I.1

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

(Apenas o esboço dum curso de iniciação)

CAPÍTULO V

NOÇÕES GERAIS DE GRUPO E CORPO

53. Axiomatização do conceito de grupo

Inicialmente, o conceito de "grupo", tal como o considerou GALOIS, dizia respeito unicamente a conjuntos de substituições. Mais tarde, por obra de SOPHUS LIE e de FELIX KLEIN, o conceito foi extendido a famílias de transformações biunívocas dum conjunto qualquer (finito ou infinito) sobre si mesmo. Sob esta forma o definimos no n.° 12: uma família não vazia de transformações diz-se um grupo, quando é fechada a respeito da multiplicação e da divisão (bastaria dizer "a respeito da divisão").

Mas o conceito de grupo extende-se expontaneamente a muitos outros domínios. Assim, por exemplo, é natural dizer que um conjunto não vazio de números, desprovido do elemento 0, forma um *grupo multiplicativo*, quando é fechado a respeito da divisão: o conjunto dos números racionais, excluído o zero, é um grupo multiplicativo; mas já o não é o conjunto dos inteiros. Um grupo multiplicativo – e até cíclico – é ainda o conjunto das raízes de índice n da unidade.

Por outro lado, é natural dizer que um conjunto não vazio de números forma um *grupo aditivo*, quando é fechado a respeito da adição e da subtracção (bastaria dizer "a respeito da subtracção"). É um grupo aditivo, por exemplo, o conjunto dos números inteiros,

positivos e negativos, o qual admite como subgrupo, entre outros, o conjunto dos números pares.

Este e muitos outros exemplos mostram a vantagem que pode haver numa definição geral de "grupo" e na construção de uma teoria abstracta, unificada, que englobe todas as possíveis concretizações deste conceito. O que desde logo se consegue por tal processo é uma notável economia de pensamento, evitando a repetição de raciocínios análogos em campos diversos, com terminologia e notações diversas. Por outro lado, este avizinhamento de ramos distintos da Matemática sob uma teoria comum é um dos mais fecundos recursos de que se têm valido até hoje o espírito criador dos matemáticos. Não se trata apenas de sistematizar, ou porventura assentar em base mais sólida, conhecimentos já adquiridos: trata-se dum autêntico método de investigação e descoberta, o chamado *método abstracto, formal ou axiomático*, que caracteriza todo o movimento das matemáticas modernas, desde a Álgebra à Topologia. Com tal orientação, a Matemática aproxima-se, por um lado, do campo da Lógica pura, ganhando em rigor e em beleza; enquanto, por outro lado, afastando-se só aparentemente da realidade concreta, se torna mais apta a penetrar no âmago das questões, por um maior poder de esquematização e de separação entre o que é essencial e o que é acidental.

Pode bem dizer-se, portanto, que a Matemática atinge, por esta via, um mais alto nível de racionalidade.

Vejamos pois como se define modernamente o conceito de "grupo" (segundo DEDEKIND). Seja H um conjunto não vazio de elementos $a, b, c, \ldots$ de natureza qualquer, e seja ϕ uma operação binária definida entre elementos de H, isto é, um processo de composição, pelo qual, a cada par ordenado (a, b) de elementos de H, devidamente escolhido, fique associado um terceiro elemento c de H.

Os elementos a, b dizem-se os *dados da operação* ϕ e o elemento c chama-se *resultado da operação* ϕ *aplicada aos elementos* a, b. Este elemento c pode ser representado indiferentemente pelos símbolos $\phi(a, b)$ ou $a \phi b$. Posto isto, diz-se que o conjunto H é um *grupo a respeito da operação* ϕ se, e só se, resultam verificadas as três seguintes condições:

g_1) A operação ϕ é *univocamente definida* em todo o conjunto H; isto é, para cada par ordenado (a, b) de elementos de H, existe um e um só elemento $c = a\phi b$.

g_2) A operação ϕ é *associativa*; isto é, tem-se

$$(a\phi b)\phi c = a\phi(b\phi c),$$

quaisquer que sejam $a, b, c \in H$.

g_3) A operação ϕ é *invertível*; isto é, dados dois elementos a, b quaisquer de H, é sempre possível encontrar em H elementos x, y tais que

$$a\phi x = b, \quad y\phi a = b.$$

Pode acontecer que, além destas, seja ainda verificada em H a condição seguinte:

g_c) $a\phi b = b\phi a$, quaisquer que sejam $a, b \in H$.

Neste caso, H diz-se um grupo *comutativo ou abeliano*. (Em geral, dois elementos a, b de H dizem-se *permutáveis*, quando se tem $a\phi b = b\phi a$).

Por exemplo, o conjunto dos números inteiros (positivos e negativos, incluido o zero) é um grupo comutativo a respeito da adição, mas já não é um grupo a respeito da subtracção, pelo facto de esta operação não ser associativa: não é lícito escrever em geral $(a-b)-c = a-(b-c)$.

Sempre que, num conjunto H, se encontra definida uma operação ϕ, o conjunto H diz-se *algebrizado* por esta operação, mesmo que não forme um grupo a respeito dela.

Observemos desde já que a família S de todas as transformações biunívocas dum conjunto A sobre si mesmo, algebrizada com a operação usual de produto, constitui um grupo segundo a presente definição, visto que nessa família são verificadas as condições g_1), g_2), g_3). Posto isto, para saber se uma dada subfamília M de S constitui ainda um grupo conforme a definição geral (a respeito da mesma operação de produto), basta averiguar se a família M é fechada a respeito da divisão, pois que, nessa hipótese, e só nessa, as condições g_1), g_2), g_3) resultam verificadas em M. O conceito actual de grupo é pois uma generalização do conceito definido no n.° 12.

Outros exemplos:

a) Seja R o conjunto dos números reais e φ a operação definida pela fórmula

$$x\varphi y = \sqrt[3]{x^3 + y^3};$$

facilmente se reconhece que R é um grupo a respeito de φ. Mas, a respeito da operação θ definida por

$$x\theta y = + \sqrt{x^2 + y^2}$$

já R não é um grupo, pela simples razão de que θ não é invertível.

b) Seja $\mathfrak{F}$ a família de todos os subconjuntos dum dado conjunto A não vazio. Em $\mathfrak{F}$ são definidas univocamente duas equações binárias – a intersecção ($\cap$) e a reunião ($\cup$) – ambas associativas e comutativas, mas nenhuma delas invertível. O conjunto $\mathfrak{F}$ não é portanto um grupo a respeito de qualquer destas operações.

c) Consideremos o conjunto $U = \{a, b\}$ e as operações φ, θ, definidas em U mediante as seguintes tabelas:

$x\varphi y$

x \ y	a	b
a	a	b
b	b	a

$x\theta y$

x \ y	a	b
a	a	a
b	a	b

É fácil ver que o conjunto U forma um grupo a respeito de φ, mas não já a respeito de θ, pois que não existe em U nenhum elemento x tal que $x\theta a = b$.

54. Primeiras consequências da axiomática dos grupos

A partir dos axiomas g_1), g_2), g_3) pode desenvolver-se, por dedução lógica, toda a teoria formal dos grupos.

Seja H um grupo a respeito duma dada operação ϕ. Tomado em H um elemento c qualquer, existirá necessariamente em H, por força de g_3), um elemento μ tal que $\mu\phi c = c$. Ora é de notar que este elemento μ goza da propriedade

$$\mu\phi a = a, \text{ qualquer que seja } a \in H.$$

Com efeito, ainda em virtude de g_3), existirá em H pelo menos um elemento x, tal que $c\phi x = a$, donde, atendendo a g_2):

$$\mu\phi a = \mu\phi(c\phi x) = (\mu\phi c)\phi x = c\phi x = a.$$

Ao elemento μ chamaremos *módulo da operação* ϕ (à esquerda). Analogamente se demonstra a existência de (pelo menos) um elemento υ de H, tal que

$$a\phi\upsilon = a, \text{ qualquer que seja } a \in H,$$

ao qual poderíamos chamar *módulo de operação* θ *à direita*. Simplesmente, o módulo à direita coincide com o módulo à esquerda, pois que:

$$\mu\phi\upsilon = \upsilon, \ \mu\phi\upsilon = \mu, \text{ donde } \mu = \upsilon.$$

Este mesmo raciocínio mostra que não pode haver mais de um módulo de cada lado.

Note-se que, usualmente, a operação grupal se apresenta umas vezes com o nome de "multiplicação", outras vezes com o nome de "adição". No primeiro caso, tem lugar a *linguagem multiplicativa*: o resultado da operação aplicada aos elementos dados *a, b* chama-se *produto* de *a* por *b* e representa-se por $a \cdot b$ ou ab; o módulo da operação chama-se *unidade* e pode representar-se por 1 (muitos autores usam o símbolo *e*), etc. No segundo caso, emprega-se a *linguagem aditiva*: em vez de *produto* (ab), diz-se *soma* ($a+b$); em vez de *unidade* (1), diz-se *zero* (0), etc.

Continuemos a usar ϕ como símbolo genérico de operação grupal em H. O axioma g_3) habilita-nos ainda a afirmar que, *para cada*

$a \in H$, *existe (pelo menos) um elemento* $\bar{a}$ *de* H, *tal que* $\bar{a}\phi a = \mu$ (*continuando a designar por* μ *o módulo de* ϕ).

Daqui resulta a univocidade da operação inversa de ϕ: *quaisquer que sejam* $a, b \in H$, *não pode haver mais de um elemento* x *tal que* $a\phi x = b$, *nem mais dum elemento* y *tal que* $y\phi a = b$. Com efeito, se for $a\phi x = a\phi x'$, virá, sucessivamente,

$$\bar{a}\phi(a\phi x) = \bar{a}\phi(a\phi x') \text{ ou seja } \mu\phi x = \mu\phi x',$$

donde, finalmente, $x = x'$. Analogamente se demonstra a segunda parte da proposição.

Em particular, podemos garantir que, para cada $a \in H$, existe *um, e um só*, elemento a de H, tal que $\bar{a}\phi a = \mu$. Em linguagem multiplicativa, o elemento a chama-se *o inverso* (à esquerda) de a e representa-se por a^{-1}; em linguagem aditiva, $\bar{a}$ chama-se o *simétrico* (*à esquerda*) de a e representa-se por $-a$. *Mas o inverso à esquerda também é inverso à direita*; isto é, tem-se não só

$$a^{-1}a = 1,$$

mas ainda $a\,a^{-1} = 1$. Com efeito, de $a^{-1}a = 1$, vem

$$(a^{-1}a)\,a^{-1} = a^{-1}$$

ou seja

$$a^{-1}(a\,a^{-1}) = a^{-1},$$

donde, multiplicando à esquerda por a:

$$a\,a^{-1} = 1, \qquad \text{q.e.d.}$$

Este mesmo resultado mostra que $(a^{-1})^{-1} = a$.

55. Representação dum grupo qualquer mediante um grupo de transformações

As noções de "homomorfismo", "isomorfismo" e "automorfismo" atrás formuladas para os grupos de transformações extendem-se automaticamente ao novo conceito de grupo. Sejam G_1, G_2 dois

grupos quaisquer, relativos a operações ϕ_1, ϕ_2, definidas respectivamente em G_1 e G_2; chamaremos *homomorfismo* do grupo G_1 sobre o grupo G_2 toda a transformação unívoca τ do primeiro sobre o segundo, tal que

1) $\tau(G_1) = G_2$,

2) $\tau(a \phi_1 b) = \tau(a) \phi_2 \tau(b)$ quaisquer que sejam $a, b \in G_1$.

Se τ é além disto reversível, diz-se um *isomorfismo*, e prova-se que a sua inversa τ^{-1} é também um isomorfismo.

Assim, por exemplo, o operador *log* estabelece um isomorfismo entre o grupo multiplicativo dos números positivos e o grupo aditivo dos números reais:

$$log\,(x \cdot y) \equiv log\, x + log\, y\,.$$

No desenvolvimento da teoria geral dos grupos, é cómodo adoptar uma só das linguagens – aditiva ou multiplicativa. Comummente opta-se pela segunda, e é o que faremos a partir deste momento.

Consideremos um grupo G qualquer. Designando por a um elemento arbitrário de G, é fácil ver que a fórmula

$$y = ax \tag{26}$$

define uma transformação biunívoca do conjunto G sobre si mesmo, pois que; 1) a cada $x \in G$ fica a corresponder um e um só elemento $y (= ax)$ de G; 2) reciprocamente, para cada elemento y de G, existe um e um só elemento x de G, tal que $ax = y$: o elemento $x = a^{-1}y$.

Mas o elemento a de G é arbitrário. Deste modo, para cada $a \in G$, tem-se uma transformação biunívoca de G sobre si mesmo, transformação que designaremos por f_a:

$$f_a(x) = ax, \text{ para cada } x \in G\,.$$

(Assim, por exemplo, se G for o grupo multiplicativo dos números positivos, f_2 será o operador que transforma 1 em 2, -3 em -6, 3/4 em 3/2, etc.)

Não oferece agora dificuldade demonstrar que: *o conjunto* $\overline{G}$ *de todas as transformações* f_a *assim obtidas (quando a percorre G) é um grupo*; e que: *a correspondência* $a \to f_a$ *é um isomorfismo de G sobre* $\overline{G}$.

Com efeito, dados dois elementos a, b quaisquer de G, tem-se:

$$f_a(x) = ax, \quad f_b(x) = bx, \quad \text{para cada } x \in G,$$

e portanto

$$(f_a f_b)(x) = f_a(f_b(x)) = a(bx) = (ab)x = f_{ab}(x).$$

Tem-se pois que, no produto ab, corresponde precisamente o produto $f_a f_b$ ou seja, em símbolos

$$f_{ab} = f_a \cdot f_b,$$

o que significa, precisamente, que a correspondência $a \to f_a$ é um homomorfismo de G sobre $\overline{G}$. Daqui resulta logo que $\overline{G}$ também é um grupo. Finalmente, é fácil ver que a referida correspondência é biunívoca, pois que a desigualdade $a \neq b$ implica $f_a \neq f_b$. Com efeito, se fosse $f_a = f_b$, ter-se-ia em particular $f_a(1) = f_b(1)$ ou seja $a \cdot 1 = b \cdot 1$, donde $a = b$.

O facto que acabamos de estabelecer tem grande importância e pode enunciar-se nestes termos: *todo o grupo G é representável isomorficamente mediante um grupo de transformações*. Deste modo, uma vez que os isomorfismos respeitam (por definição) as propriedades algébricas dos grupos, somos levados a concluir que *todos os anteriores teoremas com carácter exclusivamente algébrico, relativos a grupos de transformações, podem ser transportados ao domínio geral dos grupos abstractos que não se encontre já representado na teoria dos grupos de transformações*.

56. Axiomatização do conceito de corpo

Observemos que todo o corpo numérico Δ é um grupo comutativo a respeito da adição e que, privado do elemento 0, é ainda um grupo (comutativo) a respeito da multiplicação; além disso, a multiplicação

é, em Δ, distributiva a respeito da adição. Daqui se parte para a noção geral de corpo: Seja M um conjunto de elementos quaisquer, algebrizado por meio de duas operações, uma das quais convencionaremos chamar *adição* e a outra *multiplicação*; diz-se que M é um *corpo* a respeito destas operações, quando são verificadas as seguintes condições:

c_1) O conjunto M é um grupo comutativo a respeito da adição;
c_2) Privado do elemento 0, o conjunto M é um grupo a respeito da multiplicação;
c_3) Em M, a multiplicação é *distributiva à direita e à esquerda* a respeito da adição; isto é, tem-se, quaisquer que sejam $a, b, c \in M$:

$$a(b+c) = ab + ac; \quad (b+c)a = ba + ca.$$

c_4) $a \cdot 0 = 0$, qualquer que seja $a \in M$.
Esta condição pode ainda ser substituída pela condição mais fraca:
c_4') O produto de 0 por cada elemento de M é sempre um determinado elemento de M (que se demonstra depois ser 0).

Se, além disto, a multiplicação for comutativa em M, dir-se-á que M é um *corpo comutativo*.

Os corpos de números e de funções atrás considerados reentram, manifestamente, na actual definição. Mas note-se que, por exemplo, o conjunto C de todas as funções contínuas num intervalo (a, b) não é um corpo, a respeito das noções usuais de soma e do produto de funções; com efeito, se designarmos por f uma função que se anule em metade do intervalo (a, b), mas não na outra metade (existam tais funções em C), o elemento $1/f$ não pertencerá a C, e tem-se, contudo, $f \neq 0$.

Exemplos notáveis de corpos são os seguintes:

Representando por E o conjunto dos inteiros, positivos e negativos, zero incluído, e fixado em E um elemento m qualquer, já sabemos (n.° 18) que a relação de congruência a respeito do módulo m determina em E uma repartição. Suponhamos, para fixar ideias, $m = 3$, e convencionemos representar por $\overline{a}$ o conjunto dos elementos de E congruentes a a mod. 3, sendo a um elemento arbitrário de E.

É claro que, neste caso, se tem uma repartição de E apenas em três classes: $\overline{0}$, $\overline{1}$, $\overline{2}$. (Note-se que é $\overline{0} = \overline{3} = \overline{6} = \cdots$, $\overline{1} = -\overline{2} = \overline{7} \cdots$, $\overline{2} = -\overline{4} = \overline{8} = \cdots$). Representemos por $\overline{E}$ o conjunto $\{\overline{0}, \overline{1}, \overline{2}\}$. É natural agora definir soma e produto de dois elementos $\overline{a}$, $\overline{b}$ de $\overline{E}$, mediante as fórmulas:

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a}\,\overline{b} = \overline{a\,b}.$$

Teremos então as duas seguintes tabelas de adição e multiplicação em $\overline{E}$:

$x + y$

x \ y	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$x \cdot y$

x \ y	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

É fácil constatar que o conjunto E assim algebrizado é um corpo comutativo.

Ter-se-ia obtido ainda um corpo comutativo (e finito), se, em vez de $m = 3$, se tivesse tomado para m um valor primo qualquer. Todavia, se m não for um número primo, o sistema algébrico obtido por este processo não será um corpo, como se pode verificar.

Uma das questões centrais da moderna Álgebra abstracta é esta: sendo C um corpo arbitrário, determinar uma condição necessária e suficiente para que a teoria de GALOIS seja válida para as equações algébricas com os coeficientes em C.

Para um estudo desenvolvido das teorias dos grupos, dos corpos, bem como de outros sistemas algébricos, podem consultar-se várias obras, nomeadamente a de VAN DER WAERDEN, *Moderne Algebra.*

O presente curso não pretende ser mais do que uma introdução às referidas teorias.

NOTAS FINAIS

A) *Sobre o teorema de LAGRANGE.*

O teorema de LAGRANGE generalizado pode ainda ser apresentado sob a seguinte forma, particularmente cómoda para a aplicação à teoria de GALOIS:

Consideremos uma equação algébrica $f(z) = 0$, *de raízes* $\alpha_1, \alpha_2, \ldots, \alpha_n$, *com os coeficientes num dado corpo* Δ, *e seja* G *um seu grupo admissível a respeito de* Δ. *Consideremos, por outro lado, uma função racional* $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *das raízes desta equação, com os coeficientes em* Δ *e pertencente em sentido restrito a um grupo* H *em* G. *Nestas condições, qualquer outra função racional das raízes,*

$$\gamma = \Psi(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

com os coeficientes em Δ, *que fique formalmente invariante para as substituições de* H, *terá o valor em* $\Delta(\beta)$.

A técnica da demonstração é inteiramente análoga à que seguimos nos n.os 30 e 32. Sejam $\beta_1 (= \beta), \beta_2, \ldots, \beta_m$ as funções conjugadas de β em G, e

$$\gamma_1 (= \gamma), \gamma_2, \ldots, \gamma_m$$

as funções correspondentes obtidas a partir de γ. Tomando para incógnitas $c_1, c_2, \ldots, c_m$, o determinante do sistema

$$(27) \qquad \gamma_i = c_1 \beta_i^{m-1} + c_2 \beta_i^{m-2} + \cdots + c_m \quad (i = 1, 2, \ldots m),$$

é o determinante de VANDERMONDE em $\beta_1, \beta_2, \ldots, \beta_m$ e portanto $\neq 0$. Por outro lado, qualquer substituição θ de G sobre os $\alpha\alpha$ não faz mais do que produzir uma substituição sobre os $\beta\beta$ e a substituição

correspondente sobre os $\gamma\gamma$, provocando assim, quando muito, uma alteração da ordem das equações (27). Os coeficientes $c_1, c_2, \ldots, c_m$ são pois, por intermédio dos $\beta\beta$ e dos $\gamma\gamma$, funções racionais dos $\alpha\alpha$, com os coeficientes em Δ que se mantêm formalmente invariantes para as substituições de G. Mas G é, por hipótese, um grupo admissível da equação $f(z) = 0$ a respeito de Δ. Logo, tem-se

$$c_1, c_2, \ldots, c_m \in \Delta,$$

o que prova a afirmação feita.

B) *Sobre as equações cíclicas.*

Nas considerações desenvolvidas no n.° 37 sobre a resolução algébrica da equação cíclica, há um ponto a rectificar. A função das raízes,

$$\beta = \sum_{k=1}^{n} \omega^{k-1} \alpha_k,$$

só pertencerá em sentido restrito ao grupo $\mathscr{T}$ em H, se for $\beta \neq 0$. Esta dificuldade pode ser removida do seguinte modo: se os $\alpha\alpha$ são todos distintos, existe necessariamente um expoente μ tal que

$$\sum_{k}^{n} \omega^{k-1} \alpha_k^{\mu} \neq 0;$$

com efeito, se assim não fosse, as equações

$$\omega^0 \alpha_1^r + \omega \alpha_2^r + \cdots + \omega^{n-1} \alpha_n^r = 0 \quad (r = 0, 1, \ldots, n-1),$$

considerando $\omega^0, \omega, \ldots, \omega^{n-1}$ como incógnitas, formariam um sistema determinado, tendo por única solução $\omega^0 = \omega = \cdots = \omega^{n-1} = 0$, o que é absurdo. Pode então tomar-se para valor de β o somatório

$$\sum_{k=1}^{n} \omega^{k-1} \alpha_k^{\mu},$$

em vez do primeiro. Deste modo se evita o inconveniente indicado, e todos os raciocínios podem seguir como foi dito no n.° 37.

Página em branco

ÍNDICE

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

CAP. I – **Generalidades sobre conjuntos e transformações**

1. Noção geral de conjunto e as relações lógicas primitivas 17
2. Operações lógicas sobre conjuntos 19
3. Conjuntos formados dum só elemento e conjuntos de conjuntos 20
4. A noção de conjunto vazio 22
5. O conceito geral de transformação 22
6. Transformações entre conjuntos finitos 26
7. Produto de duas transformações 28
8. Propriedades gerais dos produtos de transformações 31
9. Potências dum operador 34
10. Período duma transformação 35
11. Substituições cíclicas 37
12. Conceito de grupo de transformações 39
13. Grupos de substituições 40
14. Grupo duma função 42
15. Intersecção de dois ou mais grupos. Geradores dum grupo 46
16. Imagem dum conjunto; imagem duma transformação 47
17. Transformado dum grupo 51

CAP. II – **Transitividade e Homomorfia**

18. Relações de equivalência; repartições dum conjunto 53
19. Equivalência a respeito dum grupo. Sistemas de transitividade . 57
20. Alusão ao programa de Erlangen 59
21. Funções conjugadas duma função dada. Conceito de subgrupo invariante 60
22. Classes laterais dum grupo 65
23. O conceito de homomorfismo entre grupos 69
24. Isomorfismos e automorfismos 71
25. Propriedades algébricas e propriedades específicas. Isomorfismos internos 73
26. Primeira noção de grupo cociente 75
27. Teoremas sobre homomorfismos. Noção geral de grupo cociente 78

CAP. III – **Resolubilidade por meio de radicais (1ª parte)**

28. O teorema das funções simétricas 85
29. Equações resolventes. Transformações de TSCHIRNHAUS 92
30. Teorema de LAGRANGE 95
31. Consequências do teorema de LAGRANGE 98
32. Generalização do teorema de LAGRANGE 102
33. Noção de corpo numérico 104
34. Funções pertencentes a um grupo em sentido restrito 106
35. O grupo de GALOIS duma equação 111
36. Pesquisa do grupo de GALOIS duma equação 114
37. Equações do terceiro grau. Equações cíclicas 116
38. Condição suficiente de resolubilidade por meio de radicais 122

CAP. IV – **Resolubilidade por meio de radicais (2ª parte)**

39. Redutibilidade dos polinómios. Corpos algebricamente fechados 133
40. Teorema fundamental da irredutibilidade. Componentes dum número num dado corpo 135

41. Isomorfismos e automorfismos entre corpos 140
42. Teorema fundamental dos isomorfismos entre corpos algébricos 142
43. O grupo de GALOIS como grupo de automorfismos 146
44. Estudo da redutibilidade através do grupo de GALOIS 150
45. Equações binómias 152
46. Teorema de GALOIS sobre adjunções 153
47. Equações ciclotómicas 156
48. Critério geral de resolubilidade por meio de radicais 159
49. Equações com coeficientes variáveis 161
50. Corpos de funções 162
51. Equação geral de grau n 164
52. O grupo S_n, para $n > 4$, não é resolúvel 165

CAP. V – **Noções Gerais de Grupo e Corpo**

53. Axiomatização do conceito de grupo 169
54. Primeiras consequências da axiomática dos grupos 172
55. Representação dum grupo qualquer mediante um grupo de transformações 174
56. Axiomatização do conceito de corpo 176

Notas finais 179
Índice 183