theta^4.\theta = \theta.\theta = \theta^2,$$

$$\theta^6 = \theta^3 = 1, \quad \theta^7 = \theta, \quad \theta^8 = \theta^2, \quad \dots \text{ pois } a \equiv b \pmod{p} \text{ e assim } \theta^{mp+a} = \theta^a.$$

O conceito de operações sucessivas permitiu a Betti introduzir o conceito de substituição inversa. Para Betti, se $\theta^p = 1$, p a ordem de θ , então, $\theta^m.\theta^{p-m} = \theta^p = 1$, estabelecendo que $\theta^{p-m} = \theta^{-m}$, onde o expoente negativo indica a substituição inversa daquela representada quando se toma o expoente positivo.

Ainda segundo Betti, uma substituição que não for circular sobre um certo número de letras será equivalente a algumas substituições circulares sobre letras diferentes. Tal substituição foi denotada por $\theta = \varphi_0\varphi_1\varphi_2\dots\varphi_{m-1}$. E sendo indiferente a ordem em que efetuamos as substituições que agem sobre letras diferentes, quando repetirmos essa operação n vezes, teremos

$$\theta^n = \varphi_0^n.\varphi_1^n.\varphi_2^n\dots\varphi_{m-1}^n.$$

Como exemplo para tal conceito, tome $n=4$ o número de símbolos da permutação e as substituições θ, γ, ϕ definidas por:

$$\theta: \varphi(0)=1, \varphi(1)=0, \varphi(2)=3, \varphi(3)=2$$

$$\gamma: \varphi_0(0)=1, \varphi_0(1)=0, \varphi_0(2)=2, \varphi_0(3)=3$$

$$\phi: \varphi_1(0)=0, \varphi_1(1)=1, \varphi_1(2)=3, \varphi_1(3)=2$$

É fácil verificar que $\theta = \gamma\phi$ e que $\theta^2 = \gamma^2\phi^2$.

A fim de que $\theta^n = 1$, devemos ter $\varphi_0^n = 1, \varphi_1^n = 1, \varphi_2^n = 1, \dots, \varphi_{m-1}^n = 1$. Se cada uma das substituições $\varphi_i, 0 \leq i \leq (m-1)$ é circular sobre $p_0, p_1, p_2, \dots, p_{m-1}$ letras, respectivamente, não teremos $\theta^n = 1$ se n não for divisível por $p_0, p_1, p_2, \dots, p_{m-1}$.

Então Betti pôde definir a *ordem* de uma substituição. Ele escreveu:

“Chamaremos ordem de uma substituição o número que indica quantas permutações diferentes podemos obter, executando a substituição sucessivamente, a qual é a menor potência da substituição que dá por resultado a unidade.”

Por fim, Betti enunciou um teorema que reúne vários conceitos que estabeleceu nessa seção:

1. *As potências de uma substituição, das quais os expoentes são côngruos com respeito a ordem, são iguais entre si.*
2. *A ordem de uma substituição circular sobre p letras é igual a p .*
3. *A ordem de uma substituição qualquer é igual ao menor número que for divisível por todas as ordens das substituições circulares sobre letras diferentes, da qual é o produto.*
4. *Se o número p das letras é primo, cada substituição de $p^{\text{ésima}}$ ordem será circular em todas as letras.*
5. *Uma substituição de ordem prima p , ou é circular sobre p letras, ou é o produto de várias substituições circulares sobre p letras diferentes.*

Vamos agora para a **seção II**, que se inicia na página 55. Como dissemos, ela apresenta resultados relativos ao que ele chamou de *substituição derivada*.

Betti começa a discussão afirmando que quando várias substituições são tais que as letras trocadas por cada uma dessas operações deixam fixas as de outras, o resultado dessa composição – que Betti nessa seção chamou de produto – não varia se trocarmos a ordem dos fatores (observe o último exemplo).

Mas, se isso não ocorrer, tal produto não será indiferente à ordem dos fatores. Sem perda de generalidade, Betti toma apenas duas substituições θ e ψ para dizer que $\theta\psi = \psi\theta$ não ocorre sempre; e que em geral $\theta\psi = \psi\theta_1$, e θ_1 realiza uma operação diferente que θ .

Suponha, por exemplo, que θ é a substituição dada por $\varphi_1(0)=2$, $\varphi_1(1)=0$, $\varphi_1(2)=1$, $\varphi_1(3)=3$, $\varphi_1(4)=4$; e que ψ é dada por $\varphi_2(0)=0$, $\varphi_2(1)=1$, $\varphi_2(2)=2$, $\varphi_2(3)=4$, $\varphi_2(4)=3$. Aplicando o conceito de operação sucessiva para a permutação $ecbad$, temos

$$(ecbad)\theta\psi = (cbead)\psi = cbeda \quad \text{e} \quad (ecbad)\psi\theta = (ecbda)\theta = cbeda.$$

Por outro lado, tome θ , a substituição dada por $\varphi_1(0)=2$, $\varphi_1(1)=0$, $\varphi_1(2)=1$, $\varphi_1(3)=3$; e ψ , dada por $\varphi_2(0)=1$, $\varphi_2(1)=2$, $\varphi_2(2)=3$, $\varphi_2(3)=0$. E, aplicando o conceito de operação sucessiva para a permutação $badc$, vem

$$(badc)\theta\psi = (adbc)\psi = cadb \quad \text{e} \quad (badc)\psi\theta = (cbad)\theta = bacd.$$

Sendo que teremos $\theta\psi = \psi\theta_1$ somente se θ_1 for a substituição definida por $\varphi_3(0)=0$, $\varphi_3(1)=3$, $\varphi_3(2)=1$, $\varphi_3(3)=2$. Isto é, θ_1 realiza uma operação diferente de θ .

Naturalmente que, é possível termos $\theta_1 = \theta$.

Considere θ , a substituição dada por $\varphi_1(0)=1$, $\varphi_1(1)=0$, $\varphi_1(2)=3$, $\varphi_1(3)=2$; e ψ , dada por $\varphi_2(0)=2$, $\varphi_2(1)=3$, $\varphi_2(2)=0$, $\varphi_2(3)=1$.

Nessas condições, para qualquer permutação que considerarmos, temos $\theta\psi = \psi\theta$.

θ_1 , no contexto desse último conceito apresentado, é a substituição que Betti definiu como a *substituição derivada de θ por meio de ψ* , θ foi chamada de substituição *primitiva*, e ψ a *derivante*.

Betti denotou θ_1 por $D_\psi\theta$: $D_\psi\theta = \theta_1 = \psi^{-1}.\theta.\psi$

Observamos que, independente do que exemplificamos acima, as operações sucessivas denotadas por $\psi^{-1}.\theta.\psi$ determinam de maneira única θ_1 .

Ilustramos isso, retomando o exemplo onde θ é a substituição dada por $\varphi_1(0)=2, \varphi_1(1)=0, \varphi_1(2)=1, \varphi_1(3)=3$; e ψ , dada por $\varphi_2(0)=1, \varphi_2(1)=2, \varphi_2(2)=3, \varphi_2(3)=0$. Logo, ψ^{-1} está definida por $\varphi_2(0)=3, \varphi_2(1)=0, \varphi_2(2)=1, \varphi_2(3)=2$. Aplicando $\psi^{-1}.\theta.\psi$ na permutação $badc$, tal como fizemos acima, vem

$$(badc)\psi^{-1}\theta\psi = (adcb)\theta\psi = (dcab)\psi = bdca,$$

determinando que θ_1 deverá ser a operação definida por $\varphi_3(0)=0, \varphi_3(1)=3, \varphi_3(2)=1, \varphi_3(3)=2$.

Lembrando que a operação composta $\psi^{-1}.\theta.\psi$, hoje, em geral, é indicada por $\psi.\theta.\psi^{-1}$ e escrevemos, tal como Herstein [H1] para transformações lineares,

$$\psi.\theta.\psi^{-1}(badc) = \psi.\theta(adcb) = \psi(dcab) = (bdca).$$

Observamos que esse conceito de substituição derivada é o conceito que atualmente conhecemos por conjugação. θ e θ_1 são ditas permutações conjugadas, sendo tal conjugação determinada por ψ .

Betti também definiu a derivada m -ésima de θ por meio de ψ , indicada por $D_\psi^m\theta$: chamando a derivada de θ_1 de derivada segunda de θ , a derivada da derivada segunda de derivada terceira de θ , e assim por diante.

Em decorrência dessas definições são enunciados tanto convenções:

- (a) $\theta\psi = \psi.D_\psi\theta$
- (b) $D_\psi^0\theta = \theta$

quanto afirmações sem suas demonstrações:

- (c) $D_\psi^n \theta \cdot \psi = \psi \cdot D_\psi^{n+1} \theta$, (pois $\psi \cdot D_\psi^{n+1} \theta = \psi \cdot D_\psi (D_\psi^n \theta) = \psi \cdot \psi^{-1} \cdot D_\psi^n \theta \cdot \psi$)
- (d) $D_\psi^m \cdot D_\psi^n \theta = D_\psi^{m+n} \theta$
- (e) $D_\psi \theta \cdot D_\psi \varphi \cdot D_\psi \chi \dots = D_\psi (\theta \varphi \chi \dots)$
- (f) $\theta^n = 1$ se, e somente se, $(D_\psi \theta)^n = 1$.

Betti enuncia sua próxima afirmação, seguida de demonstração:

“A derivada por meio de uma substituição φ , da derivada por meio de uma outra ψ , de uma qualquer θ , é igual a derivada de θ por meio do produto $\psi\varphi$.”

Vamos mostrar que $D_\varphi (D_\psi \theta) = D_{\psi\varphi} \theta$.

Sabemos, por definição, que $\theta\psi = \psi \cdot D_\varphi \theta$ e $D_\psi \theta \cdot \varphi = \varphi \cdot D_\varphi (D_\psi \theta)$.

Como $D_\psi \theta \cdot \varphi = \varphi \cdot D_\varphi (D_\psi \theta) \Leftrightarrow \underbrace{\psi \cdot D_\psi \theta \cdot \varphi}_{\theta\psi \cdot \varphi} = \psi \cdot \varphi D_\varphi (D_\psi \theta)$

Mas, por definição, $\theta \cdot \psi\varphi = \psi\varphi \cdot D_{\psi\varphi} \theta$

Logo, $\psi\varphi \cdot D_{\psi\varphi} \theta = \psi\varphi \cdot D_{\psi\varphi} \theta$

Portanto, $D_{\psi\varphi} \theta = D_\varphi D_\psi \theta$.

E, em geral, $D_\varphi D_\psi D_\chi \dots D_\gamma \theta = D_{\gamma \dots \chi \psi \varphi} \theta$.

Como consequência, se $\varphi = \psi = \chi = \dots = \gamma$, então $\theta \cdot \psi^p = \psi^p \cdot D_\psi^p \theta$

e portanto, $D_{\psi^p} \theta = D_\psi^p \theta$.

Isto é, “a derivada por meio da $p^{ésima}$ potência de uma substituição é igual a derivada $p^{ésima}$ por meio da mesma substituição.”

E ainda, se

$$D_\psi^p \theta = D_\psi^p \varphi \quad \text{e} \quad D_{\psi^p} \theta = D_{\psi^p} \varphi$$

então

$$\theta \cdot \psi^p = \varphi \cdot \psi^p \quad \text{e} \quad \theta = \varphi.$$

Portanto, “derivadas de índices iguais têm iguais as suas primitivas.

Betti finaliza essa seção com o seguinte resultado, seguido de sua demonstração:

“o índice mínimo de uma derivada igual à sua primitiva é um divisor da ordem da derivante; e são iguais as derivadas que têm índices côngruos com respeito ao mesmo.”

Seja n o número mínimo para que se tenha $D_{\psi}^n \theta = \theta$ e $p = mn + r$, sendo p a ordem de ψ .

Ao derivarmos $D_{\psi^p} \theta = D_{\psi}^p \theta$, $(m-1)n$ vezes, temos $D_{\psi}^{m^n} \theta = D_{\psi}^{(m-1)n} \theta = \theta$.

Mas, $D_{\psi}^p \theta = \theta$, o que implica $D_{\psi}^{mn+r} \theta = D_{\psi}^{mn} \theta \cdot D_{\psi}^r \theta = \theta$.

Igualando essa última equação com a anterior, vem

$$D_{\psi}^{mn} \theta \cdot D_{\psi}^r \theta = D_{\psi}^{m^n} \theta,$$

tal que, $D_{\psi}^r \theta = \theta$.

Como $r < n$, devemos ter $r = 0$.

3.2.2 Capítulo Segundo.

O Capítulo Segundo, página 59, é composto por três seções.

Betti inicia a **Seção I** caracterizando *Grupo de permutações* e *Grau de um Grupo*.

Um *Grupo de permutações* será composto por uma série de permutações tais que uma substituição, executada em cada uma das permutações, realiza a troca entre elas sem produzir qualquer outra que não pertença à série.

Um grupo que contenha n permutações será de *grau* n .

Vamos ilustrar essa definição, o que Betti não o faz, construindo grupos de permutações. Supondo três símbolos a, b e c , temos abaixo suas seis permutações possíveis:

abc	acb
bca	bca
cab	bac

Esse conjunto de permutações define um grupo de permutações de grau 6. Observe que aplicando cada uma das substituições

$$\begin{aligned}\psi_0 : \varphi_0(0) &= 0, \varphi_0(1) = 1, \varphi_0(2) = 2, \\ \psi_1 : \varphi_1(0) &= 1, \varphi_1(1) = 2, \varphi_1(2) = 0, \\ \psi_2 : \varphi_2(0) &= 2, \varphi_2(1) = 0, \varphi_2(2) = 1, \\ \psi_3 : \varphi_3(0) &= 0, \varphi_3(1) = 2, \varphi_3(2) = 1, \\ \psi_4 : \varphi_4(0) &= 2, \varphi_4(1) = 1, \varphi_4(2) = 0, \\ \psi_5 : \varphi_5(0) &= 1, \varphi_5(1) = 0, \varphi_5(2) = 2,\end{aligned}$$

para cada uma das permutações acima, obteremos uma permutação desse próprio conjunto.

Podemos também, com a mesma quantidade de símbolos, estabelecer dois grupos de permutações de grau 3:

$$\begin{array}{ccc} abc & & acb \\ bca & \text{e} & bca \\ cab & & bac \end{array}$$

Esses grupos são definidos pelas mesmas três substituições, a saber,

$$\psi_0 : \varphi_0(0)=0, \varphi_0(1)=1, \varphi_0(2)=2,$$

$$\psi_1 : \varphi_1(0)=1, \varphi_1(1)=2, \varphi_1(2)=0,$$

$$\psi_2 : \varphi_2(0)=2, \varphi_2(1)=0, \varphi_2(2)=1.$$

Por outro lado, o conjunto de permutações

$$\begin{array}{c} abc \\ cba \\ cab \end{array}$$

não forma um grupo. Basta observar que a substituição $\psi : \varphi(0)=0, \varphi(1)=2, \varphi(2)=1$, é uma substituição desse conjunto de permutações, pois leva a permutação cba na permutação cab . Entretanto, $\psi(abc)=acb$ não pertence ao conjunto acima, ou seja, nem toda substituição desse conjunto leva qualquer permutação dele em uma outra permutação dele mesmo.

Para formar grupos de permutação de quatro símbolos, temos mais possibilidades. Vamos explicitar alguns grupos, a partir de todas as 24 possibilidades de permutações:

$$\begin{array}{cccccc} abcd & acdb & adbc & abdc & acbd & adcb \\ badc & cabd & dacb & bacd & cadb & dabc \\ cdab & dbac & bcad & dcab & bdac & cbad \\ dcba & bdca & cbda & cdba & dbca & bcda \end{array}$$

Observemos que as substituições que levam cada permutação de uma dessas colunas em outra permutação da mesma coluna é uma das quatro substituições abaixo:

$$\psi_0 : \varphi_0(0)=0, \varphi_0(1)=1, \varphi_0(2)=2, \varphi_0(3)=3,$$

$$\psi_1 : \varphi_1(0)=1, \varphi_1(1)=0, \varphi_1(2)=3, \varphi_1(3)=2,$$

$$\psi_2 : \varphi_2(0)=2, \varphi_2(1)=3, \varphi_2(2)=0, \varphi_2(3)=1,$$

$$\psi_3 : \varphi_3(0)=3, \varphi_3(1)=2, \varphi_3(2)=1, \varphi_3(3)=0,$$

Além do mais, cada uma dessas quatro substituições leva qualquer permutação de cada uma das colunas acima em uma outra da mesma coluna. Desse modo, segundo a definição de Betti, cada uma dessas colunas é um grupo de permutação. Temos assim, seis grupos de permutações distintos, de quatro permutações cada um, mas que possuem as mesmas substituições.

É interessante, desde já, observar que, para qualquer $i, 0 \leq i < 4$, temos $\psi_i^2 = 1$ e $\psi_i^{-1} = \psi_i$. E ainda, que $\psi_2 \cdot \psi_3 = \psi_1$. Ou também que, $\psi_2 \cdot \psi_1 = \psi_3$, qualquer que seja a permutação envolvida na operação realizada.

Podemos também definir os oito grupos de permutação de grau três, cada um dado por uma das colunas abaixo:

$$\begin{array}{cccccccc} abcd & abdc & badc & bacd & cdab & cdba & dcab & dcba \\ acdb, & acbd, & bdca, & bcda, & cabd, & cbad, & dabc & \text{ou } dbac. \\ adbc & adcb & bcad & bdac & cbda & cadb & dbca & dacb \end{array}$$

Cada um deles possui as mesmas substituições, que são as seguintes:

$$\psi_0 : \varphi_0(0)=0, \varphi_0(1)=1, \varphi_0(2)=2, \varphi_0(3)=3,$$

$$\psi_1 : \varphi_1(0)=1, \varphi_1(1)=2, \varphi_1(2)=3, \varphi_1(3)=1,$$

$$\psi_2 : \varphi_2(0)=0, \varphi_2(1)=3, \varphi_2(2)=1, \varphi_2(3)=2.$$

Tal como no exemplo anterior, observemos que, para qualquer $i, 0 \leq i < 3$, temos $\psi_i^3 = 1$, ou seja, cada uma das substituições tem grau três.

Para os grupos acima, temos $\psi_1, \psi_1^2 = \psi_2, \psi_i^3 = \psi_0$.

Observamos ainda, que $\psi_2^{-1} = \psi_2^2 = \psi_1$. Ou que, $\psi_2 \cdot \psi_1 = \psi_0$. Esse fato ocorre em geral, isto é, se $\psi_0, \psi_1, \psi_2, \dots, \psi_{p-1}$ são as substituições que definem um grupo de permutações, deveremos ter $\psi_m \cdot \psi_n = \psi_r$, sendo então r um valor inteiro que depende de m e n , e é menor do que p .

Por fim, queremos observar que um grupo de permutações no sentido moderno é formado pelo conjunto das substituições de um grupo de permutações, no sentido de Betti.

A próxima proposição enunciada por Betti pode ser interpretada como uma versão da afirmação que hoje é conhecida por Teorema de Lagrange: *a ordem do subgrupo divide a ordem do grupo* (ordem, número de elementos de um grupo finito):

A ordem de uma substituição qualquer de um grupo é um divisor do número de permutações do grupo. Consequentemente, se um grupo tem um número primo de permutações, suas substituições serão todas potências de uma só de ordem p .

Betti demonstrou essa afirmação como segue,

Seja q a ordem de uma substituição ψ_0 de um grupo;

ou q será igual ao número das permutações desse grupo, e assim por ψ_0 teremos todas as permutações,

ou q será menor do que o número das permutações desse grupo, e por ψ_0 não teremos todas as q permutações, existindo, portanto, outra substituição.

Seja ψ_1 esta outra substituição, de ordem n ; pelas duas substituições teremos qn permutações diferentes; porque supondo duas iguais temos

$$\psi_0^r \cdot \psi_1^s = \psi_0^{r'} \cdot \psi_1^{s'} \Leftrightarrow \psi_1^{s-s'} = \psi_0^{r-r'}$$

Tomando $(s - s')k \equiv 1 \pmod{n}$, e elevando a potência k , teremos $\psi_1 = \psi_0^{(r-r')k}$

e então a substituição ψ_1 não será outra que uma potência de ψ_0 , e não uma nova que possa produzir outra permutação.

Se qn não é igual ao número das permutações do grupo, existirá também uma outra permutação ψ_2 , com a qual obteremos outras q permutações, todas diferentes da precedente, pois supondo

$$\psi_0^r \cdot \psi_1^s = \psi_0^n \cdot \psi_2$$

Teremos

$$\psi_2 = \psi_0^{r-n'} \cdot \psi_1^s$$

ou melhor ψ_2 igual a uma das substituições precedentes, contrário ao suposto.

Se com estas $q(n+1)$ permutações não são exauridas todas aquelas do grupo, a outra substituição não poderá igualmente dar mais que um número múltiplo de q .

c.q.d.

Vamos destacar esse resultado, retomando exemplos. Considere o grupo de permutações de três símbolos

$$\begin{array}{ll} abc & acb \\ bca & bac \\ cab & bac \end{array}$$

cujas substituições são

$$\begin{aligned} \psi_0 : \varphi_0(0)=0, \varphi_0(1)=1, \varphi_0(2)=2, & \quad \psi_1 : \varphi_1(0)=1, \varphi_1(1)=2, \varphi_1(2)=0, \\ \psi_2 : \varphi_2(0)=2, \varphi_2(1)=0, \varphi_2(2)=1, & \quad \psi_3 : \varphi_3(0)=1, \varphi_3(1)=0, \varphi_3(2)=2 \\ \psi_4 : \varphi_4(0)=0, \varphi_4(1)=2, \varphi_4(2)=1, & \quad \psi_5 : \varphi_5(0)=2, \varphi_5(1)=1, \varphi_5(2)=0. \end{aligned}$$

É fácil verificar que $\psi_1^3 = 1$, $\psi_3^2 = 1$; e que $\psi_5 = \psi_1^2 \cdot \psi_3$. Sendo a ordem de ψ_1 é igual 3, e o grau do grupo igual a 6, segue a afirmação acima. A mesma observação vale para ψ_3 .

Vejamos um caso para grupo com 4 símbolos.

Tome

<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>

o grupo de permutações.

As substituições

$$\psi_1 : \varphi_1(0)=1, \varphi_1(1)=0, \varphi_1(2)=3, \varphi_1(3)=2,$$

$$\psi_2 : \varphi_2(0)=0, \varphi_2(1)=2, \varphi_2(2)=3, \varphi_2(3)=1$$

$$\psi_3 : \varphi_3(0)=3, \varphi_3(1)=2, \varphi_3(2)=1, \varphi_3(3)=0,$$

$$\psi_4 : \varphi_4(0)=3, \varphi_4(1)=0, \varphi_4(2)=2, \varphi_4(3)=1,$$

definem algumas dessas permutações.

$$\text{Temos } \psi_1^2 = 1, \psi_2^3 = 1, \psi_3 = \psi_2^2 \cdot \psi_1, \psi_4 = \psi_1 \cdot \psi_2^2.$$

Finalmente, observe que o grupo

abcde
bcdea
cdeab
deabc
eabcd

tem por substituições $\psi_1, \psi_2 = \psi_1^2, \psi_3 = \psi_1^3, \psi_4 = \psi_1^4, \psi_0 = \psi_1^5 = 1$. O que exemplifica a segunda parte da proposição.

Ao final dessa seção I, Betti define grupos *iguais* como aqueles que possuem as mesmas substituições, mesmo que com permutações diferentes. Se as substituições forem diferentes, mas de mesmo número e igual ordem, e o mesmo número de permutações, os grupos serão chamadas *semelhantes*. Esses conceitos são abordados nas próximas duas seções.

As **seções II** (final da página 60) e **III** (início da página 62), são dedicadas, respectivamente, aos *grupos derivados semelhantes* e aos *grupos derivados iguais*, estabelecendo também os conceitos de *multiplicador e divisor de um grupo*.

Betti inicia sua abordagem para esses assuntos definindo *grupos derivados*. Tome dois grupos G, Γ ; o primeiro com p substituições θ_i , e o segundo com n substituições ψ_j . Ao executarmos cada substituição $\psi_m, m < n$, em todas as permutações de G , obtemos um grupo que tem todas as suas substituições derivadas daquelas de G por meio de ψ_m . Esse grupo será chamado de *Grupo derivado de G por meio de ψ_m* , sendo indicado pela notação $D_{\psi_m} G$.

Podemos demonstrar esse fato da seguinte maneira: tomemos as permutações x_i do grupo G . Sabemos, por definição, que para cada i , temos $\theta_k(x_i) = x_j$, para algum j , com $1 \leq j \leq m, 1 \leq i \leq n$. Sabemos, também por definição que, tomando uma substituição ψ_m de Γ , temos que $\psi_m(x_i) = y_t, 1 \leq t \leq m$, sendo y_t uma permutação que não está, necessariamente, contida em G . Nessas condições, $x_i = (y_t) \psi_m^{-1}$. Aplicando sucessivamente, nessa equação, θ_k e ψ_m , pela direita, temos

$$(x_i) \theta_k = (y_t) \psi_m^{-1} \theta_k$$

$$x_j = (y_t) \psi_m^{-1} \theta_k$$

$$(x_j) \psi_m = (y_t) \psi_m^{-1} \theta_k \psi_m$$

$$y_u = (y_t) \psi_m^{-1} \theta_k \psi_m$$

As permutações y_u formam um grupo, que Betti chamou *Grupo derivado de G por meio de ψ_m* , e indicou pela notação $D_{\psi_m} G$.

Isto é, *uma substituição φ que converte uma permutação de um grupo G em uma de seu derivado, troca inteiramente o primeiro pelo segundo*.

$$\text{Tomemos os grupos de permutações } G: \begin{bmatrix} abcde \\ eabcd \\ deabc \\ cdeab \\ bcdea \end{bmatrix} \text{ e } \Gamma: \begin{bmatrix} abcde \\ acedb \\ aebdc \end{bmatrix}.$$

O primeiro com substituições:

$$\theta_0: \varphi_0(0)=0, \varphi_0(1)=1, \varphi_0(2)=2, \varphi_0(3)=3, \varphi_0(4)=4,$$

$$\theta_1: \varphi_1(0)=1, \varphi_1(1)=2, \varphi_1(2)=3, \varphi_1(3)=4, \varphi_1(4)=0,$$

$$\theta_2: \varphi_2(0)=2, \varphi_2(1)=3, \varphi_2(2)=4, \varphi_2(3)=0, \varphi_2(4)=1,$$

$$\theta_3: \varphi_3(0)=3, \varphi_3(1)=4, \varphi_3(2)=0, \varphi_3(3)=1, \varphi_3(4)=2,$$

$$\theta_4: \varphi_4(0)=4, \varphi_4(1)=0, \varphi_4(2)=1, \varphi_4(3)=2, \varphi_4(4)=3;$$

e o segundo com substituições

$$\psi_0: \varphi_0(0)=0, \varphi_0(1)=1, \varphi_0(2)=2, \varphi_0(3)=3, \varphi_0(4)=4,$$

$$\psi_1: \varphi_1(0)=0, \varphi_1(1)=2, \varphi_1(2)=4, \varphi_1(3)=3, \varphi_1(4)=1$$

$$\psi_2: \varphi_2(0)=0, \varphi_2(1)=4, \varphi_2(2)=1, \varphi_2(3)=0, \varphi_2(4)=2$$

Segundo a definição de Betti, para obtermos um grupo derivado, devemos aplicar uma substituição de Γ em cada permutação de G .

Tomemos ψ_1 . Temos que

$$\psi_1(abcde) = aebdc \quad \psi_1(eabcd) = edacb$$

$$\psi_1(deabc) = dceba \quad \psi_1(cdeab) = cbdae$$

$$\psi_1(bcdea) = baced$$

Esse é o grupo derivado de G por meio de ψ_1 , ou $D_{\psi_1}G$. E, pela definição de grupo derivado, as substituições de $D_{\psi_1}G$ serão as $\psi_1^{-1}\theta_i\psi_1$, $0 \leq i \leq 4$.

Observemos que, neste exemplo, as substituições de G e $D_{\psi_1}G$ são diferentes, mas em igual número; e também possuem a mesma ordem e o mesmo número de

permutações. Por esse motivo, eles foram chamados, por Betti, *grupos derivados semelhantes*.

Por outro lado, ao considerarmos os grupos:

$$G_1 : \begin{bmatrix} abcd \\ badc \\ cdab \\ dcba \end{bmatrix} \quad \text{e} \quad \Gamma : \begin{bmatrix} abcd \\ acdb \\ adbc \end{bmatrix} ,$$

e tomando, como exemplo, a substituição

$$\psi_1 : \varphi_1(0)=0, \varphi_1(1)=3, \varphi_1(2)=1, \varphi_1(3)=2$$

de Γ , o grupo derivado $D_{\psi_1}G$ será:

$$\begin{aligned} \psi_1(abcd) &= acdb & \psi_1(badc) &= bdca \\ \psi_1(cdab) &= cabd & \psi_1(dcba) &= dbac \end{aligned}$$

Este é o grupo derivado de G por meio de ψ_1 . Suas substituições são $\psi_1^{-1}\theta_i\psi_1$, $0 \leq i \leq 3$.

Como G e $D_{\psi_1}G$ possuem o mesmo número de permutações e as mesmas substituições (observemos que $\psi_1^{-1}\theta_i\psi_1 = \theta_i$, $0 \leq i \leq 3$) eles foram chamado por Betti de *derivados iguais*.

Vamos repetir as contas acima para

$$\psi_2 : \varphi_2(0)=0, \varphi_2(1)=2, \varphi_2(2)=3, \varphi_2(3)=1.$$

Isto é, vamos definir $D_{\psi_2}G$.

$$\begin{aligned} \psi_2(abcd) &= adbc & \psi_2(badc) &= bcad \\ \psi_2(cdab) &= cbda & \psi_2(dcba) &= dacb \end{aligned}$$

$D_{\psi_2}G$ também é derivado igual a G .

A união de grupos derivados iguais, dado pela soma das permutações de $G_1, D_{\psi_1}G, D_{\psi_2}G$ forma um grupo, o qual Betti chamou de H , que conterà as p substituições θ_i e as n substituições ψ_j .

No nosso exemplo, H é o grupo

$abcd$	$acdb$	$adbc$
$badc$	$cabd$	$dacb$
$cdab$	$dbac$	$bcad$
$dcba$	$bdca$	$cbda$

Nesse ponto da obra, Betti está definindo o que hoje conhecemos por subgrupos normais. Os grupos $G_1, D_{\psi_1}G, D_{\psi_2}G$, se observados como grupos no sentido moderno, isto é, compostos pelas substituições θ_i , são subgrupos normais do grupo H , já que, por definição, para qualquer substituição ψ_j do grupo H e qualquer substituição θ_i de um de grupos, a substituição $\psi_j^{-1}\theta_i\psi_j$ está nesse mesmo grupo. Tal conceito foi introduzido por Galois, e por ele chamado grupo parcial, tal como descrevemos no capítulo anterior, item 2.4.

E, se os grupos derivados por meio de um grupo derivante Γ , forem iguais, isto é, se

$$G = D_{\psi_0}G = D_{\psi_1}G = \dots = D_{\psi_{n-1}}G,$$

Γ será chamado de o *multiplicador* do grupo G , como também de o *divisor* do grupo H .

O grupo H será chamado o *produto* de G por Γ , o qual Betti indicou por $H = G\Gamma$.

Hoje dizemos que um grupo como subgrupo de um outro é um subgrupo normal do segundo. Betti segue um caminho inverso. Começa com um grupo G e a partir de um grupo Γ constrói um grupo H do qual G é um subgrupo normal. Não só isso, no caso de os grupos derivados serem iguais cada um dos derivados de G também é subgrupo normal de H . Além do mais, se tomarmos o exemplo anterior a

união de G_1 com $D_{\psi_1} G$ também é um subgrupo normal de H e G_1 é um subgrupo normal do grupo obtido pela união de G_1 com $D_{\psi_1} G$.

E ainda, se

$$\Gamma = G_1 \Gamma_1, \Gamma_1 = G_2 \Gamma_2, \dots, \Gamma_{n-2} = G_{n-2} \Gamma_{n-1}, \text{ com } H = G G_1 G_2 \dots G_{n-1},$$

onde G_{n-1} é o primeiro divisor (e o $(n-1)^{\text{ésimo}}$ multiplicador), G_{n-2} é o segundo divisor (e o $(n-2)^{\text{ésimo}}$ multiplicador, e assim sucessivamente nessa ordem, do grupo H .

Se não existir nenhum outro multiplicador depois de Γ , ele será o *máximo multiplicador de G* . De *primo* será chamado o grupo que não admite qualquer divisor. E aquele que não tem nenhum multiplicador, de *grupo máximo*.

Por fim, ele mostra que o derivado do produto dos grupos é igual ao produto dos derivados, com todos de mesma ordem.

Por essa definição, se retornarmos ao último exemplo, vemos que G_1, G_2, G_3 não deverão ser máximos, uma vez que não são primos. De fato, é possível dividir cada um deles em dois grupos derivados iguais:

$$\begin{array}{ccc} \overbrace{\begin{array}{cc} abcd & cdab \\ badc & dcba \end{array}}^{G_1} & \overbrace{\begin{array}{cc} acdb & dbac \\ cabd & bdca \end{array}}^{G_2} & \overbrace{\begin{array}{cc} adbc & bcad \\ dacb & cbda \end{array}}^{G_3} \end{array} ,$$

repetindo as contas acima apresentadas.

Observemos que na impossibilidade de decompor um grupo em uma sequência decrescente de subgrupos normais, já que Betti começa com um grupo menor, ele faz o inverso. Começa com um grupo e constrói uma sequência crescente de grupos maiores, em que o anterior é subgrupo normal do seguinte.

3.2.3 Capítulo Terceiro.

O terceiro capítulo (ao final da página 63) possui cinco seções. Todas elas estão dedicadas à determinação dos multiplicadores e divisores de um grupo, como dissemos.

A seção I, como relataremos, resume as ações de Betti por todo Terceiro Capítulo. A seção II define um grupo primitivo e seu respectivo multiplicador que irão fundamentar as construções que Betti propõe nas seções seguintes. As seções III e IV, preocupam-se em construir os atualmente chamados grupos quociente. Essas duas últimas seções são de difícil leitura e interpretação e, nossa análise se restringirá a elaboração de conjecturas sobre o que Betti fez. Enfim, a seção V trata da determinação dos divisores de grupos quociente; acreditamos que tais divisores estarão bem explicitados na nossa análise até a seção IV.

Em particular, as seções IV e V exibem as demonstrações que Betti elaborou para fundamentar as construções dos grupos quociente que propôs. Acreditamos que essa parte do texto não contemple o foco de nossa análise. Para um bom estudo sobre essas demonstrações sugerimos os textos de Betti, [B4], e Mammone, [M1].

Vamos à nossa análise para esse capítulo.

Na primeira seção Betti resume o que expôs no capítulo anterior, propondo dois problemas; o da determinação do grupo multiplicador e o da determinação do divisor de um dado grupo, por meio de suas equações.

Como ponto de partida para as soluções, determina as substituições θ_i que definem o grupo primitivo dado e, então:

1. Tomando n substituições ψ de um grupo multiplicador Γ , e p substituições θ_i do grupo primitivo G devemos, para cada ψ , encontrar as p permutações de cada grupo $D_\psi \theta_i$, satisfazendo a equação $\psi \theta_i = \theta_j \psi$, gerando o grupo $H = G\Gamma$.
2. Para a decomposição do grupo em sucessivos divisores primos, deveremos considerar as substituições θ_i de um grupo G e as ψ_j de um

outro grupo Γ_n , de forma que $H = G\Gamma_n$ seja o produto deles. Para tanto, as substituições de G devem satisfazer as equações $\theta_r\theta_s = \theta_t$ e $D_{\psi_j}\theta_i = \theta_k$. Nessas condições, o grupo G será o divisor do grupo H .

Ao final dessa seção, Betti distingue três casos para a determinação do multiplicador:

- (1°) aquele no qual o número de letras é primo;
- (2°) quando o número de letras é o produto de números primos diferentes entre si;
- (3°) quando o número de letras é uma potência de um número primo.

Esses três casos, um por vez e na ordem acima, foram tratados nas seções 2, 3 e 4.

Na **seção II** (página 66), cujo título é: *Máximo multiplicador de um grupo de um número primo de permutações sobre um número igual de letras*, Betti diz que o grupo primitivo G , é circular sobre todas as letras e, suas substituições $\theta(i)$, $0 \leq i \leq 4$, de ordem p , devem ser dadas pelas potências de uma dessas θ , tal que $\phi(i) = i + 1$.

Tomando $p = 5$ como exemplo e sendo $abcde$ a primeira permutação do grupo, temos

G
 $abcde$
 $bcdea$
 $cdeab$
 $deabc$
 $eabcd$

Começando com a primeira permutação, observemos que, de fato, temos:

$$(abcde)\theta^0 = abcde; \quad (abcde)\theta^1 = eabcd;$$

$$(abcde)\theta^2 = ((abcde)\theta).\theta = (eabcd)\theta = deabc;$$

$$(abcde)\theta^3 = (abcde)\theta^2.\theta = (deabc)\theta = cdeab;$$

$$(abcde)\theta^4 = (abcde)\theta^3.\theta = (cdeab)\theta = bcdea;$$

$$\theta^5 = \theta^0 = 1; \quad \theta^6 = \theta^1; \quad \theta^7 = \theta^2; \quad \dots$$

Betti definiu as substituições do multiplicador Γ pelos índices da φ , uma vez que elas devem satisfazer a equação simbólica $\psi\theta_i = \theta\psi$. Isto é, sendo θ e θ_i circulares e, portanto, uma potência da outra, segue pela equação acima que as ψ serão circulares. Pela definição de substituição de Betti, uma substituição circular estará definida, em geral, pela função $\psi(i) = ai + b$. Assumindo $\psi(i) = ai + b = a(i + c) = a[\varphi(i)]^c$, ele determinou uma relação entre φ e ψ , desde que $ac \equiv b \pmod{p}$.

Assim, as substituições ψ do multiplicador Γ serão dadas por $\psi(i) = ai$, ou melhor, por $\varphi(i) = \lambda i$.

De volta ao nosso exemplo temos $0 \leq \lambda \leq 4$ e:

$$\varphi_0(i) \equiv i \pmod{5}, \text{ ou } \varphi_0(0) = 0, \varphi_0(1) = 1, \varphi_0(2) = 2, \varphi_0(3) = 3, \varphi_0(4) = 4.$$

$$\varphi_0(i) \equiv 2i \pmod{5}, \text{ ou } \varphi_0(0) = 0, \varphi_0(1) = 2, \varphi_0(2) = 4, \varphi_0(3) = 1, \varphi_0(4) = 3.$$

$$\varphi_0(i) \equiv 3i \pmod{5}, \text{ ou } \varphi_0(0) = 0, \varphi_0(1) = 3, \varphi_0(2) = 1, \varphi_0(3) = 4, \varphi_0(4) = 2.$$

$$\varphi_0(i) \equiv 4i \pmod{5}, \text{ ou } \varphi_0(0) = 0, \varphi_0(1) = 4, \varphi_0(2) = 3, \varphi_0(3) = 2, \varphi_0(4) = 1.$$

O que nos leva, partindo da permutação $abcde$, ao grupo:

Γ
 $abcde$
 $acebd$
 $aedcb$
 $adbec$

E, enfim, aplicando cada uma das substituições ψ nas permutações de G , obtemos

$H = G\Gamma$, abaixo:

$abcde$	$acebd$	$aedcb$	$adbec$
$bcdea$	$cebda$	$edcba$	$dbeca$
$cdeab$	$ebdac$	$dcbae$	$becad$,
$deabc$	$bdace$	$cbaed$	$ecadb$
$eabcd$	$daceb$	$baedc$	$cadbe$

Por tudo isso, Betti conclui que a substituição do máximo multiplicador de um grupo de um número primo de permutações sobre um número primo de letras, e que tem por substituição somente as potências de $\begin{pmatrix} i \\ i+1 \end{pmatrix}$, são todas potências de $\begin{pmatrix} i \\ \lambda i \end{pmatrix}$;

e então o grupo cujas substituições são todas compreendidas na notação $\begin{pmatrix} i \\ ai+b \end{pmatrix}$ é um máximo.

Passemos à **seção III** (página 67): *Máximo multiplicador de um grupo de um número primo de permutações sobre um número de letras que tem os fatores primos diferentes entre si.*

Em primeiro lugar Betti toma o grupo G composto por um número primo p de permutações. O número de letras dessas permutações será m , produto de números primos diferentes entre si. As substituições de G serão as potências de uma só, de ordem p , resultantes do produto de q substituições circulares; e cada uma

dessas q substituições circulares estarão definidas por meio de um *sistema* de p letras diferentes.

Vamos tomar o exemplo de $m=6$ e $p=3$. Nessa condição, teremos dois sistemas ($q=2$) de três letras diferentes ($p=3$). Acreditamos, para uma melhor compreensão do que foi dito no parágrafo acima, construir o grupo primitivo G , primeiro com a notação sugerida por Betti para as permutações.

Tomemos $x_1x_2x_3y_1y_2y_3$ a permutação inicial. O grupo G será:

$$\begin{array}{c} G \\ x_1x_2x_3y_1y_2y_3 \\ x_3x_1x_2y_3y_1y_2 \\ x_2x_3x_1y_2y_3y_1 \end{array}.$$

Podemos observar que G é um grupo com $p=3$ permutações e $q=2$ sistemas circulares de ordem 3. As substituições desses dois sistemas estão dadas, pelas potências de

$$\theta_0 : \varphi_0(0)=1 ; \varphi_0(1)=2 ; \varphi_0(2)=0 , \text{ para as permutações das letras } x_1, x_2, x_3,$$

e

$$\theta_1 : \varphi_1(0)=1 ; \varphi_1(1)=2 ; \varphi_1(2)=0, \text{ para as permutações das letras } y_1, y_2, y_3.$$

As substituições de G serão as potências de uma só, de ordem p , resultantes do produto de q substituições circulares, dadas pela justaposição de θ_0 e θ_1 .

Retornando à notação que adotamos, fica fácil reescrever o grupo primitivo G , considerando $abcdef$ a permutação inicial,

$$\begin{array}{c}
G \\
abcdef \\
cabfde \\
bcaefd
\end{array}$$

composto por três permutações e com os dois sistemas circulares de ordem 3.

Betti usa a notação $\begin{pmatrix} x_{k,h} \\ x_{k+a,h} \end{pmatrix}$ para denotar as substituições de G , onde o índice k indica a posição das letras nos q sistemas e o índice h indica a posição dos sistemas com relação ao grupo G .

Um primeiro grupo multiplicador Γ , do grupo G , será definido levando-se em conta esses sistemas circulares. Como os sistemas são constituídos por um número primo p letras diferentes, Betti fez tal como na seção anterior: as substituições ψ_i , desses sistemas, são dadas por $\varphi(k) = \lambda k$, de tal maneira que as substituições de Γ também deverão ser um produto de circulares: $\psi = \psi_0 \psi_1 \dots \psi_q$.

Em nosso exemplo, em cada sistema teremos

$\psi_0 : \varphi_0(k) = k \pmod{3}, \varphi_0(0) = 0; \varphi_1(1) = 1; \varphi_2(2) = 2$ para as permutações das letras a, b, c ;

e,

$\psi_1 : \varphi_1(k) = 2k \pmod{3}, \varphi_1(0) = 0; \varphi_1(1) = 2; \varphi_1(2) = 1$ para as permutações das letras d, e, f .

Betti utiliza $\begin{pmatrix} x_{k,h} \\ x_{\lambda k,h} \end{pmatrix}$ para denotar todas as substituições de Γ .

Considerando $abcdef$ a permutação inicial, o grupo Γ será

$$\Gamma$$

$$abcdef .$$

$$acbdfe$$

Quando aplicamos cada substituição de Γ nas permutações de G , obtemos o produto $G\Gamma$:

$$G\Gamma$$

$$abcdef \quad acbdfe$$

$$cab fde \quad cba fed .$$

$$bcaefd \quad bac edf$$

Logo após, Betti indica que um próximo passo é a obtenção do multiplicador H , do grupo $G\Gamma$, que será aquele com substituições definidas pelo índice h . Betti as denotou por

$$\begin{pmatrix} x_{k,h} \\ x_{k,\gamma(h)} \end{pmatrix}.$$

Essa notação indica que as substituições de H deixam fixas as letras em cada sistema, mas muda a posição desses sistemas no grupo $G\Gamma$. Em nosso exemplo, devemos ter $\gamma(h)=h+1$. Dada a permutação inicial $abcdef$, tal grupo poderá ser representado pelas permutações

$$H$$

$$abcdef .$$

$$def abc$$

Aplicando cada substituição de H nas permutações de $G\Gamma$, obtemos o grupo $L = KH = G\Gamma H$, cujas permutações serão

L

$abcdef$	$acbdfe$
$cabfde$	$cbafed$
$bcaefd$	$bacedf$

$defabc$	$dfeacb$
$fdecab$	$fedcba$.
$efdbca$	$edfbac$

O grupo L , produto dos grupos H e K , foi construído de tal forma que H somente tenha substituições definidas pelo índice h , e K , substituições definidas pelo índice k . Betti chamou esse grupo L de *grupo por letras adjuntadas*, sendo *letras adjuntadas* aquelas com um mesmo índice h .

Em nosso exemplo, temos dois tipos de sistemas de letras adjuntadas, formados pelo índice k : aquele que adjunta e permuta três letras, e aquele que adjunta três letras e permuta duas delas.

Em seguida, no terceiro parágrafo da página 68, Betti faz a seguinte afirmação, que é uma parte do teorema enunciado quando ele encerra esta seção: “*Se não existe algum multiplicador do grupo, que dá um produto por letras adjuntadas, L será um grupo máximo, ao menos que o número das letras que entram nas permutações não tenham iguais entre si os seus fatores primos.*” Betti não faz a demonstração completa dessa afirmação.

Na página 69, 3º parágrafo, para melhor esclarecer o conceito de letras adjuntadas, Betti demonstra que *as letras que forem adjuntadas não podem fazer parte de mais de um sistema* e então, *os sistemas diferentes de letras adjuntadas terão uma só letra igual*. Para essa afirmação Betti argumenta, e isso pode ser verificado nos sistemas do exemplo que fazemos acima, que toda substituição que troca a posição da letra a também troca a posição das letras b e c ; analogamente para as letras d , e , f .

Já nos sistemas definidos pelas substituições cujas potências estão compreendidas na notação $\begin{pmatrix} x_{k,h} \\ x_{\lambda k,h} \end{pmatrix}$, vemos que os seis sistemas diferentes que foram formados, permutam duas de suas letras, deixando fixada uma outra.

No fim da página 69 e no início da página 70, Betti ainda nos propõe o que chamou de *Quadro A*, dispondo as permutações do grupo construído de uma maneira específica: cada um dos p sistemas deverão ser dispostos em linhas evidenciando, ao mesmo tempo, os sistemas formados pelo índice k nas suas respectivas posições, definidas pelo índice h : “... as letras de cada sistema sendo p , os sistemas serão ao menos p e as letras p^2 . Sejam as seguintes linhas horizontais os primeiros p sistemas de letras adjuntadas, e aquela formada por uma letra de cada um desses, seja a primeira linha vertical

$$A \left\{ \begin{array}{ccccc} x_{0,0} & x_{1,0} & x_{2,0} & \dots & x_{p-1,0} \\ x_{0,1} & x_{1,1} & x_{2,1} & \dots & x_{p-1,1} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ x_{0,p-1} & x_{1,p-1} & x_{2,p-1} & \dots & x_{p-1,p-1} \end{array} \right. \text{ ”}$$

Cada $x_{i,j}$, $0 \leq i, j \leq (p-1)$, nas posições do quadro A , representam cada um dos sistemas do grupo construído.

Considerando as conjecturas que apresentamos até aqui, esse quadro não faz muito sentido, uma vez que, em nosso exemplo, o grupo L não teria p sistemas de letras adjuntadas. Nossa opção de representação do grupo L , acima construído, nos mostra $p-1$ sistemas dispostos em duas *linhas* e duas colunas:

L

$abc\ def$	$acb\ dfe$
$cab\ fde$	$cba\ fed$
$bca\ efd$	$bac\ edf$

$def\ abc$	$dfe\ acb$
$fde\ cab$	$fed\ cba$
$efd\ bca$	$edf\ bac$

Entretanto, após a apresentação do Quadro A, Betti descreve, ou melhor reescreve em linguagem retórica a construção do grupo L , detalhando a interdependência existente entre os sistemas gradualmente gerados pelas substituições compreendidas nas três notações apresentadas:

$$\begin{pmatrix} x_{k,h} \\ x_{k+a,h} \end{pmatrix}, \begin{pmatrix} x_{k,h} \\ x_{\lambda k,h} \end{pmatrix} \text{ e } \begin{pmatrix} x_{k,h} \\ x_{k,\gamma(h)} \end{pmatrix};$$

interdependência já demonstrada nas afirmações: “as letras que forem adjuntadas não podem fazer parte de mais de um sistema” e então, “os sistemas diferentes de letras adjuntadas terão uma só letra igual”.

Essa interdependência entre os vários sistemas de letras adjuntadas, assegura que as substituições do grupo L serão todas circulares. E como a construção de L se dá passo a passo, e prevendo a necessidade de vários sistemas de letras adjuntadas, Betti apresenta uma notação geral para indicar todas as substituições desse grupo:

$$\begin{pmatrix} x_{k,h,l,\dots} \\ x_{k+a,h+b,l+c,\dots} \end{pmatrix}.$$

Tal notação está inserida no teorema que Betti enuncia ao final dessa seção:

“Para que um grupo por letras adjuntadas admita um multiplicador, pelo qual multiplicado, o produto não seja por letra adjuntada, é necessário que o número das letras seja a potência de um número primo, e que esse não contenha outras substituições que compreendidas no símbolo

$$\begin{pmatrix} x_{k,h,l,\dots} \\ x_{k+a,h+b,l+c,\dots} \end{pmatrix}.$$

Um grupo de permutações de um número de letras que admite os fatores primos diferentes entre si, não pode ter por divisor nenhum grupo por letra adjuntada, ao menos que ele próprio não seja um grupo por letra adjuntada.”

Enfim, na **seção IV**, *Máximo multiplicador de um grupo de um número primo de permutações sobre um número de letras que é potência de um número primo*, Betti toma p^v letras que entram nas permutações, para gerar sistemas de letras adjuntadas, e conseqüentemente, o grupo primitivo G com p permutações. O divisor desse primitivo será aquele cujas substituições estarão compreendidas na notação:

$$\begin{pmatrix} x_{k,h,l,\dots} \\ x_{k+a,h+b,l+c,\dots} \end{pmatrix}.$$

Vamos, como exemplo, tomar $m = 4 = 2^2$. Seguindo o que foi feito da seção III, se a permutação inicial for $abcd$, o grupo G terá as permutações

G
 $abcd$,
 $badc$

todas compreendidas na notação $\begin{pmatrix} x_{k,h} \\ x_{k+a,h} \end{pmatrix}$.

Como $p = 2$, o multiplicador Γ , gerado pelas substituições compreendidas na notação $\begin{pmatrix} x_{k,h} \\ x_{\lambda k,h} \end{pmatrix}$, não existe e, assim passamos àquele multiplicador que obedece as substituições compreendidas na notação $\begin{pmatrix} x_{k,h} \\ x_{k,\varphi(h)} \end{pmatrix}$. Tal grupo, dada a permutação inicial $abcd$, terá as permutações

$$\begin{array}{c} H \\ abcd . \\ cdab \end{array}$$

Ao aplicarmos as substituições de H em cada permutação de G , obtemos o produto $L = GH$

$$\begin{array}{c} L \\ abcd \\ badc . \\ cdab \\ dcba \end{array}$$

CONSIDERAÇÕES FINAIS.

Betti sempre foi um pioneiro, quer em assuntos políticos ou políticos educacionais de seu país, quer na participação internacional em pesquisas em Matemática. Sua contribuição à Teoria de Galois destaca-se devido ao seu espírito audacioso em investigar conceitos absolutamente novos e poderosos, mostrando ímpeto em arranhar a superfície de um assunto, até então, de difícil compreensão para todos.

A então chamada Teoria das Substituições, tal como apresentada na Parte Primeira, exhibe a relação que Betti faz entre permutação e substituição, diante de seu interesse na resolução de equações algébricas, numa conexão direta com a obra de Galois: uma permutação é a disposição das raízes de uma equação em certa ordem, enquanto que a substituição é a alteração dessa ordem. Na medida em que opera sucessivamente qualquer par de substituições, pela noção do que conhecemos atualmente por composição de funções, Betti obtém o conceito de substituição derivada, hoje conhecido por conjugação.

Betti define grupo de permutação: um *Grupo de permutações* será composto por uma série de permutações tais que uma substituição, executada em cada uma das permutações, realiza a troca entre elas sem produzir qualquer outra que não pertença à série, que no sentido moderno é aquele composto pelas substituições desse grupo

Estende o conceito de derivação para o que chamou de grupos derivados iguais e semelhantes. Dados dois grupos G , com n substituições θ , e Γ , com m substituições ψ , ao aplicarmos cada substituição de Γ em cada permutação de G obtemos os chamados grupos derivados de G por meio de ψ , podendo esses serem iguais, de mesmas substituições, ou semelhantes, com substituições diferentes, mas de igual número. A união de grupos derivados iguais é chamada produto $G\Gamma$. No sentido moderno, temos que cada derivado igual $D_{\psi_i} G$ é uma classe lateral de $G\Gamma$ e G será sub-grupo normal de $G\Gamma$.

Atualmente, pela Moderna Teoria de Galois, ao discutirmos se uma equação é resolúvel por radicais, tomamos o grupo de Galois, H , dessa equação e verificamos se podemos definir uma cadeia finita de subgrupos

$$H = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k,$$

onde cada N_i é sub-grupo normal de H e tal que todo sub-grupo quociente N_{i+1}/N_i seja abeliano, isto é, verificamos se o grupo é solúvel.

Dessa maneira, Betti caminha no sentido contrário; como ele não define, inicialmente, o que é o grupo de Galois da equação, começa com um grupo G de permutações das raízes e um outro grupo Γ e constrói $G\Gamma$, no qual G é normal. Se $G\Gamma$ não for máximo, ele constrói um $G\Gamma_1$, no qual $G\Gamma$ é normal, determinando, assim, uma cadeia ascendente e não descendente como fazemos hoje.

Na verdade, essas ideias estavam em gestação desde a pesquisa de Lagrange que, após estudar os métodos de solução para equações de grau 2, 3 e 4, investigou uma maneira de unificá-los, criando o procedimento que exemplificamos na seção 2.3. Ao substituir uma equação por outra, exibindo as raízes da primeira em função da segunda, percebeu que propriedades importantes da primeira, poderiam ser deduzidas examinando o efeito produzido pela permutação das raízes na segunda e na equação auxiliar.

Galois, influenciado pela ideias de Lagrange, estabeleceu as 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.

A obra de Betti como um todo, nos traz uma tentativa de maior sistematização tanto da então conhecida Teoria das Substituições, hoje Permutações, quanto da teoria proposta por Galois. Ela foi uma das principais referências para as obras de Cayley e Jordan, sendo essas o ponto de partida para os trabalhos dos matemáticos alemães no século XIX e início do século XX, de tal maneira que em todo esse processo, o conceito de grupo foi aos poucos se desprendendo do estudo das equações algébricas, tornando-se um conceito muito mais abstrato e abrangente.

BIBLIOGRAFIA.

[A1] 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] Belhoste, B. (1985). “*Cauchy, Um Mathématicien Légitimiste au XIX Siècle*”. Librairie Classique Eugène Belin.

[B2] Betti, E. (1851). “*Sopra la Risolubilità per Radicali delle Equazioni Algebriche Irreducibili di Grado Primo*”. *Annali di Scienze Matematiche e Fisiche* 2. p 5-19.

[B3] Betti, E. (1852). “*Sulla Risoluzione delle Equazioni Algebriche*”. *Annali di Scienze Matematiche e Fisiche*. T. III p 49-115.

[B4] Betti, E. (1855). “*Sopra la Teorica delle Sostituzioni*”. *Annali di Scienze Matematiche e Fisiche* 6. p 5-34.

[B5] Betti, E. (1903). *Opere Matematiche*. 2 Volumes. Milão: Ulrico Hoepli.

[B6] 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.

[C1] O'Connor, J.J & Robertson, E.F. *Enrico Betti*, in <http://www-history.mcs.st-and.ac.uk/~history/Biographies/Betti.html>, consultado em Janeiro de 2010.

- [C2] Corry, L. (1996). *Modern Algebra and the Rise of Mathematical Structures*. Basel, Boston, Berlin: Birkhäuser.
- [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. Domíngues. 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 lès conditions de résolubilité des équations par radicaux"*. Trad. Harold M. Edwards, in *Galois Theory*. New York: Springer-Verlag.
- [G2] Gatto, R. *"Lettere di Giuseppe Battaglini a Enrico Betti."* (Documenti per una Storia della Facoltà di Scienze dell'Università di Napoli) in *Annali di Storia della Scienza*, X, 1: 217-256.
- [G3] Giusti, E & Pepe, L. *"Un itinerario attraverso la matematica italiana contemporanea"*, in http://www.dm.unito.it/sism/m_italiani/schede_opere/saggio.html, consultado em Janeiro de 2010.
- [G4] Gonçalves, A. (2001). *"Introdução à Álgebra"*. Rio de Janeiro: IMPA.
- [G5] Grabner, J. V. (1975). *"The Mathematician, The Historian, and The History of Mathematics"*, in *Historia Mathematica* 2 p 439-447.
- [H1] Herstein, I. (1970). *"Tópicos de Álgebra"*. São Paulo: Polígono.
- [J1] Jordan, C. (1870). *"Traité des Substitutions"*. Paris: Gauthier-Villars.

- [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.
- [M1] Mammone, P. (1989). "Sur l'aport d'Enrico Betti en théorie de Galois" in *Bollettino di Storia delle Scienze Matematiche*, Anno IX – número 2, pp. 143-169.
- [M2] May, Kenneth O. (1975). "What is a good history and who should do it ?" in *Historia Mathematica*, Ano 1, número 2, pp. 449-455.
- [M3] Martins, C. R. P. (2006). "Resolução de Equações Algébricas por Radicais". Dissertação de Mestrado. UNESP-RC.
- [M4] 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.
- [M5] Milies, C. P. (2004) "*Breve História da Álgebra Abstrata*". II Bienal da Sociedade Brasileira de Matemática ([www. bienasbm.ufba.br/M18.pdf](http://www.bienasbm.ufba.br/M18.pdf)).
- [N1] Nagliati, I. (2000). "Le prime ricerche di Enrico Betti nel carteggio con Mossotti" in *Bollettino di Storia delle Scienze Matematiche*, Anno XX – número único, pp. 3-85.
- [N2] 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.

- [N3] 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.
- [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] Serret, J. A. (1877). "*Cours s'Algèbre Supérieure*", 2 vols. Paris: Gauthier-Villars.
- [S2] Smith, D. E. (1959). "*A Source Book in Mathematics*". Dover Publications: New York.
- [S3] Stillwell, J.(1989). "*Mathematics and Its History*". Springer-Verlag: New York. Undergraduate Texts in Mathematics.
- [S4] Stillwell, J.(1994). "*Elements of Algebra*". Springer-Verlag: New York. Undergraduate Texts in Mathematics.
- [W1] Wussing, H.(1984). "*The Genesis of the Abstract Group Concept*". The MIT Press: Massachusetts.

SULLA RISOLUZIONE DELLE EQUAZIONI ALGEBRICHE

MEMORIA

DEL SIG. DOTT. ENRICO BETTI

Professore di Matematiche nel liceo Forteguerri di Pistoja.

Nella presente memoria ho preso a trattare colla massima generalità i problemi relativi alla risolubilità delle equazioni algebriche, che si proposero i duo sommi geometri *Abel* e *Galois*, e intorno ai quali, per la morte che li rapì ambedue alla scienza ancor giovanissimi, non poterono lasciare altro che poche tracce della via tenuta per raggiunger lo scopo, e molti dei più importanti teoremi, ma privi in gran parte delle loro dimostrazioni.

Dopo che *Puolo Ruffini* di Modena ebbe dimostrata l'impossibilità di risolvere per radicali le equazioni di grado superiore al quarto in generale, *Abel* il primo si propose di determinare le condizioni da verificarsi, affinchè una equazione di grado qualunque fosse in particolare risolubile per radicali. Il metodo da lui seguito in questa ardua ricerca si trova in parte abbozzato in un frammento di memoria ritrovato tra le sue carte, e pubblicato nella collezione delle sue opere fatta per cura del professore *Holmboe*. I chiarissimi Sigg. *Malmsten* e *Luther* hanno sviluppato, ed esteso nel Giornale di *Crelle* questo bel metodo, per applicarlo, il primo, alla dimostrazione del teorema di *Abel* sulla risolubilità delle equazioni di grado primo, il secondo alla determinazione dei criterj di risolubilità delle equazioni di 5° e 6° grado.

Galois quasi contemporaneamente all' *Abel* meditava sullo stesso problema, e 17 mesi dopo la morte di questi, presentava all'Accademia delle Scienze di Parigi una memoria dove esponeva una nuova e profonda teoria da lui creata per risolvere il problema preso sotto un punto di vista più generale, e l'applicava alla dimostrazione di un teorema sulla risolubilità per

radicali delle equazioni di grado primo, il quale non è, come io ho già fatto conoscere (*), che una trasformazione di quello di *Abel*, poi dimostrato da *Malmsten*, e del quale egli non poteva aver cognizione. *Poisson* e *Lacroix* eletti a riferire sulla medesima la ritennero quasi inintelligibile, e rimproverarono al giovane autore la mancanza della chiarezza.

Il chiarissimo Sig. *Liouville*, pubblicando questa memoria, e altri frammenti sullo stesso soggetto ritrovati dopo la morte di *Galois*, annunciò di esser giunto, dopo aver colmato alcune leggieri lacune, a riconoscere l'esattezza intera del metodo col quale è provato in particolare il rammentato teorema, e fece conoscere la intenzione che egli aveva di pubblicare un Commentario per completare certi passaggi, e rischiarare certi punti delicati di quella memoria.

Le condizioni di risolubilità per radicali delle equazioni di grado primo possono pertanto ritenersi determinate e dimostrate con ambedue i metodi dei due sommi geometri. Rimanevano però fin ora da determinarsi quelle relative alle equazioni di grado non primo, molte delle quali trovansi annunziate da essi sotto forme differenti, può dirsi senza dimostrazione, nei frammenti postumi. Riempire questa lacuna è l'oggetto principale del mio lavoro.

Io ho istituita con qualche novità una teoria delle sostituzioni, e per mezzo di essa ho potuto dedurre con facilità e rigore dalla bella teoria del *Galois* che ho sviluppata ed estesa, la determinazione delle condizioni di risolubilità per radicali, delle equazioni di un grado qualunque, e dimostrare tutti i teoremi relativi, tanto sotto la forma nella quale li annunziò *Abel*, quanto sotto quella colla quale li annunziò *Galois*, e aggiungerne alcuni nuovi per completare la soluzione del problema.

Le condizioni generali necessarie e sufficienti alla risolubilità di una equazione di grado qualunque non le ho date

(*) Vedi Annali di scienze Fis. e Mat. compilati da B. Tortolini, febbrajo 1834.

soltanto per il caso in cui vogliasi una risoluzione per radicali, ma anche per quello in cui ci contenteremo di averla con radici di altre equazioni algebriche; e ho accennato un principio di classificazione degli irrazionali, il quale spero di potere sviluppare in altro lavoro.

Ho divisa la memoria in due parti. Nella prima ho esposta la teoria delle sostituzioni: nella seconda la determinazione delle condizioni di risolubilità delle equazioni algebriche.

P A R T E P R I M A

CAPITOLO PRIMO

DELLE SOSTITUZIONI

I.

PRINCIPI DEL CALCOLO DELLE SOSTITUZIONI

1.° Una *sostituzione* è la operazione mediante la quale si passa da una ad un'altra permutazione di più quantità.

Ci serviremo di una sola lettera x con diversi indici i posti al basso per distinguer tra loro tutte le quantità che entrano nelle permutazioni. Perciò potremo ritenere che ogni sostituzione si eseguisca sostituendo a tutti gli apici i una funzione $\varphi(i)$ dei medesimi; e la indicheremo colla notazione

$$\begin{pmatrix} x_i \\ x_{\varphi(i)} \end{pmatrix}.$$

La funzione $\varphi(i)$ dovrà godere la proprietà di prendere per tutti i valori successivi di i , li stessi valori che prende i , ma in ordine differente.

2.° Adotteremo diversi sistemi di apici secondo il numero n delle lettere.

1.° Se

$$n = p,$$

e p numero primo, prenderemo per apici le p radici della congruenza

$$x^p \equiv i \pmod{p},$$

le quali saranno i numeri naturali da zero a $p - 1$; poichè riguarderemo eguale a zero la parte di ogni numero multipla di p .

2.° Quando sia

$$n = p^v,$$

p un numero primo e v un numero qualunque, ci scriveremo per apici, delle p^v radici della congruenza

$$(1) \quad x^{p^v} \equiv i \pmod{p},$$

Galois ha osservato che, se

$$F(x) \equiv 0 \pmod{p}$$

è una congruenza irriducibile di grado v , e x una radice incommensurabile della medesima; tutte le radici della (1) sono date dalla espressione

$$x = a_0 + a_1 x + a_2 x^2 + \dots + a_{v-1} x^{v-1};$$

dove $a_0, a_1, \dots, a_{v-1}$ prendono successivamente tutti i valori interi minori di p , e si riguardano eguali a zero le quantità multiple di p (*). Le proprietà principali di questa specie di numeri complessi sono state poi dimostrate con molta chiarezza e rigore dal Sig. *Schönemann* in una Memoria inserita nel tomo 31 del giornale di Crelle, intitolata *Grandzüge einer allgemeinen Theorie von höhern Congruenzen*.

3.° Se

$$n = p^v q^\mu r^\sigma \dots,$$

e p, q, r numeri primi, e $v, \mu, \sigma \dots$ qualunque, distingue-

(*) Vedi Journal de Liouville T. XI, pag. 396, ovvero Bulletin de Ferrussac T. XIII, pag. 428.

remo le quantità con più apici per ciascuna lettera, i quali siano della natura dei precedenti, cioè radici delle congruenze

$$k^{p'} \equiv k \pmod{p}, \quad h^{q''} \equiv h \pmod{q}, \quad l^{r'''} \equiv l \pmod{r} \dots$$

Per brevità, in questa prima parte, indicheremo le sostituzioni col semplice segno delle funzioni degli apici che debbono sostituirsi ai medesimi per eseguirle, servendoci per il segno di funzione, sempre di lettere greche. Così scriveremo φ in luogo di $\begin{pmatrix} x_i \\ x_{\varphi(i)} \end{pmatrix}$.

4.° Le operazioni successive di più sostituzioni $\theta_0, \theta_1, \theta_2, \dots, \theta_{n-1}$ equivalgono a una sola sostituzione φ che rappresenteremo, come il primo fece *Cauchy* (*), col prodotto di quelle:

$$\varphi = \theta_0 \theta_1 \theta_2 \dots \theta_{n-1};$$

disponendo i fattori nell'ordine col quale sono state eseguite le rispettive sostituzioni

Se fosse

$$\theta_0 = \theta_1 = \theta_2 \dots = \theta_{n-1},$$

si avrebbe

$$\varphi = \theta^n.$$

5.° Se θ è una sostituzione circolare sopra p lettere, ripetuta p volte riprodurrà la permutazione d'onde siamo partiti; perciò si avrà la stessa permutazione eseguendola a o b volte, quando sia

$$a \equiv b \pmod{p},$$

e si potrà porre

$$\theta^{mp+a} = \theta^a;$$

onde si dovrà stabilire

$$\theta^p = 1.$$

6.° Ogni sostituzione, che non è circolare sopra un certo numero di lettere, equivale a più sostituzioni circolari effe-

(*) Vedi *Journal de l'École Pol.* T. X.

tuate sopra lettere differenti, è quindi con un ordine qualunque (*).

Siano $\varphi_0 \varphi_1 \dots \varphi_{m-1}$ queste sostituzioni circolari, avremo

$$\theta = \varphi_0 \varphi_1 \varphi_2 \dots \varphi_{m-1}$$

e ripetendola n volte, poichè è indifferente l'ordine con cui si eseguiscano le sostituzioni su lettere differenti, si otterrà

$$\theta^n = \varphi_0^n \varphi_1^n \varphi_2^n \dots \varphi_{m-1}^n.$$

Affinchè $\theta^n = 1$ è evidente che dovranno esser soddisfatte le seguenti equazioni

$$\varphi_0^n = 1, \varphi_1^n = 1, \varphi_2^n = 1, \dots, \varphi_{m-1}^n = 1.$$

Se $p_0 p_1 \dots p_{m-1}$ sono i numeri delle lettere sopra le quali rispettivamente sono eseguite le sostituzioni $\varphi_0 \varphi_1 \dots \varphi_{m-1}$, queste equazioni non potranno esser soddisfatte a meno che n non sia divisibile per $p_0, p_1, \dots, p_{m-1}$.

7.° Chiameremo *ordine* di una sostituzione il numero che indica quante permutazioni differenti si possono ottenere eseguendola più volte successive, o che è la minima potenza della sostituzione, che dà per risultato l'unità. Ciò che si è stabilito nei due paragrafi precedenti dà i seguenti teoremi:

1. Le potenze di una sostituzione, gli esponenti delle quali sono congrui rispetto all'ordine, sono eguali tra loro.

2. L'ordine di una sostituzione circolare su p lettere è eguale a p .

3. L'ordine di una sostituzione qualunque è eguale al minimo divisibile per tutti gli ordini delle sostituzioni circolari sopra lettere differenti, delle quali è il prodotto.

4. Se il numero p delle lettere è primo, ogni sostituzione di p^{esimo} ordine sarà circolare su tutte le lettere.

5. Una sostituzione di ordine primo p , o è circolare su p lettere, o è il prodotto di più circolari su p lettere differenti ciascuna.

(*) V. Serret, Cours d'Alg. sup. pag. 252 o Journal de l'Ecole Polytechnique T.X.

8.° La sostituzione mediante la quale dalla permutazione ottenuta colla θ^m , si torna a quella d'onde siamo partiti è θ^{p-m} ; se p è l'ordine di θ . Ora poichè $\theta^p = 1$ si potrà stabilire che

$$\theta^{p-m} = \theta^{-m},$$

ossia che un esponente negativo indica una sostituzione inversa a quella che rappresenterebbe quando si prendesse positivamente.

Per passare dalla permutazione ottenuta colla sostituzione θ^m a quella ottenuta colla ψ^m , la sostituzione da farsi potrà rappresentarsi con $\theta^{-m} \psi^m$.

9. Se si ha eguaglianza tra due prodotti di più sostituzioni si potranno moltiplicare ambedue a destra per una stessa sostituzione, come pure a sinistra; ma non però in generale uno a destra e l'altro a sinistra.

II.

DELLE SOSTITUZIONI DERIVATE.

10.° Allorchè più sostituzioni sono tali che le lettere cangiate da ciascuna di esse sono lasciate ferme da tutte le altre, il loro prodotto non varia se si cangia l'ordine col quale sono disposti i fattori. Ma se due sostituzioni θ o ψ inducono cangiamento anche sulle stesse lettere, non è più indifferente l'ordine dei fattori, non è più in generale

$$\theta\psi = \psi\theta,$$

ma invece

$$(1) \quad \theta\psi = \psi\theta_1;$$

dove θ_1 è un'altra sostituzione.

Moltiplicando da ambe le parti per ψ^{-1} si ricava

$$(2) \quad \theta_1 = \psi^{-1} \theta \psi.$$

La sostituzione θ_1 la diremo la *derivata di θ per mezzo di ψ* , θ la sostituzione *primitiva* e ψ la *derivante*.

La derivata di θ_1 la chiameremo *derivata seconda di θ* , la derivata della derivata seconda, derivata terza, e così di seguito.

Indichiamo colla notazione D_ψ^n la derivata n^{esima} di θ per mezzo di ψ ; avremo

$$(3) \quad D_\psi^n \theta \cdot \psi = \psi D_{\psi^{-1}}^{n+1} \theta; \quad D_\psi^m D_\psi^n \theta = D_\psi^{m+n} \theta; \quad D_\psi^0 \theta = \theta;$$

La quantità n la chiameremo l'indice della derivata.

11.° Prendiamo le equazioni

$$D_\psi \theta = \psi^{-1} \theta \psi, \quad D_\psi \varphi = \psi^{-1} \varphi \psi, \quad D_\psi \chi = \psi^{-1} \chi \psi$$

.

Moltiplicandole tra loro, avremo

$$D_\psi \theta \cdot D_\psi \varphi \cdot D_\psi \chi \dots = \psi^{-1} \theta \varphi \chi \dots \psi = D_\psi \theta \varphi \chi \dots$$

ossia: la derivata del prodotto di più sostituzioni è eguale al prodotto delle derivate delle medesime.

So

$$\theta = \varphi = \chi = \dots; \quad \text{sarà} \quad (D_\psi \theta)^n = D_\psi^n \theta;$$

essendo n il numero delle sostituzioni: dunque la derivata della potenza n^{esima} di una sostituzione è la potenza n^{esima} della derivata.

12.° Se

$$\theta^n = 1,$$

sarà

$$(D_\psi \theta)^n = D_\psi^n 1 = \psi^{-1} 1 \psi = 1:$$

viceversa, quando

$$(D_\psi \theta)^n = 1,$$

è

$$D_\psi \theta^n = 1;$$

e quindi

$$1 = \psi^{-1} \theta^n \psi, \quad \psi = \theta^n \psi, \quad 1 = \theta^n.$$

Di qui è facile dedurre che la sostituzione e la sua derivata sono dello stesso ordine.

13.° La derivata per mezzo di una sostituzione φ , della derivata per mezzo di un'altra ψ , di una qualunque θ , è eguale alla derivata della medesima θ per mezzo del prodotto $\psi\varphi$.

Infatti

$$\theta\psi = \psi D_{\psi} \theta, \quad D_{\psi} \theta \cdot \varphi = \varphi D_{\varphi} D_{\psi} \theta : . .$$

moltiplichiamo a sinistra la 2.^a per ψ , avremo riducendo colla 1.^a

$$\theta\psi\varphi = \psi\varphi D_{\varphi} D_{\psi} \theta;$$

ma

$$\theta\psi\varphi = \psi\varphi D_{\psi\varphi} \theta;$$

dunque

$$D_{\varphi} D_{\psi} \theta = D_{\psi\varphi} \theta;$$

e in generale si può dedurre da queste

$$(4) \quad \theta\gamma \dots \chi\psi\varphi = \gamma \dots \chi\psi\varphi D_{\gamma} D_{\psi} D_{\chi} \dots D_{\gamma} \theta$$

$$(5) \quad D_{\gamma} D_{\psi} D_{\chi} \dots D_{\gamma} \theta = D_{\gamma \dots \chi\psi\varphi} \theta.$$

Se

$$\varphi = \psi = \chi \dots = \gamma,$$

la (4) e la (5) divengono

$$(6) \quad \theta\psi^p = \psi^p D_{\psi}^p \theta,$$

o

$$(7) \quad D_{\psi^p} \theta = D_{\psi}^p \theta;$$

quindi la derivata per mezzo della potenza p^{esima} di una sostituzione è eguale alla derivata p^{esima} per mezzo della medesima sostituzione.

14.° Quando

$$D_{\psi}^p \theta = D_{\psi}^p \varphi$$

è anche (v. n.° 13.°)

$$D_{\psi^p} \theta = D_{\psi^p} \varphi,$$

quindi

$$\theta\psi^p = \varphi\psi^p, \quad \theta = \varphi;$$

dunque derivate dello stesso indice eguali hanno eguali le loro primitive.

Se $\psi^p = 1$, la (6) dà

$$(8) \quad D_{\psi}^n \theta = \theta ;$$

dalla quale si ricava

$$D_{\psi}^a \theta = D_{\psi}^b \theta$$

quando è

$$a \equiv b \pmod{p} ;$$

le derivate gl'indici delle quali sono congrui rispetto all'ordine della derivante sono eguali tra loro.

Sia ora n il minimo numero per il quale si abbia

$$(9) \quad D_{\psi}^n \theta = \theta,$$

e

$$(10) \quad p = mn + r,$$

essendo p l'ordine di ψ .

Derivando $(m-1)n$ volte la (7), si ha

$$(11) \quad D_{\psi}^{mn} \theta = D_{\psi}^{(m-1)n} \theta = \theta;$$

e dalla (8) sostituendo in essa a p il valore (10),

$$(12) \quad D_{\psi}^{mn} \theta. D_{\psi}^r \theta = \theta \dots$$

Eguagliando la (11) e la (12), si ha

$$D_{\psi}^{mn} \theta. D_{\psi}^r \theta = D_{\psi}^{mn} \theta;$$

onde

$$D_{\psi}^r \theta = \theta,$$

e perchè $r < n$, dovrà essero

$$r = 0.$$

Dunque l'indice minimo di una derivata eguale alla primitiva, è un divisore dell'ordine della derivante; e sono eguali le derivate che hanno gl'indici congrui rispetto al medesimo.

Se l'ordine di ψ è un numero primo p le derivate differenti di una sostituzione qualunque rispetto a ψ saranno p .

CAPITOLO SECONDO

DEI GRUPPI DI PERMUTAZIONI

I.

DELLE SOSTITUZIONI DI UN GRUPPO.

15.° Dicesi *Gruppo di permutazioni* una serie di permutazioni tali che una sostituzione mediante la quale si passa da una ad un'altra qualunque di esse, eseguita su tutte, non faccia che permutarle tra loro, senza produrne nessuna nuova che non appartenga già al gruppo. Si dicono sostituzioni del gruppo quelle colle quali si passa da una a tutte le altre permutazioni del medesimo. Se queste siano $\psi_0, \psi_1, \psi_2, \dots, \psi_{p-1}$, dovrà aversi

$$\psi_m \psi_n = \psi_r,$$

essendo r un valore intero dipendente da m e da n , e minore di p .

Un gruppo che contenga n permutazioni lo diremo di *grado* n^{esimo} .

Una funzione di più quantità che non muti valore altro che per le sostituzioni di un gruppo, avrà altrettanti valori quante sono le permutazioni di questo.

16.° Sia q l'ordine di una sostituzione ψ_0 del gruppo; q , o sarà eguale al numero delle permutazioni del gruppo medesimo, e si avranno con essa tutte le permutazioni: o sarà minore di quel numero, e se ne avranno soltanto q , e vi saranno poi delle altre sostituzioni. Sia una di queste ψ_1 di ordine n ; da ambedue si avranno qn permutazioni differenti; poichè supponiamone due eguali

$$\psi_0 \psi_1 = \psi_0' \psi_1' :$$

moltiplicando a destra per ψ_0^{-1} , a sinistra per ψ_1^{-1} ,

$$\psi_1^{-1} \psi_0 = \psi_1'^{-1} \psi_0' ,$$

Prendiamo $(s - s')^k \equiv 1 \pmod{n}$, e inalziamo alla potenza k , si avrebbe

$$\psi_1 = \psi_0^{r'^k},$$

e quindi la sostituzione ψ_1 non sarebbe altro che una potenza di ψ_0 , e non una nuova che potesse dare dello altro permutazioni. Se qn non è eguale al numero delle permutazioni del gruppo, si avrà anche un'altra sostituzione ψ_2 , colla quale si otterranno altre qn permutazioni, tutte differenti dalle precedenti: poichè supponiamo

$$\psi_0 \psi_1^s = \psi_0^u \psi_2^t,$$

si avrebbe

$$\psi_2 = \psi_0^{u/s} \psi_1^{t/s},$$

ossia ψ_2 eguale a una delle precedenti sostituzioni, contro il supposto. Se con queste $q(n+1)$ permutazioni non sono esaurito tutte quelle del gruppo, le altre sostituzioni non potranno egualmente dare che un numero multiplo di q : dunque l'ordine di una sostituzione qualunque di un gruppo è un divisore del numero delle permutazioni del gruppo.

Se un gruppo avrà un numero primo di permutazioni, le sostituzioni del medesimo saranno tutte potenze di una sola di ordine p .

17.° Chiameremo eguali due gruppi quando tutte le sostituzioni di uno saranno eguali a quelle dell'altro, ancorchè differenti siano le permutazioni.

Se le sostituzioni saranno differenti, ma nello stesso numero e di ordini eguali, i gruppi conterranno anche uno stesso numero di permutazioni, e li diremo simili.

II.

DEI GRUPPI DERIVATI SIMILI.

18.° Siano $\theta_0, \theta_1, \theta_2, \dots, \theta_{n-1}$ tutte le sostituzioni di un gruppo G ; $\psi_0, \psi_1, \dots, \psi_{n-1}$ quelle di un altro Γ . Un gruppo ottenuto

eseguendo sulle permutazioni di G una sostituzione ψ_m ha le sue sostituzioni derivate di quelle di G per mezzo di ψ_m , e perciò lo diremo *Gruppo derivato di G per mezzo di ψ_m* , e lo indicheremo colla notazione

$$D_{\psi_m} G$$

Poichè le sostituzioni derivate sono dello stesso ordine delle primitive (v. n.° 12), i gruppi derivati saranno o simili, o eguali al primitivo o tra loro.

I gruppi derivati di uno G per mezzo delle sostituzioni di un altro Γ si dicono *derivati di G per mezzo di Γ* , che dicesi *derivante*. Se sono simili e sommandoli si ha un gruppo, questo si chiamerà *gruppo della somma dei derivati di G per mezzo di Γ* .

19.° Una sostituzione φ che converte una permutazione di un gruppo G in una di un suo derivato, cangia il primo gruppo interamente nel secondo.

Infatti, sia

$$\vartheta_m \varphi = \psi_r D_{\psi_r} \vartheta_{m'}$$

Moltiplichiamo per ϑ_q a sinistra, avremo

$$\vartheta_q \vartheta_m \varphi = \vartheta_q \psi_r D_{\psi_r} \vartheta_{m'} = \psi_r D_{\psi_r} \vartheta_q \vartheta_{m'}$$

Ora

$$\vartheta_q \vartheta_m = \vartheta_a, \quad \vartheta_q \vartheta_{m'} = \vartheta_a \vartheta_m^{-1} \vartheta_{m'} = \vartheta_b;$$

onde

$$\vartheta_a \varphi = \psi_r D_{\psi_r} \vartheta_b$$

Poichè q e quindi a possono esser qualunque, se ne deduce che tutte le permutazioni di un gruppo rimangono cangiate in quelle di un suo derivato, quando rimanga cangiata una sola di esso in una di quelle dell'altro, come volevamo dimostrare.

20.° Se tutti i gruppi derivati sono soltanto simili, tutte le sostituzioni del gruppo H che ne è somma, li permuteranno tra loro; e il gruppo K somma di queste permutazioni conterrà un numero di sostituzioni eguale al numero delle sostituzioni

di II, e tutte di ordini rispettivamente eguali a quelli di queste ultime, e perciò sarà simile a II.

Il gruppo K lo diremo *gruppo delle permutazioni sopra i derivati*, e potremo stabilire che il *gruppo delle permutazioni sopra i derivati è simile al gruppo della somma dei derivati*, allorchando questi sono soltanto simili tra loro.

III.

DEI GRUPPI DERIVATI EGUALI.

21.° Quando i gruppi derivati per mezzo di un gruppo Γ sono tutti eguali ma non identici tra loro, cioè quando hanno eguali le sostituzioni, ma non le permutazioni, e si ha

$$G = D_{\psi_0} G = D_{\psi_1} G = \dots = D_{\psi_{n-1}} G;$$

il gruppo *derivante* Γ delle sostituzioni $\psi_0, \psi_1, \dots, \psi_{n-1}$, prenderà il nome di *moltiplicatore* del gruppo primitivo G ; e anche quello di *divisore* del gruppo H che risulta dalla somma di tutti i gruppi derivati.

Il gruppo H lo chiameremo il prodotto di G per Γ , e porremo

$$H = G\Gamma.$$

Se

$$\Gamma = G, \Gamma_1, \Gamma_1 = G_2, \Gamma_2, \dots, \Gamma_{n-2} = G_{n-2}, G_{n-1},$$

sarà

$$H = G G_1 G_2 \dots G_{n-1};$$

e poichè l'ordine di questi fattori non è indifferente, distingueremo questi gruppi tra loro, chiamando G_{n-1} il 1.° divisore, G_{n-2} il 2.° G l' n^{esimo} , ultimo divisore; e G_1 il primo, G_2 il 2.° G_{n-1} l' $(n-1)^{\text{esimo}}$ moltiplicatore di G .

Se non possono esistere altri moltiplicatori dopo Γ , si dirà questo il *massimo moltiplicatore* di G .

Un gruppo che non ammette nessun divisore lo diremo *primo*. Uno che non abbia nessun moltiplicatore gruppo *massimo*.

Poichè del gruppo H le sole sostituzioni che ha comuni con Γ permutano tra loro i derivati di G ; si può stabilire che

il gruppo delle permutazioni sopra i derivati per mezzo di un moltiplicatore di essi è simile a questo moltiplicatore.

22.° Il derivato del prodotto di più gruppi è eguale al prodotto dei derivati di ciascuno di essi presi nello stesso ordine.

Sia

$$H = G\Gamma,$$

e θ_m le sostituzioni di G , ψ_n quelle di Γ ; avremo

$$D_{\psi_n} \theta_m = \theta_{m'}.$$

Deriviamo H per mezzo di φ ; nel gruppo che si otterrà, alle θ_m corrisponderanno le $D_\varphi \theta_m$, alle ψ_n , le $D_\varphi \psi_n$. Ora si ha (v. n.° 11.)

$$D_\varphi \theta_m D_\varphi \psi_n = D_\varphi \theta_m \psi_n = D_\varphi \psi_n \theta_{m'} = D_\varphi \psi_n D_\varphi \theta_{m'};$$

onde

$$D_{D_\varphi \psi_n} D_\varphi \theta_m = D_\varphi \theta_{m'},$$

e il gruppo $D_\varphi H$ sarà il prodotto dei due derivati

$$D_\varphi G \text{ e } D_\varphi \Gamma;$$

$$D_\varphi G\Gamma = D_\varphi G D_\varphi \Gamma;$$

e in generale se

$$H = G G_1 G_2 \dots G_{n-1};$$

$$D_\varphi H = D_\varphi G D_\varphi G_1 D_\varphi G_2 \dots D_\varphi G_{n-1}.$$



CAPITOLO TERZO

DELLA DETERMINAZIONE DEI MOLTIPLICATORI E DIVISORI DI UN GRUPPO.

I.

EQUAZIONI DEL MASSIMO MOLTIPLICATORE E DEI DIVISORI DI UN GRUPPO.

23.° Dato un gruppo, possono esser proposti due problemi; determinarne, 1.° i gruppi moltiplicatori, 2.° i divisori.

La soluzione di ambedue questi problemi richiede prima la determinazione di una funzione θ degli apici che dia tutte le sostituzioni del gruppo per i differenti valori che prendono le costanti o parametri che entrano nella medesima.

1. Per la determinazione dei moltiplicatori osserviamo che, indicando con ψ le loro sostituzioni, e con θ quelle del gruppo dato II, dovranno i derivati per mezzo delle ψ essere eguali tra loro, e quindi le sostituzioni derivate delle θ per mezzo di ψ eguali ad altre delle medesime θ ; onde deve aversi la equazione

$$(13) \quad D_{\psi} \theta_n = \theta_m;$$

dove essendo θ_n una sostituzione del gruppo dato, θ_m ne è un'altra le costanti della quale sono dipendenti da quelle di θ_n . Questa equazione corrisponde all'altra

$$(14)' \quad \psi[\theta_n(i)] = \theta_m[\psi(i)].$$

Il valore di ψ che è l'integrale più generale di questa conterrà tutti i valori che soddisfano la (14), o quindi tutte le sostituzioni del massimo moltiplicatore del gruppo proposto.

2. Passiamo ora alla decomposizione di un gruppo nei suoi successivi divisori primi.

Siano

$$(a) \quad \theta_{a_1} \theta_{a_2} \theta_{a_3} \dots \theta_{a_{v-2}},$$

le sostituzioni di un gruppo G ,

$$(b) \quad \theta_{b_1} \theta_{b_2} \theta_{b_3} \dots \theta_{b_{v-2}};$$

quelle di un altro Γ_n : affinchè un gruppo H sia il prodotto di questi, cioè

$$H = G\Gamma_n,$$

sarà necessario e sufficiente che le (a) formino un gruppo effettivo, e che quindi soddisfacciano la equazione

$$(15) \quad \theta_{a_n} \theta_{a_m} = \theta_{a_r}$$

(v. n.° 15.°); e che inoltre siano eguali i derivati di G per mezzo di Γ_n (v. n.° 21.°), cioè

$$(16) \quad D_{\theta_b} \theta_{a_n} = \theta_{a_n},$$

$$(17) \quad \theta_b [\theta_{a_n}(i)] = \theta_{a_n} [\theta_b(i)].$$

Le sostituzioni di Γ_n che sono il prodotto di una medesima sostituzione per due differenti dello (a), danno dei derivati non solo eguali, ma anche identici, cioè colle stesse permutazioni, o quindi esse dovranno ritenersi eguali tra loro nel gruppo Γ_n ; il grado del quale sarà dato perciò dal numero di quelle sostituzioni soltanto che permutano effettivamente tra loro i derivati, e che perciò non hanno per fattore nessuna delle (a), o potranno anche non formare un vero gruppo. Con questa considerazione riman sempre vero il teorema del num.° 21, e inoltre si può stabilire che il prodotto dei gradi dei divisori di un gruppo è eguale al grado del gruppo stesso.

I valori più generali che soddisfanno le equazioni (15) e (17) danno le sostituzioni del secondo divisore G , sul quale operando come sopra H , se ne potrà ottenere un terzo G_1 , e così seguitando si giungerà finalmente a un ultimo divisore primo Γ_1 .

Le sostituzioni dell'ultimo gruppo G_{n-2} di cui è divisore Γ_1 , private dei fattori eguali a qualcuna delle sostituzioni di Γ_1 , daranno un primo moltiplicatore Γ_2 , quelle di G_{n-3} , tolti da essi fattori eguali a alcuna di quelle di G_{n-2} , daranno un secondo moltiplicatore Γ_3 , e così di seguito avremo tutti i moltiplicatori fino all'ultimo Γ_n , e sarà

$$H = \Gamma_1 \Gamma_2 \Gamma_3 \dots \Gamma_n.$$

Tutti questi divisori saranno primi, perchè altrimenti non si sarebbero presi per i valori che soddisfanno la (15) e la (17) tutti i possibili come abbiamo supposto.

Quando si trovassero una serie di valori (a) che soddisfacessero la (15) e non la (17), le sostituzioni che essi rappre-

senterebbero; darebbero tanti gruppi derivati simili, quante fossero quelle di II non comprese nelle (a). La decomposizione di un gruppo nei suoi divisori primi corrisponde a quella che Galois chiamava *decomposizione propria*. La determinazione di più derivati simili dei quali un gruppo dato sia la somma, corrisponde alla decomposizione che egli chiamava *impropria*.

Nella ricerca dei moltiplicatori di un gruppo distingueremo tre casi: 1.° quello nel quale il numero delle lettere è primo: 2.° quando è il prodotto di numeri primi differenti tra loro: 3.° quando è una potenza di un numero primo.

II.

MASSIMO MOLTIPLICATORE DEI GRUPPI DI UN NUMERO PRIMO
DI PERMUTAZIONI SOPRA UN NUMERO EGUALE DI LETTERE.

21.° Sia p il numero primo delle lettere, o delle permutazioni del gruppo. Le sostituzioni del gruppo saranno tutte le potenze differenti di una sola di ordine p (v. n. 16), circolare sopra tutte le lettere (v. n. 7.4), la quale disponendo convenientemente gli apici numerici i della prima permutazione, sarà

$$\varphi(i) = i + 1.$$

La equazione (14) da integrarsi per avere il massimo moltiplicatore diverrà

$$\psi(i+1) = \psi(i) + a,$$

la quale ha per integrale generale

$$\psi(i) = ai + b = a(i + c) = a [\varphi(i)]^c,$$

dove $ac \equiv 1$.

Le potenze di $\varphi(i)$ essendo poi sostituzioni del gruppo primitivo, tutte le sostituzioni del massimo moltiplicatore saranno date da

$$\psi(i) = ai;$$

ed essendo λ una radice primitiva di p , e ponendo

$$\theta(i) = \lambda i;$$

tutte saranno potenze di $\theta(i)$: dunque le sostituzioni del massimo moltiplicatore di un gruppo di un numero primo di permutazioni sopra un numero primo di lettere, e che perciò ha per sostituzioni le potenze di $\binom{i}{i+1}$ soltanto, sono tutte potenze della unica

$$\binom{i}{\lambda i};$$

e quindi il gruppo le cui sostituzioni sono tutte comprese nella notazione

$$\binom{i}{ai+b}$$

è un massimo.

III.

MASSIMO MOLTIPLICATORE DI UN GRUPPO DI UN NUMERO PRIMO
DI PERMUTAZIONI SOPRA UN NUMERO DI LETTERE CHE HA
DEI FATTORI PRIMI DIFFERENTI TRA LORO.

25.° Sia primo il numero p delle permutazioni di un gruppo G , e il numero m delle lettere che entrano nelle medesime, sia il prodotto di più fattori primi differenti tra loro. Avremo che tutte le sostituzioni di G saranno potenze di una sola di ordine p (V. num. 16) che risulterà dal prodotto di q circolari, ciascuna sopra un sistema di p lettere differenti (v. n.° 7: 5) Distinguiamo tra loro con un primo apice k le lettere di un sistema, con un secondo h indiciamo il sistema al quale appartengono. Il simbolo

$$\binom{x_k, h}{x_{k+a}, h}$$

comprenderà tutte le sostituzioni di G .

Un primo moltiplicatore, per ciò che si è detto precedentemente (v. n.° 24) sarà un gruppo Γ le sostituzioni del quale sono potenze di

$$\binom{x_k, h}{x_{\lambda k}, h}.$$

Moltiplicatore del gruppo GI , che ne risulta, sarà ogni gruppo II che non abbia altre sostituzioni che sui sistemi; cioè comprese nella notazione

$$\begin{pmatrix} x_k, h \\ x_k, o(h) \end{pmatrix};$$

perchè evidentemente queste non cangiano le permutazioni delle lettere di ogni sistema in particolare.

26.° Un gruppo $L = KH$, dove K non abbia altre sostituzioni che sopra gl'indici k , H sopra gli h , lo diremo a *lettere congiunte*, e *lettere congiunte* quelle che hanno uno stesso indice h . Tra le sostituzioni di K ve ne potranno essere anche alcune che permutino soltanto gl'indici k di uno, o di alcuni sistemi; come pure alcune che permutino quelli di un sistema in un modo, e quelli di un altro in un modo differente. Ma vi dovranno essere insieme tutte le derivate differenti di queste sostituzioni, per mezzo di un'altra qualunque sopra gl'indici h soltanto.

Se non esiste alcun moltiplicatore del gruppo, che dia un prodotto a lettere congiunte, L sarà un gruppo *massimo*, o *meno*, che il numero delle lettere che entrano nelle permutazioni non abbia tutti eguali tra loro i suoi fattori primi come passiamo a dimostrare.

Supponiamo che sia un moltiplicatore di L il gruppo Γ di ν permutazioni. Le sostituzioni $\psi_0, \psi_1, \dots, \psi_{\nu-1}$ di esso non potranno essere nè sugli indici h , nè sui k soltanto, perchè altrimenti L non sarebbe il massimo gruppo a lettere congiunte, come abbiamo supposto.

Le lettere che in un gruppo derivato $D_{\psi_n} L$ corrispondono a quelle di ciascuno dei diversi sistemi di lettere congiunte nel primitivo L , formeranno altrettanti nuovi sistemi di lettere congiunte nel derivato, e poichè i gruppi L e $D_{\psi_n} L$ sono eguali, le lettere congiunte nell'uno sono congiunte anche nell'altro, e quindi nel gruppo L le m lettere si potranno disporre almeno in ν differenti modi in q sistemi di p lettere congiunte ciascuno.

Fra questi modi ve ne sarà sempre uno tale, che faccia appartenere due lettere qualunque per es. x_a , x_b , allo stesso sistema.

Infatti tutte le lettere che fanno parte dei sistemi che contengono la lettera x_a non potranno esser differenti da tutte quelle dei sistemi che contengono x_b ; perchè altrimenti tanto quelle che queste farebbero un sistema di lettere congiunte nel gruppo $L\Gamma$, contro il supposto. Sia per tanto x_c una lettera che fa parte di un sistema con x_a e di uno con x_b . Nel gruppo L non vi saranno sostituzioni che cangiano x_c in una lettera di un sistema qualunque, e che non permutino contemporaneamente x_a e x_b in due altro del medesimo; dunque x_a e x_b faranno parte di uno stesso sistema, c. v. d.

27.° Due lettere non possono far parte altro che di un solo sistema di lettere congiunte. È chiaro se $p=2$. Se $p>2$, supponiamo che x_a e x_b facciano parte di due sistemi differenti in tutte le altre lettere. Nel gruppo L , in questo caso, non vi sarebbe sostituzione che permutasse x_a senza permutare anche x_b , e viceversa: poichè anche cangiando x_a in una x_c a lei congiunta, x_a formando parte con x_b anche di un altro sistema che non contiene x_c , dovrebbero tutte le lettere di questo ultimo rimaner cangiate in quelle del primo, e quindi anche la x_b . Quelle lettere poi nelle quali rimarrebbero cangiate x_a e x_b , verrebbero a far parte di due sistemi, e sarebbero nello stesso caso; e così di seguito. Dunque L sarebbe un gruppo a lettere congiunte, i sistemi del quale sarebbero di due lettere, contro il supposto.

Uguualmente si dimostrerebbe lo stesso per un numero di lettere > 2 e $< p$. Dunque i sistemi differenti di lettere congiunte avranno una sola lettera eguale.

28.° Disposte le lettere in un modo qualunque in sistemi congiunti, sarà sempre possibile anche un'altra disposizione (v. n.° 26), nella quale un sistema non potrà contenere che una lettera di ciascuno dei primi (v. n.° 27); dunque, le lettere di ogni sistema essendo p , i sistemi saranno almeno p , e le lettere p^2 . Siano le seguenti linee orizzontali i primi p sistemi

di lettere congiunte, e quello formato da una di ciascuno di essi sia la prima linea verticale

$$(A) \left\{ \begin{array}{ccccccc} x_{0,0} & x_{1,0} & x_{2,0} & \dots & x_{p-1,0} \\ x_{0,1} & x_{1,1} & x_{2,1} & \dots & x_{p-1,1} \\ \dots & \dots & \dots & \dots & \dots \\ x_{0,p-1} & x_{1,p-1} & x_{2,p-1} & \dots & x_{p-1,p-1} \end{array} \right.$$

e poichè nei sistemi di lettere congiunte non si possono mutare alcune di uno in alcune di un altro senza mutarle tutte quante; le sostituzioni sulle lettere di una linea orizzontale, o lasceranno ferma la prima linea verticale, o ne convertiranno tutte quante le lettere in altre corrispondenti rispettivamente alla stessa linea orizzontale, e congiunte tra loro: le quali potremo supporre essere quelle di una delle altre linee verticali: poichè la prima permutazione è arbitraria. In conseguenza nel quadro (A) saranno linee congiunte tanto quelle situate in una stessa linea orizzontale, quanto quelle della medesima verticale.

Ora osserviamo che le sostituzioni del gruppo L non possono lasciare una linea verticale ferma, e permutar le altre; perchè altrimenti contro ciò che abbiamo dimostrato al n.° 26, due lettere di due sistemi verticali non potrebbero esser congiunte; lo stesso può dirsi delle orizzontali; dunque tutte le sostituzioni di L non potranno essere che le circolari comprese nella notazione

$$\left(\begin{array}{c} x_k, a \\ x_{k+a}, a+b \end{array} \right);$$

e saranno congiunte anche tutte le lettere che si trovano sulla stessa diagonale.

Se le lettere sono in numero maggiore di p^2 , a quelli del quadro (A) andranno aggiunti altri sistemi; e sarà possibile un'altra disposizione in sistemi di lettere congiunte, in ciascuno dei quali entri una sola delle lettere del quadro A (ved. num. 26, 27); dunque per ciascuna delle p^2 lettere ve ne saranno

altre $p-1$; onde le lettere saranno almeno p^3 . E poichè non si può permutare una lettera del quadro (A) in una che non si trovi in esso, senza convertirle tutte quante in altre egualmente congiunte; le p^3 lettere si potranno disporre in p sistemi di lettere congiunte simili ad (A).

Distinguiamo con un terzo apico l le lettere di questi sistemi: poichè non si può tener fermo nessuno di questi sistemi permutandone alcuni tra loro, anche rispetto all'apico l saranno in L le sostituzioni tutte circolari; e quindi tutte quante comprese nel simbolo

$$\begin{pmatrix} x_k, h, l \\ x_{k+a}, h+b, l+c \end{pmatrix}.$$

Generalizzando si può finalmente stabilire il seguente Teorema:

Affinchè un gruppo a lettere congiunte ammetta un moltiplicatore per il quale moltiplicato, il prodotto non sia a lettere congiunte, è necessario che il numero delle lettere sia la potenza di un numero primo, e che esso non contenga altre sostituzioni che quelle comprese nel simbolo

$$\begin{pmatrix} x_k, h, l, \dots \\ x_{k+a}, h+b, l+c, \dots \end{pmatrix}.$$

Un gruppo di permutazioni di un numero di lettere che ammette dei fattori primi differenti tra loro, non può aver per divisore nessun gruppo a lettere congiunte, a meno che non sia a lettere congiunte esso stesso.

IV.

MASSIMO MOLTIPLICATORE DI UN GRUPPO DI UN NUMERO PRIMO
DI PERMUTAZIONI SOPRA UN NUMERO DI LETTERE
CHE È POTENZA DI UN NUMERO PRIMO

29.° Sia p^v il numero delle lettere, p numero primo e v qualunque. Il gruppo di p permutazioni sarà a lettere congiunte, e un divisore di quello, le sostituzioni del quale sono comprese tutte nella notazione

$$(a) \quad \begin{pmatrix} x_k, l, m, \dots \\ x_{k+a}, h+b, l+c, m+d, \dots \end{pmatrix}$$

Determineremo perciò il massimo moltiplicatore di questo ultimo gruppo.

Adottiamo per apici delle lettere, come abbiamo detto in principio, le p radici della congruenza

$$(b) \quad k^p \equiv k \pmod{p};$$

le quali sappiamo essere espresse da

$$k = a_0 + a_1 i + a_2 i^2 + \dots + a_{v-1} i^{v-1};$$

dove i è radice incommensurabile della congruenza di grado v , irriducibile

$$(c) \quad F(i) \equiv 0 \pmod{p}.$$

I coefficienti della i corrisponderanno agli apici $k, l, m, n, \dots$, onde le sostituzioni (a) saranno tutte date da

$$\left\{ \begin{array}{l} x_{a_0+a_1 i+a_2 i^2+\dots+a_{v-1} i^{v-1}} \\ x_{a_0+a+(a_1+b)i+(a_2+c)i^2+\dots+(a_{v-1}+g)i^{v-1}} \end{array} \right\}$$

o anche, poichè $a + bi + ci^2 + \dots + gi^{v-1}$ è una radice k_0 della (b), queste sostituzioni possono rappresentarsi con

$$(d) \quad \begin{pmatrix} x_k \\ x_{k+k_0} \end{pmatrix},$$

dove k_0 può avere per valori tutte le radici della (b). Onde le permutazioni che con esso si ottengono saranno p^v ; e, poichè $pk_0 \equiv 0$, tutte quelle sostituzioni saranno di ordine p .

Sia $\psi(k)$ una sostituzione del moltiplicatore Γ del gruppo G che nasce dalle sostituzioni (d); dovrà aversi (v. n.° 23°)

$$(e) \quad \psi(k + k_0) \equiv \psi(k) + k_0$$

dove k_0 è pure una radice della (b) dipendente da k_0 .

L'integrale più generale della congruenza (e) alle differenze finite è

$$\psi(k) \equiv \sum_{n=0}^{n=\nu-1} B_n k^{p^n} + B_\nu ;$$

dove i B_n sono radici della (6) tali che

$$\sum_{n=0}^{n=\nu-1} B_n k_0^{p^n} \equiv h_0 .$$

È facile verificare questo integrale ponendo mente alla proprietà, della quale godono questa specie di quantità, che cioè

$$(k + k_0)^{p^n} \equiv k^{p^n} + k_0^{p^n} .$$

Poichè le sostituzioni

$$\begin{pmatrix} x_k \\ x_{k+B_\nu} \end{pmatrix}$$

appartengono tutte al gruppo G ; tutte le sostituzioni del massimo moltiplicatore Γ saranno soltanto quelle comprese nel simbolo

$$\cup \begin{pmatrix} x_k \\ \sum_{n=0}^{n=\nu-1} B_n k^{p^n} \end{pmatrix}$$

Esprimendo le B_n e k in funzione di i , è facile ottenere la (7) sotto la forma

$$(f') \left\{ \begin{array}{l} x_{a_0 + a_1 i + a_2 i^2 + \dots + a_{\nu-1} i^{\nu-1}} \\ x_{m_0 a_0 + m_1 a_1 + \dots + m_{\nu-1} a_{\nu-1} + (m'_0 a_0 + m'_1 a_1 + \dots + m'_{\nu-1} a_{\nu-1}) i + \dots} \\ \quad + (m''_0 a_0 + m''_1 a_1 + \dots + m''_{\nu-1} a_{\nu-1}) i^2 + \dots \end{array} \right\}$$

dove tutte le a o le m sono numeri interi eguali o maggiori di zero, e $< p$.

Per qualunque valore dei B_n non si hanno sempre sostituzioni. Poichè tutte le permutazioni non devono contenere

che una sola volta una medesima lettera, sarà necessario che i B_n siano tali che la congruenza

$$\sum_{n=0}^{p^v-1} B_n k^{p^n} \equiv k_0$$

non abbia che una sola radice comune colla (b) qualunque sia k_0 .

30.° Tutte le sostituzioni (f) di Γ lasciano ferma la x_0 ; ed esso è un gruppo a lettere congiunte rispetto alle altre $p^v - 1$. Infatti se

$$\sum_{n=0}^{p^v-1} B_n k^{p^n} \equiv k_1,$$

anche

$$\sum_{n=0}^{p^v-1} B_n (ak_0)^{p^n} \equiv ak_1$$

dove a è un intero qualunque $< p$; poichè

$$a^{p^n} \equiv a;$$

duque nel gruppo massimo moltiplicatore lo $p^v - 1$ lettere che hanno per indici le radici della congruenza

$$k^{p^v-1} \equiv 1 \pmod{p},$$

si dividono in $\frac{p^v-1}{p-1}$ sistemi di $p-1$ lettere congiunte ciascuno, e queste sono precisamente quelle gli apici delle quali hanno un rapporto numerico.

31.° Il numero di lettere che può lasciar ferme una sostituzione (c) è sempre un divisore p^m di p^v .

Sia x_{k_0} una lettera che rimanga ferma per una delle (f); si avrà

$$(g) \quad \sum_{n=0}^{p^v-1} B_n k_0^{p^n} = k_0;$$

della quale saranno radici tutti gli apici dello stesso sistema di lettere congiunte, ak_0 : dunque se sta ferma una lettera ne staranno ferme almeno p .

Sia k_1 un'altra radice della (g) diversa dalle precedenti; ne saranno radici anche tutti i p^2 valori, che prende la espressione

$$ak_0 + bk_1,$$

ponendo in essa per a e per b tutti i numeri intieri $< p$. Questi p^2 valori saranno differenti, poichè altrimenti si avrebbe

$$ak_0 + bk_1 \equiv a_1k_0 + b_1k_1 \pmod{p},$$

ossia

$$(a - a_1)k_0 \equiv (b_1 - b)k_1.$$

Moltiplicando per un numero h tale, che

$$(b_1 - b)h \equiv 1,$$

si ha

$$k_1 \equiv (a - a_1)hk_0$$

contro il supposto: dunque se stanno ferme più di p lettere, ne staranno ferme almeno p^2 .

Se sta ferma un'altra lettera, sia l'apice di questa k_2 , che sarà una radice della (g) differente dalle precedenti: o ne saranno radici tutte le p^3 comprese al solito nella espressione

$$ak_0 + bk_1 + ck_2;$$

e queste saranno tutte differenti; che altrimenti si avrebbe

$$ak_0 + bk_1 + ck_2 \equiv a_1k_0 + b_1k_1 + c_1k_2;$$

ossia

$$(a - a_1)k_0 + (b - b_1)k_1 \equiv (c_1 - c)k_2;$$

e moltiplicando per il numero h che dà

$$(c_1 - c)h \equiv 1,$$

si ha

$$k_2 \equiv h(a - a_1)k_0 + h(b - b_1)k_1,$$

contro ciò che avevamo supposto: così seguitando, si può stabilire, che le lettere che stanno ferme saranno sempre in numero p^n divisore di p^n .

32.° Le ν lettere che hanno per apici $k_0, k_1, k_2, \dots, k_\nu$ tali, che uno qualunque di essi non si può esprimere linearmente per gli altri, non possono esser lasciate ferme da nessuna sostituzione che non lasci fermo altresì tutte quante le lettere, cioè che non equivalga a nessuna operazione. Queste lettere possono essere una radice primitiva λ di p , e le potenze di una radice i della congruenza (c).

Per le sostituzioni potenze di

$$\begin{pmatrix} x_k \\ x_p \end{pmatrix}$$

non possono esser lasciate ferme che le p lettere

$$x_0, x_1, x_2, \dots, x_{p-1};$$

poichè i numeri interi $< p$ sono le uniche radici della congruenza

$$k^p \equiv k \pmod{p}.$$

33.° Dal non esser contenute nel gruppo Γ le sostituzioni che lasciano ferme un numero di lettere differente da p^m , dove m è un intero qualunque minore di ν , si deduce che tutte le sostituzioni di Γ sono di ordine $p^\nu - p^m$, o che quindi (vedi n.° 16.) il numero delle permutazioni del gruppo massimo che non è a lettere congiunte, e che ammette un divisore a lettere congiunte è eguale a M o a un divisore di M , essendo

$$M = p^\nu(p^\nu - 1)(p^\nu - p) \dots (p^\nu - p^{\nu-1}).$$

V.

DECOMPOSIZIONE DI UN GRUPPO NEI SUOI DIVISORI PRIMI.

34.° Abbiamo già osservato (v. n.° 23) che quando sia dato un gruppo, e si voglia decomporlo nei gruppi primi dei quali

è il prodotto, è necessario determinare prima la funzione $\theta(i)$ degl'indici, la quale dà per tutti i differenti valori dei suoi parametri, tutte le sostituzioni del gruppo; poi risolvere le equazioni (15) e (17). Quando non esistano valori dei parametri di θ , che le soddisfacciano, il gruppo è primo. La classificazione dei gruppi primi sarà soggetto di un altro mio lavoro, se avrò agio a seguitare con risultato le ricerche intraprese. Ora mi contenterò di parlare dei gruppi di prima classe, dei quali solo abbisognano le applicazioni che fo nella seconda parte di questa Memoria.

Gruppi di *prima classe* diremo quelli che contengono un numero primo di permutazioni; e che perciò hanno tutte le loro sostituzioni potenze di una soltanto (v. n.° 16).

35.° *I gruppi le sostituzioni dei quali sono tutte quante potenze di una sola θ di ordine m , sono decomponibili in tanti gruppi di prima classe quanti sono i fattori primi di m , e che sono di grado rispettivamente eguale a questi fattori.*

Infatti, se $m = pn$, dove p è un fattore primo; la funzione che dà tutte le sostituzioni del gruppo è θ^n . La equazione (17) diviene in questo caso

$$\theta^{a+b}(i) = \theta^{c+a}(i);$$

la quale è soddisfatta da

$$b = c,$$

qualunque sia a . La equazione (15) poi diviene

$$\theta^{b_m} \theta^{b_n} = \theta^{b_r};$$

che è soddisfatta da $b_i = pi$. L'ultimo divisore avrà dunque per sostituzioni

$$\theta^p \theta^{2p} \theta^{3p} \dots \theta^{p(n-1)}$$

e per l'altro rimarranno

$$\theta, \theta^2, \theta^3 \dots \theta^{p-1}.$$

Questo è di prima classe e di grado p , e quello è puro di prima classe se n è primo, altrimenti è decomponibile nuo-

vamente in uno di prima classe e in un altro che è di prima classe, oppure decomponibile, e così di seguito.

36.° Un gruppo di grado pq , le permutazioni del quale si ottengono tutte con due sostituzioni una di ordine p l'altra di ordine q , è sempre il prodotto di due gruppi di prima classe, o prodotti di gruppi di prima classe, e se $p > q$ il primo divisore è di grado q^{imo} , il secondo di grado p^{imo} .

Se θ è la sostituzione di ordine p , ψ quella di ordine q , è evidente che tutte le permutazioni si otterranno eseguendo sopra una sola le sostituzioni

$$\theta^m \psi^n$$

prendendo per m tutti i valori da 0 a $p-1$ inclusivamente, e per n da 0 a $q-1$.

Se si eseguissero invece prima tutte le sostituzioni

$$\theta^m \psi,$$

e poi su questo nuovamente tutte le potenze di θ , si avrebbero p^2 permutazioni, cioè un numero $> pq$, e in conseguenza alcune dovrebbero esser eguali, e quindi si avrebbero alcuni valori a, a', b o b' per i quali

$$\theta^a \psi \theta^{a'} = \theta^b \psi \theta^{b'},$$

o anche

$$\theta^{a-b} \psi = \psi \theta^{b'-a'};$$

ed essendo h dato dalla congruenza

$$h(a-b) \equiv 1 \pmod{p},$$

risulterebbe

$$\theta \psi = \psi \theta^{h(b'-a')} = \psi \theta^k,$$

posto

$$k = h(b'-a');$$

o quindi

$$D_\psi \theta = \theta^k;$$

dalla quale si ha qualunque sia m (v. n.° 11)

$$D_\psi \theta^m = \theta^{mk};$$

onde chiamando G il gruppo delle θ

$$D_4 G = G:$$

e detto Γ il gruppo delle ψ , sarà il proposto eguale al prodotto $G\Gamma$, come volevamo dimostrare.

Le sostituzioni di un gruppo pg , quando p e q siano primi, sono di ordine p o di ordine q (v. n.° 16): dunque ogni gruppo il grado del quale è il prodotto di due numeri primi differenti non è mai primo.

37.° È evidente una prima decomposizione dei gruppi a lettere congiunte in due, uno dei quali contenga tutte le sostituzioni sulle lettere congiunte, e l'altro quelle sui sistemi delle medesime; e per avere i gruppi primi, in questo caso basta determinare i divisori primi di questi due

38.° Il massimo moltiplicatore Γ del gruppo a lettere congiunte (d) nel caso che le lettere siano la potenza di un numero primo p^n è sempre decomponibile in più gruppi primi, ma che in generale non sono tutti di prima classe.

Le sostituzioni di questo moltiplicatore sono tutte date dalla funzione

$$\theta(k) = \sum_{n=0}^{n=p-1} B_n k^{p^n};$$

o anche da

$$\theta(a_0 + a_1 i + a_2 i^2 + \dots + a_{p-1} i^{p-1})$$

$$= \sum_{n=0}^{n=p-1} \left(m_0^{(n)} a_0 + m_1^{(n)} a_1 + m_2^{(n)} a_2 + \dots + m_{p-1}^{(n)} a_{p-1} \right) i^n$$

(v. n.° 29). Ora gl'indici che hanno un rapporto numerico appartengono a lettere congiunte (v. n.° 30); onde queste si potranno distinguere con un indice eguale al numero che esprime il rapporto che hanno, a una qualunque tra loro, che sarà intero e $< p$, ritenendo al solito eguali a zero i multipli di p ; i sistemi poi ai quali esse appartengono si potranno contrassegnare con un indice funzione del primitivo, che rimanga

lo stesso moltiplicando questo per un fattore numerico. Ciò si ottiene ponendo

$$x_{\frac{a_0+a_1 i+\dots+a_{v-1} i^{v-1}}{a_0}} = x_{\frac{a_1}{a_0} i + \frac{a_2}{a_0} i^2 + \dots + \frac{a_{v-1}}{a_0} i^{v-1}},$$

e meglio

$$x_{\frac{a_0+a_1 i+\dots+a_{v-1} i^{v-1}}{a_0}} = x_i, k_1 i + k_2 i^2 + \dots + k_{v-1} i^{v-1};$$

dove $k_n = \frac{a_n}{a_0}$ dovrà prendere i $p+1$ valori $0, 1, 2, \dots$

$p-1, \frac{1}{0}$; i poi prenderà i soli $1, 2, 3 \dots p-1$.

Questa mutazione d'indici trasforma la (f') nella seguente

$$(h) \left\{ \begin{array}{l} x_i, k_0 i + k_1 i^2 + \dots + k_{v-1} i^{v-1} \\ x_{\frac{n=v-1}{\lambda i, \sum_{n=1}^{n=v-1} \frac{m_0^{(n)} + m_1^{(n)} k_1 + m_2^{(n)} k_2 + \dots + m_{v-1}^{(n)} k_{v-1}}{m_0 + m_1 k_1 + m_2 k_2 + \dots + m_{v-1} k_{v-1}}} i^n} \end{array} \right\}$$

Chiamiamo *determinante della sostituzione* (h) , e indichiamo con D , la determinante del sistema dei v^2 numeri interi

$$m_0 \ m_1 \ m_2 \ \dots \ m_{v-1}$$

$$m'_0 \ m'_1 \ m'_2 \ \dots \ m'_{v-1}$$

$$m''_0 \ m''_1 \ m''_2 \ \dots \ m''_{v-1}$$

$$\dots \dots \dots \dots \dots$$

$$m^{(v-1)}_0 \ m^{(v-1)}_1 \ m^{(v-1)}_2 \ \dots \ m^{(v-1)}_{v-1}$$

Per moltiplicare la sostituzione (h) per un'altra (h') , la determinante D' della quale sia quella del sistema

$$\begin{array}{ccccccc} n_0 & n_1 & n_2 & \dots & n_{v-1} \\ n'_0 & n'_1 & n'_2 & \dots & n'_{v-1} \\ n''_0 & n''_1 & n''_2 & \dots & n''_{v-1} \\ \dots & \dots & \dots & \dots & \dots \\ n^{(v-1)}_0 & n^{(v-1)}_1 & n^{(v-1)}_2 & \dots & n^{(v-1)}_{v-1} \end{array}$$

basta porre in luogo di $k_1, k_2, \dots, k_{v-1}$ nella (h') i coefficienti delle corrispondenti potenze d' i della (h) . Quindi dal noto teorema della moltiplicazione delle determinanti è facile dedurre che, se si chiama Δ la determinante del prodotto delle due sostituzioni (h) e (h') , avremo

$$(i) \quad \Delta = DD';$$

cioè, la determinante del prodotto di due sostituzioni è eguale al prodotto delle loro determinanti.

Siano

$$(a) \quad \theta_{a_0} \theta_{a_1} \theta_{a_2} \dots \theta_{a_M}$$

tutte quante le sostituzioni comprese nella notazione (h) , la determinante delle quali è residuo quadratico di p . Poichè il prodotto di due residui è residuo, esse soddisfaranno la (15) del n.º 23, e formeranno un gruppo L . Se s'indica poi con θ_b una sostituzione qualunque compresa nella (h) , la determinante della quale è non residuo quadratico di p , avremo soddisfatta la (17) del n.º 23, che diviene

$$\theta_{a_n} \theta_b = \theta_b \theta_{a_m};$$

perchè, il primo prodotto avendo la determinante non residuo, dovrà averla non residuo anche il secondo, ed essendo non

residuo la determinante di θ_b , dovrà esser residuo quella di θ_a . Dunque se si chiama G_2 il gruppo delle θ_b avremo

$$\Gamma = LG_2.$$

Ma tutte le sostituzioni a determinante non residuo si ottengono facendo il prodotto di una sola o medesima a determinante non residuo con tutte quelle a determinante residuo; dunque G_2 è di 2° grado (v. n.° 23).

Ora se indichiamo con G il gruppo che si ottiene colle $p-1$ potenze della sostituzione

$$\left\{ \begin{array}{l} x_i, k_1 i + k_2 i^2 + \dots + k_{v-1} i^{v-1} \\ x_j, k_1 j + k_2 j^2 + \dots + k_{v-1} j^{v-1} \end{array} \right\}$$

nella quale λ è una radice primitiva di p ; e con G_1 il gruppo di tutte le sostituzioni che rimangono del gruppo L , tolti dalle medesime i fattori eguali a qualcuna delle sostituzioni di G , che saranno perciò

$$\left\{ \begin{array}{l} x_i, k_1 i + k_2 i^2 + \dots + k_{v-1} i^{v-1} \\ x_i, \sum \frac{m_i^{(n)} + m_i^{(n)} k_1 + \dots + m_i^{(n)} k_{v-1}}{m_0 + m_1 k_1 + \dots + m_{v-1} k_{v-1}} i^n \end{array} \right\}$$

è evidente che si avrà

$$L = GG_1,$$

$$\Gamma = GG_1 G_2.$$

G è di grado $(p-1)^{v-1}$ e decomponibile in gruppi di prima classe, G_2 di 2° grado, G_1 sarà di grado

$$\frac{(p^v - 1)(p^v - p)(p^v - p^2) \dots (p^v - p^{v-1})}{2(p-1)}.$$

Onde Γ sarà decomponibile in gruppi di prima classe soltanto quando lo sarà G_1 .

Questo avviene quando

$$1.^{\circ} \quad p=2, \quad v=2:$$

$$2.^{\circ} \quad p=3, \quad v=2:$$

nel 1.^o caso G_1 essendo di 3.^o grado, e quindi primo, nel 2.^o essendo un gruppo di 24 permutazioni su 4 lettere, che è decomponibile sempre in gruppi di prima classe, come si vede nell'esempio che abbiamo sviluppato qui appresso.

39.^o Quando un gruppo G ha le sostituzioni tutte comprese nel simbolo

$$(k) \quad \left\{ \begin{array}{l} x_k \\ x_{(Bk+C)^{p^v}} \end{array} \right\},$$

avremo sempre

$$G = \Gamma \Gamma_1 \Gamma_2;$$

essendo le sostituzioni di Γ date da

$$\begin{pmatrix} x_k \\ x_{k+c} \end{pmatrix},$$

o quindi

$$\Gamma = G_1 G_2 G_3 \dots G_v,$$

indicando con G_i il gruppo le sostituzioni del quale sono le p differenti potenze di

$$\begin{pmatrix} x_k \\ x_{k+i} \end{pmatrix}.$$

Le sostituzioni di Γ_1 poi saranno le $p^v - 1$ potenze differenti di

$$\begin{pmatrix} x_k \\ x_{Bk} \end{pmatrix};$$

dove B è una radice primitiva della (b) : e quelle di Γ_2 le v potenze di

$$\begin{pmatrix} x \\ x_p \end{pmatrix}$$

Dunque il gruppo G conterrà $p^2(p^2-1)p$ permutazioni (v. n.° 23), e sarà il prodotto di gruppi tutti di prima classe (vedi num. 35).

ESEMPPIO

Per indicare che le sostituzioni di un gruppo sono comprese in un dato simbolo, stabiliremo l'eguaglianza della lettera che indica il gruppo, col simbolo stesso.

Se

$$i^2 + i + 1 \equiv 0 \pmod{2},$$

le radici della congruenza

$$k^2 \equiv k \pmod{2}$$

saranno

$$k_0 \equiv 0 \quad k_1 \equiv i \quad k_2 \equiv i+1 \quad k_3 \equiv 1.$$

Il gruppo H che comprende tutte le 24 permutazioni che si possono fare con 4 lettere, sarà sempre decomponibile in gruppi di prima classe ; poichè le sue sostituzioni possono ottenersi tutte dalla (k) , e se

$$G = \begin{pmatrix} x_k \\ x_{k+k_1} \end{pmatrix}, \quad G_1 = \begin{pmatrix} x_k \\ x_{k+k_1} \end{pmatrix}$$

$$G_2 = \begin{pmatrix} x_k \\ x_{k+k_2} \end{pmatrix}, \quad G_3 = \begin{pmatrix} x_k \\ x_{k+k_3} \end{pmatrix}$$

sarà

$$H = GG_1G_2G_3 :$$

e avremo la seguente decomposizione, rappresentando le lettere cogli esponenti degli indici, e con zero x_{k_0} ,

(G ₃)	{	(G ₁)	(G)	{	0123	(G)	{	1032
			(G)	{	3210	(G)	{	2301
	{	(G ₁)	(G)	{	0231	(G)	{	1320
			(G)	{	3102	(G)	{	2013
	{	(G ₁)	(G)	{	0312	(G)	{	1203
			(G)	{	3021	(G)	{	2130
(G ₂)	{	(G ₁)	(G)	{	0213	(G)	{	1302
			(G)	{	3120	(G)	{	2031
	{	(G ₁)	(G)	{	0321	(G)	{	1230
			(G)	{	3012	(G)	{	2103
	{	(G ₁)	(G)	{	0132	(G)	{	1023
			(G)	{	3201	(G)	{	2310

PARTE SECONDA

CAPITOLO PRIMO

DELLE CONDIZIONI GENERALI DI RISOLUBILITÀ DELLE EQUAZIONI ALGEBRICHE PER RADICI DI EQUAZIONI AUSILIARIE.

I.

DELLA RISOLVENTE DI GALOIS.

1.° **E** noto che una funzione razionale delle radici di una equazione irriducibile di grado μ

$$(1) \quad f(x) = 0,$$

la quale prende, per qualunque sostituzione eseguita sulle radici, valori tutti differenti tra loro, gode la proprietà che le μ radici della (1) possono essere espresse razionalmente in funzione della medesima (*).

Siano

$$V = F(x_0, x_1, x_2, \dots, x_{\mu-1})$$

questa funzione, o

$$(2) \quad V_0, V_1, V_2, \dots, V_{M-1}$$

gli M valori che essa prende per tutte le diverse permutazioni delle radici: sarà

$$M = 1.2.3. \dots \mu - 1. \mu,$$

e potranno esprimersi tutti i valori (2) in funzione razionale di uno qualunque tra loro (**).

2.° Sia

$$(3) \quad \Theta(V) = 0$$

la equazione di grado M che ha per radici i valori (2), e che perciò avrà i coefficienti funzioni simmetriche delle radici, o quindi razionali dei coefficienti della (1). Questa equazione la quale ha alcune proprietà scoperte da Galois, che fanno il fondamento della presente Teoria, la chiameremo ad onore di questo profondo geometra la *risolvente di Galois*.

Indicheremo con

$$\varphi_0(V), \varphi_1(V), \varphi_2(V), \dots, \varphi_{\mu-1}(V)$$

le μ funzioni razionali di un valore qualunque di V , che danno le radici della (1).

3.° La Risolvente di Galois in generale sarà irriducibile, ma potrà decomporci in fattori irrazionali, cioè in fattori che contengono delle radici di equazioni algebriche ausiliarie. Queste radici, quando si stabilisca d'introdurle nel calcolo, come

(*) Vedi Serret. Cours. d'Alg. sup. pag. 140.

(**) V. lvi, pag. 152.

Siano aggiunte tali radici di equazioni ausiliarie che rendano la (3) riducibile; $\psi(V)$ sia uno dei fattori razionali della medesima di grado ν , e

le radici di

$$(5) \quad \psi(V) = 0.$$

$$(A) \left\{ \begin{array}{l} \varphi_0(V_0), \varphi_1(V_0), \varphi_2(V_0) \dots \varphi_{\mu-1}(V_0) \\ \varphi_0(V_1), \varphi_1(V_1), \varphi_2(V_1) \dots \varphi_{\mu-1}(V_1) \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ \varphi_0(V_{r-1}), \varphi_1(V_{r-1}), \varphi_2(V_{r-1}) \dots \varphi_{\mu-1}(V_{r-1}) \end{array} \right.$$

Ora sappiamo che

$$V_m = \lambda(V_a) ,$$

$$(6) \quad V_n, \lambda(V_n), \lambda^2(V_n), \dots, \lambda^{F-1}(V_n),$$

essendo p il più piccol numero per cui

(*) Vedei Serret Cours-d'Alg. Sup. pag. 345.

$$\lambda^p(V_n) = V_n :$$

e se la serie dei valori (6) non esaurisce la (4), saranno $\mu(V_n)$, $\mu_1(V_n)$, $\mu_2(V_n)$. . . altre funzioni razionali che daranno altrettante radici,

$$(7) \quad \left\{ \begin{array}{l} \mu(V_n), \mu\lambda(V_n), \mu\lambda^2(V_n) \dots \mu\lambda^{p-1}(V_n) \\ \mu_1(V_n), \mu_1\lambda(V_n), \mu_1\lambda^2(V_n) \dots \mu_1\lambda^{p-1}(V_n) \\ \dots \dots \dots \dots \dots \dots \dots \end{array} \right.$$

Ora cangiando V_n in V_m , ossia V_n in $\lambda(V_n)$, si permutano circolarmente in tutti i loro termini ciascuna delle linee orizzontali di valori (6) e (7), ossia si permutano tra loro tutti i valori (4); dunque eseguendo su tutte le (A) una sostituzione qualunque che faccia passare da una ad un'altra delle medesime, esse si permutano tutte quante tra loro, senza che nasca nessuna nuova permutazione; dunque le ν permutazioni (A) costituiscono un gruppo.

Questo gruppo lo chiameremo *gruppo della equazione ridotto dalle quantità che si sono aggiunte*.

Se non si fosse aggiunta nessuna quantità irrazionale il grado del gruppo della equazione in generale sarebbe stato M.

5.° Tutte le funzioni razionali delle radici della (1) invariabili per tutte le sostituzioni del gruppo (A), sono esprimibili razionalmente per i coefficienti della (1) e per le quantità aggiunte dalle quali è stato ridotto.

Esprimendo tutte le radici della (1) per uno qualunque V_0 dei valori (4), una funzione razionale qualunque delle radici sarà eguale a una funzione razionale di V_0 .

$$\chi(V_0).$$

Se essa è invariabile per tutte le sostituzioni del gruppo (A), equivalendo queste alle permutazioni dei valori (4) tra loro, avremo

$$\chi(V_0) = \chi(V_1) = \chi(V_2) = \dots = \chi(V_{v-1}),$$

e quindi

$$\chi(V_0) = \frac{1}{v} (\chi(V_0) + \chi(V_1) + \dots + \chi(V_{v-1})).$$

Dunque una funzione razionale qualunque delle radici della (1), che sia invariabile per le sostituzioni del gruppo (A), sarà simmetrica delle radici della (5), e perciò esprimibile razionalmente per i coefficienti della (5), ossia di quelli della (1) e delle quantità aggiunte.

Una funzione razionale delle radici e irrazionale dei coefficienti e delle quantità aggiunte dovrà esser variabile per alcune delle sostituzioni del gruppo.

6.° Se una funzione razionale delle radici, e invariabile per alcune sostituzioni soltanto, è esprimibile razionalmente per i coefficienti e per alcune quantità aggiunte, il gruppo ridotto non conterrà nessuna sostituzione per la quale essa non sia invariabile.

Sia

$$(8) \quad \psi(V_0) = B;$$

e il primo membro una funzione razionale delle radici della (1), il secondo dei coefficienti e delle quantità aggiunte. Poichè la (5) è irriducibile, e la (8) ha i coefficienti razionali di quelli della (5), ed è soddisfatta da una radice della medesima, dovrà esserlo anche da tutte le altre. Dunque sostituendovi a V_0 qualunque altro valore (4), ossia facendo qualunque sostituzione del gruppo (A) sulle radici della (1), rimarrà invariabile; come volevamo dimostrare.

7.° Allorchè una funzione razionale delle radici variabile per ogni sostituzione che muta il posto di alcune soltanto di esse, è cognita razionalmente; il gruppo non può contenere sostituzioni che sull'altre radici; o quelle essendo invariabili per tutte le sostituzioni del gruppo saranno cognite razionalmente, e la equazione non sarà irriducibile.

Da ciò ne segue che le sostituzioni del gruppo di una equa-

zione irriducibile non potranno mai esser in numero minore del grado della equazione stessa.

8.° Quando la Risolvente di Galois si decompone in fattori, ciascuno dei quali è razionale dei coefficienti e di una sola delle radici

$$(9) \quad r_0, r_1, r_2, \dots, r_{n-1}$$

di una equazione ausiliare irriducibile di grado n .

$$(10) \quad \varphi(r) = 0;$$

il gruppo della proposta si divide in n gruppi derivati simili, e ciascuno di questi diviene gruppo della equazione quando si aggiunga una sola delle (9); e il gruppo della (10) è simile a quello della proposta.

I fattori della risolvente (3) dovranno esser n , e differenti tra loro soltanto per i valori di r ; perchè altrimenti $\Theta(V)$ razionale dei coefficienti della (10) o non sarebbe invariabile per alcuna sostituzione sopra le r , e unicamente per quelle che mutano il posto di alcune soltanto di esse, e quindi la (10) (V. n.° 7) non sarebbe irriducibile. Pertanto potremo porre

$$\Theta(V) = \theta(V, r_0) \theta(V, r_1) \dots \theta(V, r_{n-1}).$$

Questi fattori saranno in V di grado

$$m = \frac{v}{n},$$

e posti a zero daranno tutte le radici della (3).

Siano

$$(11) \quad V_0, V_1, V_2, \dots, V_{m-1},$$

le radici di una qualunque delle equazioni che ne nascono

$$(12) \quad \theta(V, r_i) = 0.$$

Se si aggiunga la sola radice r_i , il gruppo della proposta sarà

$\{A_i\}$

Se Y_0 , o $F(Y_0)$ sono due radici della (12), si avrà

$$(13) \quad \theta(V_{o,t}, r_t) = 0, \theta(F(V_{o,t}), r_t) = 0 :$$

o poichè la 1.^a è irriducibile, e la 2.^a razionale delle quantità che entrano nei coefficienti della 1.^a, sarà il resto della divisione della 2.^a per la 1.^a

$$(14) \quad \bar{\omega}(r_i) = 0.$$

Questa che ha tutti i suoi coefficienti razionali, e ammette una radice della (10) che è irriducibile, dovrà ammettere anche tutte le altre. Perciò essendo r_i un'altra qualunque delle (9) si avrà

$$\hat{\omega}(r_i) = 0, \quad \text{с} \quad \theta(F(V_{s_i, i}), r_i)$$

divisibile per

$$\mathcal{O}(V_{\alpha, i'}, r_{i'}) .$$

Da ciò ne segue che, essendo le radici di un fattore (12) date da certe funzioni razionali di una tra loro, anche quello di un altro fattore qualunque saranno date dalle stesse funzioni di una tra loro. Dunque, cangiando uno dei valori V_{σ_i} , che entrano in un gruppo (A_i) , in uno $V_{\sigma_i'}$, di un altro gruppo $(A_{i'})$, tutte le permutazioni di (A_i) si cangiano rispettiva-

mente in quelle di (A_i) : e poichè il cangiamento di un valore V , in un altro, corrisponde a una sostituzione sulle radici della (1), una sola e medesima sostituzione converte tutte le permutazioni di un gruppo in quelle di un altro, e i gruppi $(A_0), (A_1), \dots, (A_{n-1})$ sono derivati uno dall'altro.

Poichè un gruppo A_i appartiene alla equazione quando è aggiunta una sola delle (9) r_i , e tutte le altre (9) rimangono irrazionali; ciascuna di esse espressa razionalmente per le radici della proposta dovrà risultare invariabile per le sostituzioni del gruppo corrispondente e variabile per quelle di tutti gli altri: dunque il gruppo della equazione (10) dovrà essere eguale a quello delle permutazioni sopra i derivati, e simile a quello della proposta (v. n.º 20. Parte I).

9.º *Se la risolvente può decomorsi in più fattori razionali dei coefficienti della proposta, e di tutte le radici*

$$(15) \quad r_0, r_1, r_2, \dots, r_{n-1}$$

di una equazione ausiliaria irriducibile

$$(16) \quad \varphi(r) = 0;$$

il gruppo deve essere il prodotto di due altri; il primo dei quali è il gruppo della equazione stessa quando siano aggiunte tutte le (15); il secondo è simile al gruppo dell'ausiliaria (16).

Sia

$$\Theta(V) = \theta_0(V, r_0, r_1, \dots, r_{n-1}) \theta_1(V, r_0, r_1, \dots, r_{n-1}) \dots \theta_{n-1}(V, r_0, r_1, \dots, r_{n-1}).$$

Poichè la risolvente ha i coefficienti razionali delle quantità che entrano in quelli della (16), dovrà essere invariabile per le sostituzioni del gruppo di queste, e quindi i fattori θ_i non dovranno differire che per l'ordine nel quale sono disposte le (15) ed esser tanti quante sono le permutazioni del gruppo della (16). Indicando, come nel caso precedente, con

$$(17) \quad V_{0,1}, V_{1,1}, V_{2,1}, \dots, V_{m-1,1}$$

le m radici del fattore irriducibile di grado $m = \frac{v}{n}$

$$(18) \quad \theta_i(V, r_0, r_1, r_2, \dots, r_{n-1}) = 0,$$

si dimostrerà ugualmente che tutti i gruppi (A_0) (A_1) ... (A_{n-1}) ottenuti dando a i tutti i valori interi da zero a $n-1$, e che appartengono alla equazione quando si aggiungano tutte le radici (15), sono derivati uno dell'altro.

Se una radice $V_{a,i}$ di un fattore (18) è data in funzione razionale di una radice $V_{a,i'}$ di un altro, per mezzo della equazione

$$V_{a,i'} = \psi(V_{a,i});$$

si avrà

$$\theta_i(V_{a,i}) = 0, \quad \theta_{i'}(\psi(V_{a,i})) = 0;$$

e poichè la prima è irriducibile, e ambedue sono razionali delle stesse quantità, le radici della prima saranno tutte radici anche dell'altra, e se queste sono

$$V_{0,i}, F_1(V_{0,i}), F_2(V_{0,i}), \dots, F_{n-1}(V_{0,i})$$

saranno radici della $\theta_{i'} = 0$

$$\psi(V_{0,i}), \psi F_1(V_{0,i}), \psi F_2(V_{0,i}), \dots, \psi F_{n-1}(V_{0,i}).$$

Onde si passerà dall'una all'altra permutazione del gruppo $(A_{i'})$ facendo li stessi cangiamenti dello $V_{a,i}$ l'una nell'altra, come per passar da una permutazione all'altra di (A_i) : dunque i gruppi derivati in questo caso sono tutti eguali, o il gruppo dell'ausiliaria che definisce lo quantità aggiunto che sono invariabili per le sole sostituzioni dei gruppi (A_i) , è simile a quello per il quale bisogna moltiplicare uno dei derivati per ottenere il gruppo stesso che appartiene alla proposta quando non siano aggiunto le (15) (v. P. I. n.° 21); come volevamo dimostrare.

10.° Se si aggiunga a una equazione una funzione U razionale delle radici, la quale prenda per tutte le sostituzioni del primo divisore del gruppo altrettanti valori differenti, e sia invariabile per le sostituzioni dell'altro fattore, il gruppo della equazione diverrà il solo fattore per le sostituzioni del quale la U è invariabile.

Poichè ogni funzione aggiunta diviene razionale, e perciò invariabile per tutte le sostituzioni del gruppo, il quale non potrà più contenere le sostituzioni per le quali essa è variabile (*).

11.° Se il gruppo è primo, non si potrà ridurre altro che aggiungendo una funzione variabile per tutte le sostituzioni del gruppo, con che il gruppo non conterrà più nessuna sostituzione, ossia una permutazione soltanto; perchè se si prenda una funzione U simmetrica dei valori, che riceve una funzione delle radici, per le sostituzioni di uno G dei derivati dei quali è somma il gruppo proposto, essa non sarà che apparentemente invariabile per queste sostituzioni; perchè eseguita una che lo converta in un altro derivato, diviene variabile anche per le sostituzioni di G . Dunque se una equazione ha un gruppo primo, non esistono funzioni delle radici che aggiunte lo riducano, tranne quelle che lo riducono a una sola permutazione.

12.° Il gruppo di una equazione, finchè non sia aggiunta una irrazionale che non si trovi già nei coefficienti, sarà in generale di grado $1. 2. 3 \dots \mu-1. \mu$; perchè le sole funzioni simmetriche sono sempre cognite razionalmente senza l'aggiunta di nessuna quantità. Se il gruppo sarà di grado minore, dovranno esistere delle relazioni particolari tra le radici, che rendano impossibili le sostituzioni che non compariscono nel gruppo. Infatti, si aggiunga una funzione delle radici variabile per tutte le sostituzioni del gruppo, o invariabile per qualunque altra, e precisamente di queste una U che contenga il minimo numero di radici; il gruppo non conterrà più nessuna sostituzione, e quindi ogni funzione delle radici, e le radici stesse risulteranno razionalmente cognite; e si potranno tutte esprimere per U e per i coefficienti:

$$x_0 = F_0(U), \quad x_1 = F_1(U), \quad x_2 = F_2(U) \dots x_{\mu-1} = F_{\mu-1}(U).$$

Ora eseguendo in questo sistema di equazioni una sostituzione

(*) Per conoscere come di fatto avviene che aggiunta una sola funzione delle radici, rimangono aggiunte tutte quelle che le son simili, e quindi anche quelle che riducono la risolvente e il gruppo, vedasi la Lez. XI dell'Algebra superiore di Serret.

qualunque che non appartenga al gruppo, i secondi membri rimarrebbero fermi, e i primi si permuterebbero tra loro; ciò che è impossibile, perchè la equazione essendo irriducibile le radici sono tutte differenti tra loro. Perciò le sostituzioni del gruppo di una equazione alla quale non è aggiunta nessuna irrazionale, le chiameremo *possibili*, e le altre *impossibili*.

Così se sulle radici di una equazione non sono possibili altre sostituzioni che quelle le quali non lasciano nessuna lettera allo stesso posto; per U potrà prendersi una radice qualunque, poichè essa sarà variabile per tutte le sostituzioni del gruppo, e invariabile per tutte le altre: quindi tutte le radici saranno funzioni razionali di una qualunque tra loro. Se non sono possibili altro che quelle che non lasciano più di due lettere allo stesso posto, si può prendere per U una funzione non simmetrica di due radici qualunque: e perciò tutte quante sono funzioni razionali di due qualunque tra loro.

13.° Reciprocamente quando esistono delle relazioni razionali tra le radici, il gruppo non contiene altre sostituzioni che quelle *possibili* nel sistema di equazioni che dà quelle relazioni, o, ciò che è lo stesso, in quello che se ne può dedurre per esprimere tutte le radici razionalmente per il minimo numero di esse. Infatti, aggiunte queste, le radici sono tutte cognite razionalmente, e il gruppo non contiene più nessuna sostituzione; dunque quelle per le quali le radici aggiunte sono invariabili, che sono le impossibili nel sistema, non le poteva contenere avanti la loro aggiunzione.

Così quando le radici sono tutte funzioni razionali di una qualunque tra loro, è evidente che, cangiata una, si debbono cangiar tutte le altre che ne sono funzioni razionali, e non son possibili altre sostituzioni che quelle che non lasciano ferma nessuna lettera: e queste sono le uniche che appartengono al gruppo.

Puiseux in questi ultimi tempi ha determinato le sostituzioni che si operano sulle radici quando si faccia percorrere con continuità una serie di valori immaginari, sì che non si torni a quello da cui siamo partiti, a una quantità della quale sono

funzioni razionali i coefficienti (*). *Hermite* ha dimostrato che queste sostituzioni sono quelle stesse del gruppo della equazione (**). Le considerazioni precedenti spiegano facilmente questa rimarchevole coincidenza.

II.

DELLA RISOLUZIONE DELLE EQUAZIONI.

14.° *Risolvere una equazione algebrica significa renderne razionali le radici coll'aggiunzione di radici di equazioni ausiliarie.*

Affinchè una equazione sia risolta è necessario e sufficiente che il suo gruppo non contenga più nessuna sostituzione: perchè ogni funzione anche variabile per qualunque sostituzione deve essere razionalmente cognita quando una equazione è risolta, e reciprocamente, se il gruppo è ridotto a non contenere più nessuna sostituzione, tutte le radici sono cognite razionalmente.

Bisogna qui distinguere due casi: o non esistono equazioni ausiliario di gruppo inferiore per le radici delle quali siano esprimibili razionalmente quello della proposta; e la operazione mediante la quale coll'aggiunzione di radici di equazione di gruppo simile si riduce il gruppo della proposta a non contenere nessuna sostituzione, la diremo *trasformazione della equazione*, o *risoluzione impropria*, e le radici di queste equazioni le diremo *irrazionali primitivi*; o esisteranno equazioni di gruppo inferiore, per le radici delle quali possano darsi razionalmente quello della proposta, e allora la equazione si dirà *risolubile propriamente*.

Il primo caso ha luogo quando il gruppo è primo: il secondo quando è il prodotto di più gruppi primi.

15.° I. Caso. Noi qui toccheremo soltanto la Teoria delle trasformazioni delle equazioni in quanto è necessario per i problemi relativi alla risoluzione propria che ci siamo proposti in

30 65 52

(*) V. Journal de Liouville T. XV.

(**) V. Comptes Rendus. Avril 1831.

questa Memoria. Gl'irrazionali primitivi, di gruppo simile che possono esprimersi razionalmente gli uni per gli altri potranno essere definiti da equazioni irriducibili di gradi differenti, o anche di grado eguale, e di maggiore o minore semplicità relativamente all'applicazione dei metodi di risoluzione numerica: noi però non ci fermeremo su queste distinzioni: e li terremo tutti della stessa classe. Osserveremo soltanto che da quanto abbiain detto al numero 11, si deduce facilmente il seguente teorema: *affinche una equazione irriducibile sia impropriamente risolubile per radici di equazioni di grado inferiore è necessario e sufficiente che il suo gruppo sia decomponibile in un numero di derivati simili minore del suo grado.*

Gl'irrazionali primitivi di gruppi non simili li distingueremo in classi corrispondenti alle classi dei loro gruppi.

16.º *Gl'irrazionali primitivi di prima classe, il gruppo dei quali è di grado primo, sono tutti esprimibili razionalmente per soli radicali.*

Il Gruppo della equazione che li definisce non contiene che le potenze di una sola sostituzione di ordine eguale al numero delle radici (v. P. I. n.º 16), e circolare sopra tutte le medesime (v. P. I. n.º 7. 4.): quindi distinguendo le radici con apici numerici, poichè il loro numero è primo (v. P. I. n.º 2), le sostituzioni del gruppo saranno soltanto le potenze di

$$(19) \quad \begin{pmatrix} x_1 \\ x_{i+1} \end{pmatrix}.$$

Costruiamo la funzione

$$U = (x_0 + \alpha x_1 + \alpha^2 x_2 + \dots + \alpha^{u-1} x_{u-1})^u,$$

dove

$$\alpha^{u-1} + \alpha^{u-2} + \dots + \alpha^2 + \alpha + 1 = 0.$$

U è invariabile per tutte le sostituzioni del gruppo (*), e perciò razionalmente cognita. Il radicale $\sqrt[u]{U}$ espresso per le ra-

(*) V. Serret. Cours d'Alg. sup. pag. 358.

Annali di Scienze Mat. e Fis. T. II. marzo 1852.

dici è variabile per tutte le potenze della (19) : dunque aggiunto ridurrà il gruppo a non contenere più alcuna sostituzione, e gl' irrazionali primitivi x risulteranno razionalmente

espressi per $\sqrt[p]{U}$, e per α , che è esprimibile per radicali, come dimostrò Gauss per il primo. (*).

17.° Tutti gl'irrazionali primitivi esprimibili per soli radicali sono di prima classe.

Aggiunte le radici p^{esime} immaginarie della unità, una equazione binomia di grado p ha tutte le sue radici funzioni razionali di una qualunque tra loro : talchè queste non si possono che aggiunger tutte insieme : e quindi il gruppo di una equazione o non è riducibile per questa aggiunta, oppure è il prodotto di un gruppo che potrà essere anche di primo grado, per un altro di grado p (v. n.° 8); dunque gl' irrazionali esprimibili per soli radicali o non sono primitivi, o sono di prima classe.

La determinazione degl'irrazionali, per i quali converrà di esprimere gl' irrazionali primitivi di classi superiori, sarà un'applicazione delle proprietà dei gruppi delle classi corrispondenti.

18.° Il. Caso. Una equazione, il gruppo della quale è il prodotto di più gruppi primi, è risolubile per irrazionali primitivi, i gruppi dei quali sono rispettivamente simili ai divisori del gruppo della proposta : e viceversa.

Sia il gruppo della proposta

$$H = \Gamma' \Gamma'' \dots \Gamma^{(i)}$$

e $\Gamma' \Gamma'' \dots \Gamma^{(i)}$ siano tutti primi. Decomponiamo il primo gruppo $\Gamma^{(i)}$ in un numero p di derivati simili (v. P. I. num. 23. 2.), e costruiamo una funzione θ delle radici, invariabile per tutte le sostituzioni degli altri gruppi $\Gamma' \Gamma'' \dots$ e per quelle

(*) V. Gauss. Disquisitiones Arithmeticae, ovvero Serret. Cours d'Alg. Sup. pag. 373.

di uno dei derivati dei quali è somma $\Gamma^{(i)}$. La funzione θ avrà p valori che saranno dati da una equazione di grado p , e di gruppo simile a $\Gamma^{(i)}$ (v. n.° 8). Aggiunte tutte le p radici di questa equazione, saranno cognite razionalmente delle funzioni variabili per le sostituzioni di $\Gamma^{(i)}$, e perciò il gruppo della proposta si ridurrà al solo prodotto degli altri. Coll'aggiunta d'irrazionali primitivi analogamente costruiti e di gruppi simili a $\Gamma^{(i-1)}$, $\Gamma^{(i-2)}$, . . . , si potrà ridurre successivamente il gruppo a contenere quanti divisori di meno si vuole, e quindi a non contenere più nessuna sostituzione, e così otterremo la risoluzione completa della equazione.

La proposizione inversa è una conseguenza immediata di ciò che si è stabilito al n. 9.

Dal Teorema precedente se ne deducono immediatamente i seguenti corollarj.

1. *Affinchè una equazione irriducibile sia risolubile per irrazionali primitivi di classi determinate, è necessario e sufficiente, che il suo gruppo sia il prodotto di gruppi di classi eguali a quelle degl'irrazionali medesimi.*

2. *Affinchè una equazione sia risolubile per radicali è necessario e sufficiente che il suo gruppo sia il prodotto di gruppi tutti di prima classe.*

3. *Il prodotto dei gradi dei gruppi delle equazioni che definiscono gl'irrazionali primitivi per i quali una equazione irriducibile è risolubile, è eguale almeno al grado del gruppo di questa medesima.*

4. *Il prodotto degl'indici dei radicali per i quali è risolubile una equazione è eguale almeno al grado della medesima, se è irriducibile.*

19.° *Il grado dell'ultimo divisore del gruppo di una equazione, o è eguale al grado della equazione, o n'è un divisore.*

L'aggiunzione dell'irrazionale U variabile per le μ sostituzioni di questo divisore rende razionali le radici, e quindi decompone la equazione in μ fattori tutti di primo grado. L'aggiunta degli altri irrazionali poteva aver già decomposta la

equazione in fattori tutti di grado eguale tra loro, e quindi μ deve essere o eguale al grado, o a un divisore del medesimo; e qui, ragionando come per istabilire il numero dei fattori nei quali si decompone la risolvente, ai n.º 8 e 9, si dimostra che μ è eguale o al grado della equazione irriduttibile che dà U , o al gruppo; e quindi a un multiplo del grado della medesima; con che rimane provato ciò che volevamo.

Da ciò che precede derivano i corollarj seguenti:

1. *Una equazione irriduttibile di grado primo non può risolversi senza irrazionali di grado eguale al proprio.*

2.º *Una equazione irriduttibile di grado qualunque non può risolversi senza irrazionali di grado divisore del proprio.*

3. *Gli irrazionali primitivi esterni nella espressione delle radici, cioè quelli che non compariscono nei coefficienti di nessuna delle ausiliarie o sono dati da equazioni di grado eguale a quello della proposta, o a un divisore del medesimo: teorema già dimostrato da Malmsten per il caso particolare dei radicali (*).*

CAPITOLO SECONDO

DELLA RISOLUBILITÀ DELLE EQUAZIONI PER RADICALI.

I.

DELLE RISOLVENTI LAGRANGIANE.

20.º Non sempre sono dato immediatamente le relazioni razionali che passano tra le diverse radici di una equazione irriduttibile da risolversi, e quindi non sempre se ne conoscono i loro gruppi direttamente, come nelle equazioni che danno la divisione delle funzioni circolari ed ellittiche. Perciò non basta conoscere le condizioni da verificarsi sui gruppi di risolubilità per radicali; ma è necessario di trasformar quello in altre facili a verificarsi direttamente sui coefficienti. Galois ebbe

(*) Crelle, Journal für die Mathematik. B. 34. In solutionem aequationum algebraicarum disquisitio: auct. Malmsten.

in vista più specialmente le condizioni relative ai gruppi, Abel ai coefficienti. Io ho sviluppato prima quelle, e poi le ho trasformate in questo.

La determinazione in particolare della natura dei gruppi di tutte le equazioni risolubili per radicali, consisterà nella ricerca del massimo moltiplicatore decomponibile in divisori di prima classe, dell'ultimo gruppo che dev'esser pure di prima classe, e di grado eguale a quello della equazione o a un divisore del medesimo (v. n.° 18° 2 e 19°).

21.° Passiamo ora a determinare come si possano coi coefficienti costruire alcuni risolvendi che abbiano proprietà particolari meno difficili a verificarsi di quelle della risolvende generale di Galois, quando appartengono a equazioni risolubili per radicali.

Abbiamo già veduto che il gruppo di queste equazioni è il prodotto di più gruppi di prima classe. Sia H il gruppo totale, e $G, G', G'', \dots G^{(\mu)}$ i suoi divisori rispettivamente di grado $\mu, \mu', \mu'' \dots \mu^{(\mu)}$, dove μ è eguale al grado n della equazione, o a un divisore del medesimo, e tutti sono numeri primi.

L'ultimo radicale da aggiungersi dovrà esser variabile per le sostituzioni dell'ultimo divisore G (v. n.° 19), e quindi per le sostituzioni circolari su tutte quante le radici se μ è primo, e se no, per il prodotto di più sostituzioni circolari su μ radici ciascuna: dovrà inoltre esser radice di una equazione binomia; la quale abbia il termine noto R razionale, allorchè siano state aggiunte altre funzioni variabili per le sostituzioni di tutti gli altri divisori, e quindi invariabile per le sostituzioni circolari sopra μ radici: dunque potrà sempre prendersi

per ultimo radicale da aggiungersi $\sqrt[\mu]{R}$, essendo μ un divisore del grado; e R la nota espressione di Lagrange

$$R = \left\{ \sum_{i=0}^{i=n-1} \alpha^i x_i \right\}^{\mu}$$

dove α è dato dalla equazione

$$\sum_{r=0}^{r=\mu-1} \alpha^r = 0.$$

I gradi $\mu', \mu'', \dots \mu^{(v)}$ degli altri divisori di H sono tutti $< n$, perchè il numero delle permutazioni di un gruppo non può contenere fattori primi maggiori del numero delle lettere; dunque si potrà prendere un gruppo prodotto dei divisori di H

$$\Gamma = G' G'' \dots G^{(v)},$$

il grado del quale sia

$$\delta = \mu' \mu'' \dots \mu^{(v)} < n.$$

Eseguiamo sulle x_i contenute in R tutte le sostituzioni di Γ , avremo δ valori per R . Costruiamo la equazione di grado δ che li ha per radici. Per averne i coefficienti basta determinare una sola funzione F simmetrica dei δ valori delle R ; poichè la nota teorica delle funzioni simili ci dà il modo di esprimere quelli in funzione razionale di questa. Eseguendo quante e quali si vogliono sostituzioni sulle x_i contenute nella F , si avranno altrettanti valori che tutti saranno radici di una equazione in generale di grado molto elevato a coefficienti razionali, e che potrà chiamarsi *Risolvente Lagrangiana* dal sommo geometra che la usò il primo. Poichè ogni funzione simmetrica dei valori che prende F per le δ' sostituzioni di Γ' , sono razionali se

$$\Gamma' = G^{(l+1)} G^{(l+2)} \dots G^{(v)},$$

e in conseguenza

$$\delta' = \mu^{(l+1)} \mu^{(l+2)} \dots \mu^{(v)};$$

la *Risolvente Lagrangiana* dovrà esser riduttibile, e avere un fattore razionale di grado δ' . Se non è $\delta' < n$, operando sopra questo fattore posto a zero, il gruppo del quale è Γ' , come abbiamo operato sulla proposta, si farà dipendere da una di grado $< n$, e da un'altra che sarà di grado $< \delta'$, e così

seguitando si avranno tante equazioni tutte di grado minore della proposta, dalla risoluzione delle quali dipenderà la risoluzione di questa. I gruppi di tutte le risolventi sono tutti evidentemente i successivi divisori di H ; dunque esse saranno risolubili per radicali quando è la proposta.

L'applicazione diretta e generale di questo metodo suppone la cognizione precedente del gruppo della equazione da risolvere. Ma vedremo come anche senza conoscere il gruppo, essendo dati soltanto i coefficienti della equazione esistono certi modi di applicarlo, differenti secondo la natura del numero al quale è eguale il grado della equazione, tali che se con essi non si può ottenere la risoluzione voluta, possiamo esser certi che essa è impossibile. Questi modi sono quelli stessi proposti da *Lagrange*. L'*Abel* aveva veduto questo pregio del metodo inventato da quel sommo Geometra, e i Teoremi annunziati nel frammento della sua Memoria postuma *Sur la resolution algebrique des equations* sono diretti tutti a dimostrarlo.

22.° La Risolvente Lagrangiana in tutti i casi, tranne alcuni nei quali il grado è potenza di un numero primo, deve sempre avere un fattore razionale di primo grado. È curioso di conoscere se, tolto questo fattore, è ulteriormente riduttibile, e se lo è, di determinare il grado e la natura dei fattori razionali che la dividono. Io ho trovato un metodo generale per risolvere questo problema, e qui passo ad esporlo.

La radice U della Risolvente Lagrangiana, data dal fattore razionale di primo grado, è invariabile per tutte le sostituzioni del gruppo H della equazione. Le altre radici sono tutti i valori che prende U per tutte le sostituzioni che non appartengono a H . Deriviamo H per mezzo di una di queste φ , e poi il gruppo derivato deriviamolo successivamente per tutte le sostituzioni $\theta_0, \theta_1, \theta_2, \dots, \theta_{n-2}$ di H ; le funzioni invariabili rispettivamente per tutte le sostituzioni di questi derivati

$$(20) \quad D_{\varphi}H, D_{\varphi\theta_0}H, D_{\varphi\theta_1}H, D_{\varphi\theta_2}H, \dots, D_{\varphi\theta_{n-2}}H$$

saranno altrettante radici della risolvente, che indicheremo con le lettere

$$(21) \quad R_0, R_1, R_2, \dots, R_{n-1}.$$

Alcune di queste potranno anche essere eguali tra loro; ma ancorchè siano tutte differenti le sostituzioni di H non saranno che permutarlo una nell'altra; dunque le funzioni simmetriche delle medesime saranno invariabili per le sostituzioni di H e quindi razionali; onde la risolvente Lagrangiana se avrà un fattore di grado primo ammetterà anche più fattori razionali di grado non superiore al grado del gruppo della equazione, quando questa sia risolubile per radicali.

Poichè il gruppo di una equazione non contiene altre sostituzioni che quelle per le quali è invariabile una funzione delle radici razionalmente esprimibile per i coefficienti (v. n. 6); il gruppo della equazione che ha per radici le (21) sarà eguale a H : dunque i fattori razionali nei quali è riducibile la risolvente Lagrangiana sono tutti risolubili per radicali, se lo è la proposta.

Affinchè alcune delle (21) siano eguali tra loro, e che il grado del fattore razionale sia perciò minore del grado del gruppo H , è necessario che alcuni dei (20) siano eguali, ossia per alcuni valori di m e m_1

$$(22) \quad D_{\bar{r}^m} H = D_{\bar{r}^{m_1}} H;$$

e quindi

$$\theta_a \varphi_{m_1} = \theta_{a_1} \varphi_m,$$

o moltiplicando a destra per θ_a a sinistra per θ_{μ} essendo

$$\theta_a \theta_{a_1} = 1 \quad \theta_{m_1} \theta_{\mu} = 1.$$

e

$$\theta_a \theta_a = \theta_b, \quad \theta_{m_1} \theta_{\mu} = \theta_c;$$

si ottiene

$$(23) \quad \theta_b \bar{r} = \varphi \theta_c;$$

dunque φ dovrà essere φ una sostituzione di un moltiplicatore di alcuno dei divisori di II. Questo poi è sufficiente, perchè con un processo inverso dalla (23) si può facilmente dedurre la (22). Dunque il numero dei fattori razionali della risolvante Lagrangiana di grado α (e α sarà sempre un divisore del grado n del gruppo della equazione) è eguale al numero delle sostituzioni dei massimi moltiplicatori dei gruppi di grado $\frac{n}{\alpha}$ divisori del gruppo II della proposta.

II.

DELLA RISOLUBILITA' PER RADICALI DELLE EQUAZIONI DI GRADO PRIMO.

23°. Affinchè una equazione irriducibile di grado primo sia risolvibile per radicali, è necessario e sufficiente che il suo gruppo non ammetta altre sostituzioni che quelle comprese nel simbolo

$$(24) \quad \left(\begin{matrix} x_1 \\ x_{ai+b} \end{matrix} \right),$$

e che in conseguenza tutte le sue radici siano funzioni razionali di due qualunque tra loro.

L'ultimo divisore del gruppo di una equazione di grado primo risolubile per radicali non ha altre sostituzioni che le potenze di

$$(25) \quad \left(\begin{matrix} x_1 \\ x_{1+i} \end{matrix} \right)$$

(v. n.° 19): il suo massimo moltiplicatore contiene solo le potenze di

$$(26) \quad \left(\begin{matrix} x_1 \\ x_{1/p} \end{matrix} \right),$$

dove p è radice primitiva del grado (v. P. I. n. 24); e quindi ha tutti i divisori di prima classe (v. P. I. num. 35); dunque è necessario e sufficiente che tutte le sostituzioni del gruppo siano i prodotti delle differenti potenze della (25) con quelle della (26), cioè le sostituzioni comprese nel simbolo (24).

Le (24) non possono dare due permutazioni che abbiano più

di una lettera allo stesso posto (*): dunque tutte le radici debbono esser funzioni razionali di due qualunque tra loro (v. n.° 12); e questo è sufficiente, come già dimostrai in una mia Nota sulla risolubilità per radicali delle equazioni di grado primo (**): e come si deduce facilmente dal num.° 13. Le (24) dando non più di $\mu(\mu-1)$ permutazioni, e per il numero 3 solo avendosi $1. 2. \dots \mu = p(\mu-1)$, tutte le equazioni di grado primo superiore a 3 non sono in generale risolubili per radicali.

24.° Affinchè una equazione di grado μ primo sia risolubile per radicali è necessario e sufficiente che la risolvente Lagrangiana ammetta un fattore razionale di primo grado.

Le radici della risolvente Lagrangiana sono in questo caso

$$\sum_{h=1}^{h=\mu-1} \left(\sum_{i=0}^{i=\mu-1} x^i x_{i\rho^h} \right)^\mu,$$

dove

$$\sum_{m=0}^{m=\mu-1} \alpha^m = 0.$$

e ρ radice primitiva di μ (***). Questa funzione è evidentemente invariabile per tutte le sostituzioni (25) o (26) del gruppo (****): dunque la risolvente ha una radice razionale; e questo basta perchè col metodo di Lagrange si possano ottenere tutte le radici espresse per radicali.

Passiamo a determinare gli altri fattori razionali della risolvente. Poichè il gruppo delle (25) ha per massimo moltiplicatore quello delle sostituzioni date dalle (26), basterà deter-

(*) Vedi Tortolini Annali di Mat. Anno 1831, pag. 8.

(**) Ivi, pag. 14.

(***) Vedi Ann. di Mat. compilati da B. Tortolini genn. 1831. Nota sulla risolubilità ec.

(****) Ivi.

minare il moltiplicatore di questo ultimo. In questo caso la equazione (14) della prima parte, diviene

$$\psi(\rho i) = \rho^m \psi(i)$$

che ha per integrale

$$\psi(i) = i^m$$

dunque la risolvente Lagrangiana delle equazioni di grado μ primo ha tanti fattori razionali di grado μ , quante sono le sostituzioni ψ cioè quanti i numeri primi inferiori a μ : gli altri sono di grado $\mu(\mu-1)$, e tutti poi risolvibili per radicali.

III.

DELLE EQUAZIONI IL GRADO DELLE QUALI È IL PRODOTTO DI PIÙ NUMERI PRIMI DIFFERENTI

25.° Una equazione il grado della quale è il prodotto di numeri primi differenti non può esser risolvibile per radicali, se il suo gruppo non è a lettere congiunte.

Poichè abbiamo veduto che l'ultimo gruppo di una equazione risolvibile per radicali dev'esser di grado primo p divisore del grado μ della equazione (v. n.° 19); e che il massimo gruppo che lo abbia per divisore è (v. P. I. n.° 26, 27, 28) a lettere congiunte quando i fattori di μ sono differenti tra loro.

26.° Una equazione irriducibile il grado $\mu = pq$ della quale ha dei fattori primi differenti non può esser risolvibile per radicali, se non è decomponibile in p fattori razionali di grado q , coll'aggiunzione delle sole radici di una equazione di grado p .

Distinguiamo con un apice h le lettere di uno stesso sistema, con un altro k il sistema al quale appartengono, avremo per il teorema precedente che tutte le sostituzioni del gruppo dovranno essere della forma

$$\begin{pmatrix} x_{h, \lambda} \\ x_{p(h), \tau(\lambda)} \end{pmatrix}$$

Siano $F_0, F_1, F_2, \dots, F_{p-1}$ altrettante funzioni ciascuna delle lettere di uno stesso sistema, e invariabili per le sostituzioni

$$(27) \quad \left(\begin{matrix} x_{h,1} \\ x_{p(h),k} \end{matrix} \right).$$

Esse saranno radici di una equazione di grado p il gruppo della quale, contiene soltanto le sostituzioni

$$(28) \quad \left(\begin{matrix} x_{h,k} \\ x_{h,pk} \end{matrix} \right);$$

e poichè esse sono variabili per tutte le sostituzioni (28), aggiunte ridurranno il gruppo alle sole (27). Dunque le funzioni invariabili per quelle saranno razionalmente cognite; e quindi anche le funzioni simmetriche di ogni sistema di radici: dunque per l'aggiunzione delle p radici F_k la proposta si ridurrà in p fattori razionali di grado q , come volevamo dimostrare.

È evidente che le funzioni simmetriche delle F , ossia i coefficienti della equazione della quale esse sono radici, saranno invariabili per tutte le sostituzioni del gruppo, e quindi razionali; o la risolvente Lagrangiana, che in questo caso è di grado

$$\frac{1.2.3.\dots\mu}{(p-1)p(1.2\dots q)^p} \quad (*)$$

dovrà avere un fattore razionale di primo grado se p è primo; se no, dovrà esser riduttibile parimente la equazione che dà le F , e così di seguito, finchè non si arrivi a una di grado primo; per la quale vale quello che abbiamo stabilito nel paragrafo precedente. Lo stesso deve dirsi dei fattori razionali di grado q , i quali posti a zero danno direttamente le radici.

Le condizioni esposte nei due teoremi dei num. 25° e 26°, non son sufficienti; ma le condizioni sufficienti sono già in esse contenute: perchè rimangono ridotte a quelle delle equazioni di grado primo, che tali sono le ultime equazioni irriducibili alle quali si arriva con questo metodo.

Quando una equazione irriducibile è di grado pq , i p e q

(*) V. Serret, Cours d'Alg. sup. pag. 240.

sono numeri primi differenti, indicando le radici colle lettere

$$x_{0,0}, x_{1,0}, \dots, x_{p-1,0}$$

$$x_{0,1}, x_{1,1}, \dots, x_{p-1,1}$$

$$\dots \dots \dots$$

$$x_{0,q-1}, x_{1,q-1}, \dots, x_{p-1,q-1}$$

i casi di risolubilità sono i soli tre seguenti :

1.° Quando il gruppo della equazione è di grado

$$p^2(p-1)^q q(q-1),$$

e le sue sostituzioni sono date da

$$\left(\begin{smallmatrix} x_{i,0} \\ x_{\varphi(i),0} \end{smallmatrix} \right), \left(\begin{smallmatrix} x_{i,1} \\ x_{\varphi(i),1} \end{smallmatrix} \right), \dots, \left(\begin{smallmatrix} x_{i,q-1} \\ x_{\varphi(i),q-1} \end{smallmatrix} \right); \left(\begin{smallmatrix} x_{i,h} \\ x_{\psi(h),h} \end{smallmatrix} \right).$$

2.° Quando è di grado

$$q^2(q-1)^p p(p-1)$$

e le sostituzioni sono

$$\left(\begin{smallmatrix} x_{0,i} \\ x_{\varphi(i),i} \end{smallmatrix} \right), \left(\begin{smallmatrix} x_{1,i} \\ x_{\varphi(i),i} \end{smallmatrix} \right), \dots, \left(\begin{smallmatrix} x_{p-1,i} \\ x_{\varphi(i),i} \end{smallmatrix} \right), \left(\begin{smallmatrix} x_{h,i} \\ x_{\psi(h),i} \end{smallmatrix} \right).$$

3.° Se il gruppo è di grado

$$pq(p-1)(q-1)$$

e le sostituzioni

$$\left(\begin{smallmatrix} x_{i,h} \\ x_{\varphi(i),\psi(h)} \end{smallmatrix} \right).$$

In tutti questi simboli dovrà aversi

$$\varphi(i) = ai + b, \quad \psi(h) = a'h + b'$$

essendo a e b numeri interi qualunque $< p$, a' e $b' < q$.

Le risolventi Lagrangiane delle equazioni di grado p e q dalle quali si fa dipendere la proposta, debbono inoltre aver tutte un fattore razionale di primo grado (v. num.° 24). Facendo $p=2$, $q=3$ si hanno i tre casi di risolubilità delle

equazioni di 6.º grado, sviluppati e dimostrati da *Luther* nel T. 36 del Giornale di Crelle.

27.º Da ciò che abbiamo stabilito nel numero precedente si deduce immediatamente che il grado del gruppo di una equazione di grado $m = pq$, dove p e q sono differenti, non deve esser maggiore di $1, 2 \dots q. 1. 2 \dots p$. Ora il Gruppo di una equazione di grado pq in generale è di grado $1.2.3 \dots pq$; dunque affinché sia risolubile per radicali dovrà aversi

$$1. 2. 3 \dots pq \leq 1. 2. 3 \dots q. 1. 2. 3 \dots p;$$

o anche

$$q + 1. q + 2 \dots pq \leq 1. 2. 3 \dots p$$

Io che evidentemente non può essere se p e $q > 1$; dunque l'equazioni i gradi delle quali ammettono dei fattori primi differenti, non sono in generale risolubili per radicali.

IV.

DELLE EQUAZIONI IL GRADO DELLE QUALI È LA POTENZA DI UN NUMERO PRIMO.

28.º Se il gruppo K di una equazione risolubile per radicali di grado p^r (p essendo un numero primo) non è a lettere congiunte, deve necessariamente 1.º non contenere altre sostituzioni che della forma

$$(29) \quad \left\{ \begin{array}{c} x_k \\ \sum_{r=0}^{p^r-1} B_r k^{p^r} + B_r \end{array} \right\}$$

(k e i B_r essendo radici di $x^{p^r} \equiv x \pmod{p}$); e in conseguenza esser di grado, o eguale a

$$M = p^r(p^r - 1)(p^r - p) \dots (p^r - p^{r-1}),$$

o a un divisore di M ; e tutte le radici della equazione debbon

essere funzioni razionali di $\nu + 1$ tra loro. 2.° Essendo sempre

$$K = K_0 G_1 G_2,$$

dove K_0 ha soltanto sostituzioni della forma

$$\begin{pmatrix} x_k \\ x_{k+k_0} \end{pmatrix},$$

e G_1, G_2 hanno il medesimo significato che al n.° 38; il gruppo G_1 il grado del quale è un divisore di

$$\frac{(p^\nu - 1)(p^\nu - p) \dots (p^\nu - p^{\nu-1})}{2(p - 1)},$$

deve essere decomponibile in gruppi di prima classe.

L'ultimo gruppo deve essere di grado p (v. n.° 19), dunque (v. n.° 28) il massimo gruppo che lo ha per ultimo divisore o è a lettere congiunte, o non contiene altre sostituzioni che lo (29) e il suo grado è un divisore di M , e non è decomponibile in gruppi di prima classe altro che quando lo è G_1 (v. P. I. n.° 38).

Le funzioni non simmetriche delle $\nu + 1$ radici che hanno per apici

$$0, \lambda, i, i^2, \dots, i^{\nu-1},$$

o di altre $\nu + 1$ delle radici della congruenza $x^\nu \equiv x \pmod{p}$, delle quali nessuna si possa esprimere linearmente per le altre (v. P. I. num.° 32) sono variabili per tutte le sostituzioni del gruppo: dunque (v. n.° 6), tutte le radici possono esprimersi razionalmente per esse.

Le prime condizioni del teorema contengono la seconda quando $p^\nu = 4$, $\equiv q$ (v. P. I. n.° 38).

29.° Affinchè una equazione irriducibile di grado p^ν (p essendo numero primo e ν qualunque) sia risolubile per radicali, è necessario e sufficiente o che essa sia decomponibile in $p^{\nu-2}$ equazioni ognuna di grado p^2 , i coefficienti delle quali siano funzioni razionali delle radici di una sola equazione di grado $p^{\nu-2}$, o che ciascuna delle radici possa prender la forma

$$x = \Lambda + \sqrt[p]{S_0} + \sqrt[p]{S_1} + \dots + \sqrt[p]{S_i},$$

essendo Λ razionale, e le S , radici di una equazione di grado $\delta \leq p^v$, i coefficienti della quale siano o razionali o funzioni razionali di equazioni di gradi minori di $p^v - 1$: e che si nell'un caso che nell'altro le equazioni dalle quali si fa così dipender la proposta siano risolubili per radicali.

Il gruppo della equazione o sarà a lettere congiunte, o sarà il gruppo K del numero precedente. Se è a lettere congiunte è evidente che si verifica il primo caso del Teorema (v. n.° 27). Se è eguale a K passiamo a dimostrare che si deve necessariamente verificare il secondo.

La espressione Lagrangiana del numero 21 sarà in questo caso :

$$S_\alpha = \left\{ \sum_{t=0}^{p-1} \alpha^t \sum_{h=0}^{p^v-1} x_{t+\sigma_h} \right\}^p,$$

essendo α radice immaginaria p^{esima} della unità, e rappresentando con σ_h la espressione

$$a_1 t + a_2 t^2 + \dots + a_{p-1} t^{p-1}$$

per una combinazione qualunque di valori numerici delle a minori di p . Essa è invariabile per le p^v sostituzioni circolari del gruppo K_0 . Ora tra i seguenti o successivi moltiplicatori di K_0 nel gruppo K se ne potranno prendere alcuni in modo che il loro prodotto sia del più alto grado $\leq p^v$, cioè al più eguale a $p^v - 1$. Chiamiamo questo gruppo Γ e δ il suo grado.

Se eseguiamo tutte le sostituzioni immaginabili sulle x_t contenute nella S_0 , avremo M valori differenti per la medesima,

$$(30) \quad S_0 S_1 S_2 \dots S_{M-1},$$

essendo, come è facile a dimostrarsi,

$$M = \frac{1 \cdot 2 \cdot 3 \cdot 4 \dots (p^v - 1)p^v}{p(1 \cdot 2 \cdot 3 \dots p^{v-1})^p}$$

Le sostituzioni di K eseguite sulle x_i della S_0 non potranno dare più di m dei valori (30), chiamando m il massimo comun divisore di M e di

$$M' = (p^v - 1)(p^v - p)(p^v - p^2) \dots (p^v - p^{v-1}).$$

Quelle di Γ non potranno dare più di δ valori (30), e δ dovrà essere divisore di m .

Ora costruiamo la equazione che ha per radici i δ valori (30) ottenuti colle sostituzioni di Γ . Il grado della risolvante Lagrangiana che ne darà i coefficienti sarà al più eguale

a $\frac{M}{\delta}$: e poichè facendo tutte le sostituzioni di K nelle funzioni simmetriche F di quei δ valori, le quali sono invariabili per le sostituzioni di $K_0\Gamma$, non si possono avere più di $\frac{m}{\delta}$ valori differenti, essendo $K_0\Gamma$ un divisore di K , la risolvante sarà riduttibile, e avrà un fattore razionale di grado non maggiore di $\frac{m}{\delta}$.

Dalla forma delle S è facile dedurre, rammentando il metodo già usato nell'Algebra, che le radici avranno la forma

$$x = A + \sqrt[p]{S_0} + \sqrt[p]{S_1} + \dots + \sqrt[p]{S_{v-1}},$$

A essendo il coefficiente del secondo termine della equazione.

Se $\frac{m}{\delta} < p^v - 1$ è già dimostrato il Teorema: ma quando non è, col metodo Lagrangiano è evidente che si potrà abbassare la equazione che dà le F finchè non si giunga a una risolvante di grado $< p^v - 1$.

Consideriamo ora alcuni casi particolari.

1.° Sia $v = 2$, $p = 2$, sarà $M = \frac{1 \cdot 2 \cdot 3 \cdot 4}{2(1 \cdot 2)^2} = 3$, $M' = 3 \cdot 2$, onde $m = 3$, e poichè δ deve essere un fattore di m , sarà

eguale a 3; e il grado del fattore razionale della risolvante Lagrangiana sarà eguale a $\frac{m}{\delta} = 1$.

$$2.^{\circ} \text{ Se } v=2; p=3; \text{ sarà } M = \frac{1.2.3 \dots 7.8.9}{3(1.2.3)^3} = 24.5.7, M' = 24.3;$$

$$m=24, \delta=8; \frac{m}{\delta} = 2.$$

$$3.^{\circ} \text{ Se } v=3, p=2; M = \frac{1.2 \dots 7.8}{2(1.2.3.4)^2} = 5.7, M' = 7.6.4,$$

$$m=7, \delta=7; \frac{m}{\delta} = 1.$$

Le risolventi Lagrangiane per l'equazioni di 4° e 8° grado debbono aver un fattore razionale di 1.° grado: per quello di 9° al più di secondo.

30.° Una equazione il gruppo della quale sia $>M$, avendo M il valore del n.° 28, e che abbia per grado una potenza di un numero primo, non può esser risolubile per radicali (v. n.° 28). Deve dunque aversi, se le radici non hanno delle particolari relazioni tra loro

$$p^v(p^v-1)(p^v-p) \dots (p^v-p^{v-1}) \geq p^v(p^v-1)(p^v-2) \dots 3.2.1,$$

o anche

$$(p^v-p)(p^v-p^2) \dots (p^v-p^{v-1}) \geq (p^v-2)(p^v-3) \dots 3.2.1.$$

Ora questo non ha luogo in generale altro che per i casi seguenti

$$\begin{array}{ll} v=1, & p=1; \quad v=2, \quad p=1 \\ & p=2; \quad p=2; \\ & p=3; \end{array}$$

dunque le equazioni il grado delle quali è potenza di un numero primo ed è >4 , non sono risolubili per radicali in generale; ma di quello il grado delle quali non è potenza di un numero primo non ve ne è alcuna (v. n.° 23 e 26); quindi nes-

una equazione di grado > 4 può essere in generale risolvibile per radicali.

Determinato se una equazione algebrica è o non è risolvibile per radicali, o per irrazionali primitivi di altre date classi, rimane a eseguire la risoluzione effettiva. Abbiamo avuto luogo di accennare il modo che può tenersi per la medesima; però, appena il grado della equazione è un poco elevato, i calcoli necessarj divengono di una lunghezza da stancare ogni paziente calcolatore. Ma le ricerche intraprese con successo da molti distinti geometri in questi ultimi tempi sulle quantità complesse della natura della espressione di Lagrange, fanno sperare che l'Algebra potrà non solo vantaggiarsi dell'acquisto di nozioni più determinate e più estese sulla natura degli irrazionali primitivi, ma giungerà anche ad arricchirsi di Tavole che diano gli elementi coi quali si possa con più speditezza condurre il calcolo della costruzione dei valori delle radici coi coefficienti; come ne abbiamo un esempio per le equazioni binomie, nei bei lavori dei Sigg. *Plana* e *Kummer*.

Pag.	Lin.	Errori	Correzioni
58	16.18	$D_{\psi}^{\pi''\theta} . D_{\psi}^{\pi'} \theta$	$D_{\psi}^{\pi''} D_{\psi}^{\pi'} \theta$
60	8	qn	q
65	24	essi fattori	esse i fattori
