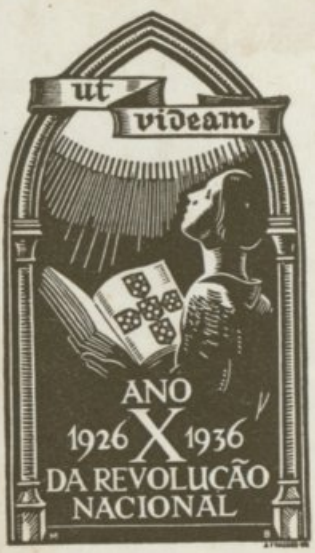

Aureliano Lopes de Mira Fernandes

Theorias de Galois

I

Elementos da theoria dos grupos de substituições de ordem finita

COIMBRA
Imprensa da Universidade
1910

Theorias de Galois

Aureliano Lopes de Mira Fernandes

Theorias de Galois

I

Elementos da theoria dos grupos de substituições de ordem finita

COIMBRA
Imprensa da Universidade
1910

O importantissimo problema da resolução algebrica das equações, largamente tratado por LAGRANGE e ABEL, tomou uma feição nova com as theorias e methodos de EVARISTO GALOIS.

Na sua Memoria *Sur les conditions de résolubilité des équations par radicaux,* publicada em 1846 no *Journal de mathématiques pures et appliquées* de LIOUVILLE, quatorze annos depois da morte do auctor, prova GALOIS que *a toda a equação algebrica corresponde um determinado grupo de substituições sobre as respectivas raizes,* de cujas propriedades, intimamente ligadas com as da equação, se póde concluir a possibilidade ou impossibilidade da sua resolução por meio de equações secundarias.

O primitivo problema baseia-se, desde então, na theoria dos grupos de substituições.

Sam os elementos d'essa theoria o objecto d'este despretencioso trabalho que terá como complemento o estudo da resolução algebrica das equações, segundo GALOIS.

I

Elementos da theoria dos grupos de substituições de ordem finita

A minha mãe

Dissertação inaugural para o acto de conclusões magnas na faculdade de Mathematica da Universidade de Coimbra

PRELIMINARES

1. A operação que transforma uma na outra duas permutações sobre os mesmos elementos chama-se uma *substituição.*

Estabelecida uma correspondencia ordenada entre os elementos das duas permutações, a substituição transforma os elementos da primeira nos elementos correspondentes da segunda.

Representamos uma substituição S pela seguinte notação

$$S = \begin{pmatrix} a_{i_1} & a_{i_2} & \dots & a_{i_n} \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

quando a substituição S é tal que transforma ordenadamente os elementos da segunda linha nos correspondentes da primeira. Consideramos identicas duas substituições que transformam cada elemento num mesmo elemento; podemos, portanto, suppor que as substituições se effectuam sempre a partir da mesma permutação.

Chama-se *identidade* á substituição que transforma cada elemento em si mesmo; representa-se pelo symbolo 1.

Á substituição que resulta de praticar successivamente duas substituições α e β chama-se *producto* das duas substituições consideradas; representa-se essa substituição pelo symbolo $\alpha\beta$, se a substituição α foi a primeira que se executou.

Em particular, representa-se por α^n a substituição que resulta de effectuar n vezes consecutivas a substituição α.

O producto de substituições, que póde ter logar para qualquer numero de factores, gosa da propriedade associativa, e não gosa, *em geral,* da propriedade commutativa. Se $\alpha\beta = \beta\alpha$ as substituições α e β dizem-se *permutaveis.*

Para mostrar que a propriedade associativa se verifica para

o producto de substituições, basta verificá-la para tres factores. Sejam α, β e γ tres substituições sobre os mesmos elementos; supponhamos que a substituição α transforma a_k em a_l; a substituição β transforma a_l em a_m; e a substituição γ transforma a_m em a_n. O producto $(\alpha\beta)\gamma$ transformará a_k em a_n; mas como o producto $\beta\gamma$ transforma a_l em a_n, a substituição $\alpha(\beta\gamma)$ transformará tambem a_k em a_n. Portanto:

$$(\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Da propriedade associativa do producto de substituições conclue-se que

$$(1) \qquad \alpha^n \cdot \alpha^m = \alpha^{n+m}.$$

Representando por α^{-1} a substituição inversa de α, por α^{-n} a substituição $(\alpha^{-1})^n$ e por α^0 a identidade, a relação (1) verificar-se-ha para quaesquer expoentes inteiros.

Effectuando successivamente a substituição α, repetir-se-ham as substituições potencias, a partir de um certo expoente, por ser finito o numero total de substituições sobre um numero n de objectos. A primeira substituição que se repete é a identidade; com effeito, se fôr $\alpha^{n+m} = \alpha^n$, será $\alpha^{n+m-n} = \alpha^{n-n}$; ou $\alpha^m = \alpha^0$.

O menor expoente m, para o qual é $\alpha^m = \alpha^0 = 1$, é o *periodo* de α. As potencias de α de expoente inferior a m sam todas distinctas.

2. Uma substituição diz-se *cyclica* quando os elementos que ella substitue se podem ordenar de modo tal que a substituição effectúa sobre elles uma permutação circular. É cyclica, por exemplo, a substituição

$$\alpha = \begin{pmatrix} a_1 & a_4 & a_2 & a_3 & a_5 \\ a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix}$$

porque as lettras que ella substitue, a_2, a_3, a_4, postas pela ordem a_2, a_4, a_3, sam permutadas circularmente pela substituição α.

Uma substituição cyclica representa-se abreviadamente escrevendo entre parentheses a permutação dos elementos sobre que ella opera circularmente. No exemplo é $\alpha = (a_2\, a_4\, a_3)$.

THEOREMA. — *Toda a substituição é um producto de substituições cyclicas sobre elementos diversos.*

Com effeito, representando por i_1 um qualquer dos elementos

sobre que opera a substituição α, suponhamos que esta substituição troca i_1 por i_2, i_2 por i_3, etc. Escrevendo a successão $i_1 i_2 \ldots$, é visivel que o primeiro elemento repetido é i_1; pois que, sendo eguaes i_n e i_m, sê-lo-ham tambem i_{n-1} e i_{m-1}. A substituição α contem, pois, o cyclo $\alpha_1 = (i_1 i_2 \ldots i_k)$, sendo i_k o elemento que α tròca por i_1.

Se a substituição α não troca mais lettras, ella equivale ao cyclo α_1. No caso contrario, a partir de uma dessas lettras b_1, formaremos outro cyclo α_2 com lettras diversas das que sam permutadas circularmente por α_1; e assim successivamente. Será $\alpha = \alpha_1 \alpha_2 \ldots \alpha_n$.

É manifesto que os factores de α sam permutaveis.

3. Chama-se *transposição* á substituição cyclica sobre dois elementos.

Uma substituição é sempre um producto de transposições, porque um cyclo de ordem k é um producto de $k-1$ transposições, e toda a substituição é um producto de cyclos permutaveis.

Qualquer que seja o modo como uma substituição se decompõe em producto de transposições, o numero d'estas guarda sempre a mesma paridade.

Com effeito, o numero de transposições em que póde decompôr-se um cyclo é sempre da mesma paridade; e cada substituição é um producto de determinados cyclos.

Uma substituição diz-se *par* ou *impar* segundo se decompõe num numero par ou impar de transposições.

A substituição $\alpha_1 = \beta^{-1} \alpha \beta$ diz-se *transformada* de α por meio de β. Será

$$\alpha = \beta \alpha_1 \beta^{-1} = (\beta^{-1})^{-1} \alpha_1 \beta^{-1}$$

a transformada de α_1 por meio de β^{-1}.

Se fôr $\alpha_1 = \alpha$, será $\alpha\beta = \beta\alpha$ e α e β serám permutaveis.

Duas substituições transformadas uma da outra dizem-se *semelhantes*. Sam semelhantes os productos $\alpha\beta$ e $\beta\alpha$: o segundo é transformado do primeiro por meio de α.

I

Grupos de ordem finita. — Transitividade e primitividade

4. Um systema de substituições $\alpha_1, \alpha_2 \ldots \alpha_n$, sobre os mesmos elementos, fórma um *grupo,* quando o producto de duas substituições do systema é ainda uma substituição do systema.

A denominação de grupo, applicada a um systema de substituições nas condições precedentes, é devida a GALOIS.

O conceito de grupo, originado na theoria das substituições, generalisa-se a qualquer cathegoria de operações, gosando das seguintes propriedades: 1.ª a applicação successiva de duas quaesquer operações d'essa cathegoria é equivalente a uma operação determinada, a que chamamos producto das duas primeiras; 2.ª esse producto gosa da propriedade associativa.

Um grupo diz-se *finito* ou *infinito,* segundo é finito ou infinito o numero de operações que o compõem.

Os grupos infinitos sam ainda *discontinuos* ou *continuos,* segundo é numeravel ou não o conjuncto das operações do grupo.

Occupar-nos hemos dos grupos finitos de substituições, aos quaes se reduz, por considerações adiante feitas, o estudo dos grupos finitos quaesquer de operações.

Chama-se *ordem* de um grupo finito de substituições ao numero de substituições do grupo.

Todo o grupo contem a identidade, como resulta da propria definição.

Chama-se *grupo total* sobre n elementos, ao grupo formado por todas as $n!$ substituições possiveis sobre as permutações d'esses elementos.

As substituições pares do grupo total formam manifestamente um grupo, a que se dá o nome de *grupo alterno.*

Chama-se *cyclico* o grupo formado por todas as potencias distinctas de uma mesma substituição.

As substituições impares do grupo total não constituem grupo.

5. Se as substituições de um grupo G_1 pertencem todas a um grupo G, diz-se que G_1 é um *subgrupo* de G.

THEOREMA. — *A ordem de um grupo é multipla da ordem de qualquer dos seus sub-grupos.*

Seja, com effeito, G_1 um sub-grupo de G, n_1 e n as respectivas ordens. Se G_1 não coincide com G (caso em qne seria $n = n_1$, o que demonstraria o theorema), haverá uma substituição g_α de G differente das substituições (1) $g_1 = 1, g_2 \ldots g_{n_1}$ de G_1. As substituições

$$(2) \qquad g_1 g_\alpha, \quad g_2 g_\alpha, \quad \cdots \quad g_{n_1} g_\alpha$$

pertencentes a G, sam todas distinctas e nenhuma d'estas pertence a G_1. Com effeito, se fôsse $g_i g_\alpha = g_k g_\alpha$, seria $g_i = g_k$ o que é impossivel, suppondo que g_i e g_k sam substituições de G_1.

Por outro lado, se $g_i g_\alpha$ pertencesse a G_1, seria $g_i g_\alpha = g_k$; d'onde

$$g_i^{-1} g_i g_\alpha = g_i^{-1} g_k;$$

ou

$$g_\alpha = g_i^{-1} g_k;$$

e nesse caso g_α pertenceria a G_1.

Se as substituições (1) e (2) sam todas as de G, é $n = 2n_1$. Se assim não succeder e g_β é uma substituição de G, differente das substituições (1) e (2), seram tambem

$$(3) \qquad g_1 g_\beta, \quad g_2 g_\beta \cdots g_{n_1} g_\beta$$

distinctas entre si e differentes das substituições (1) e (2).

A continuação do raciocinio mostra que as substituições do grupo G se podem agrupar no quadro seguinte:

$$(4) \qquad G \begin{cases} g_1, & g_2 & \cdots g_{n_1} \\ g_1 g_\alpha, & g_2 g_\alpha & \cdots g_{n_1} g_\alpha \\ g_1 g_\beta, & g_2 g_\beta & \cdots g_{n_1} g_\beta \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ g_1 g_\lambda, & g_2 g_\lambda & \cdots g_{n_1} g_\lambda \end{cases}$$

o que demonstra o theorema.

O quociente $\frac{n}{n_1} = k$ chama-se o *indice* do subgrupo G_1 no grupo G.

THEOREMA. — *O grupo alterno é um subgrupo, de indice 2, do grupo total.*

Com effeito, multiplicando todas as substituições do grupo total por uma substituição impar, as substituições pares mudam-se em impares e reciprocamente.

Ha, pois, tantas substituições pares como impares no grupo total; e o grupo alterno é de indice 2.

6. Um grupo diz-se *transitivo* se, dados dois elementos quaesquer a_i e a_k, ha sempre no grupo uma substituição que troca a_i por a_k.

Basta, para isso, que haja no grupo substituições que troquem um certo elemento a_1 por cada um dos outros.

Num grupo *intransitivo* de substituições sobre n elementos, um elemento a_1 só póde ser trocado, pelas substituições do grupo, nalguns elementos $a_2, a_3 \ldots a_k$, sendo $k < n$. Diz-se que os elementos $a_1, a_2 \ldots a_k$ formam um *systema de transitividade* para as substituições do grupo.

Os elementos, sobre que operam as substituições de um grupo intransitivo, decompõem-se em systemas de transitividade. Nenhuma substituição do grupo póde trocar um elemento de um systema por um elemento de outro systema; ha sempre uma substituição do grupo que troca dois elementos quaesquer de um mesmo systema.

Um grupo transitivo diz-se *m vezes transitivo* quando, escolhidos dois systemas de m elementos cada um, entre aquelles sobre que opera o grupo, e ordenados de qualquer maneira os elementos dos dois systemas, ha sempre uma substituição do grupo que troca os elementos do primeiro systema ordenadamente nos do segundo.

7. Um grupo transitivo diz-se *imprimitivo* se os elementos sobre que opera o grupo se podem dividir em systemas de *egual numero de elementos*, de modo tal que cada substituição do grupo troca *todos* os elementos de um systema pelos de outro systema, que póde coincidir com o primeiro.

No caso contrario, um grupo transitivo diz-se *primitivo*.

Da definição resulta que um grupo transitivo sobre m elementos é primitivo, se fôr $m > 1$.

THEOREMA. — *É imprimitivo todo o grupo transitivo, differente do grupo total, que contem uma transposição.*

Seja $(a_1\, a_i)$ essa transposição, e $a_1, a_2 \ldots a_n$, os elementos sobre que opera o grupo G.

Poderám existir no grupo outras transposições:

$$(1) \qquad \{(a_2\, a_i),\quad (a_3\, a_i) \ldots (a_k\, a_i)\}$$

contendo a_i; mas o seu numero k será menor que n, porque, se fôsse $k = n$, o grupo coincidiria com o grupo total.

Não ha no grupo G nenhuma transposição que troque um dos elementos (2) $a_1, a_2, \ldots a_k, a_i$ por outro elemento a_{i+1} differente de todos elles; porque então o grupo G conteria a transposição $(a_{i+1}\, a_i)$. Haverá, porém, uma substituição α que troca a_1 por a_{i+1}, visto ser o grupo transitivo.

Seja

$$\alpha = \begin{pmatrix} a_{i+1}\, a_{i+2} \ldots & a_{2i} \\ a_1 \quad a_2 \quad \ldots\, a_k\, a_i & \end{pmatrix}.$$

No grupo G existirám as transposições

$$(a_{i+1}\, a_{i+2}),\quad (a_{i+1}\, a_{i+3}) \ldots (a_{i+1}\, a_{2i}),$$

que sam transformadas das transposições (1) por meio de α; e não haverá em G nenhuma transposição que troque um dos elementos (3) $a_{i+1}, a_{i+2} \ldots a_{2i}$ por outro elemento a_{2i+1}, porque a sua transformada por meio de α^{-1} seria uma transposição, trocando um dos elementos (2) por outro elemento não pertencente a (2).

Vê-se, pois, continuando o raciocinio, que os n elementos do grupo se decompõem em systemas de i elementos cada um, que sam systemas de imprimitividade.

II

Isomorphismo e composição dos grupos. — Theoremas de Jordan, Hölder e Sylow. — Grupos resoluveis

8. Dois grupos G e G′ dizem-se *isomorphos* quando entre as substituições de um e de outro se póde estabelecer uma correspondencia tal que ao producto $g_1 g_2$, de duas substituições quaesquer do primeiro, corresponde no segundo o producto $g'_1 g'_2$ das duas substituições g'_1 e g'_2, respectivamente correspondentes a g_1 e g_2.

Se G e G′ sam da mesma ordem e a correspondencia entre as respectivas substituições é biunivoca, o isomorphismo diz-se *holoedrico*. Se a cada substituição de G corresponde uma só substituição em G′, mas a cada substituição de G′ corresponde mais de uma em G, o isomorphismo é *meriedrico*.

Da definição resulta que, em dois grupos holoedricamente isomorphos:

1.° *As identidades sam substituições correspondentes.*

2.° *Duas substituições correspondentes têem o mesmo periodo.*

3.° *Se dois grupos* G *e* G′ *sam holoedricamente isomorphos, a cada sub-grupo do primeiro corresponde um sub-grupo do segundo que lhe é holoedricamente isomorpho.*

Em dois grupos meriedricamente isomorphos, G e G′, se a ordem de G é maior que a de G′, o periodo de qualquer substituição de G é multiplo do periodo da substituicão correspondente de G′.

THEOREMA. — *Se* G *e* G′ *sam meriedricamente isomorphos, as substituições de* G, *que correspondem á identidade em* G′, *formam em* G *um subgrupo.*

Com effeito, se fôrem

(1) $\qquad g_1, g_2 \cdots g_i, g_k \cdots g_l$

as substituições de G correspondentes á identidade em G', ao producto $g_i g_k$ corresponde em G' o producto $1.1 = 1$ e, portanto, $g_i g_k$ é uma substituição de (1).

THEOREMA. — *Se fôr* k *a ordem do subgrupo de* G *correspondente á identidade em* G', *a cada substituição de* G' *correspondem* k *substituições em* G.

Com effeito, sendo $g_1, g_2 \ldots g_k$ (1) as substituições de G correspondentes á identidade em G', e g_n uma substituição de G não pertencente a (1), as substituições

$$g_n g_1, \quad g_n g_2 \cdots g_n g_k$$

de G, e só essas, sam correspondentes á substituição g'_n de g' que corresponde a g_n.

O numero k chama-se *o gráo de meriedria.*

9. As transformadas das substituições de um grupo G, por meio de uma substituição qualquer α, fórmam um grupo que se diz *transformado de* G por meio de α, e que se representa por $G_1 = \alpha^{-1} G \alpha$.

Se α é permutavel com todas as substituições de G, ou pertence a G, α é permutavel com G.

Dois grupos dizem-se *permutaveis* entre si, quando cada um d'elles é permutavel com todas as substituições do outro.

10. Diz-se *invariante* de um grupo G todo o subgrupo permutavel com todas as substituições de G. Um invariante diz-se *maximo,* quando não ha nenhum subgrupo invariante de ordem superior que o contenha.

Sam sempre invariantes de um grupo a identidade e o proprio grupo. Quando não ha outros invariantes, o grupo diz-se *simples.*

THEOREMA. — *Em dois grupos isomorphos meriedricos* G *e* G', *é invariante em* G *o subgrupo* G_1 *correspondente á identidade em* G'.

Com effeito, sendo g_i uma substituição qualquer de G_1, e g_α uma substituição qualquer de G, não pertencente a G_1, á substituição $g_\alpha^{-1} g_i g_\alpha$ de G, corresponde em G' a substituição

$$g'^{-1}_\alpha . 1 . g'_\alpha = 1,$$

sendo g'_α a substituição correspondente a g_α. Logo $g_\alpha^{-1} g_i g_\alpha$ pertence a G_1.

THEOREMA. — *Sendo* m *e* n *as ordens de dois grupos permutaveis* G *e* G', *que admittem um subgrupo commum* G_1 *de ordem* k, *as substituições que se obtêem multiplicando cada substituição de* G *por cada substituição de* G', *formam um grupo de ordem* $\frac{mn}{k}$, *que tem* G, G' *e* G_1 *como subgrupos invariantes.*

Com effeito, sendo g uma substituição de G e g' uma substituição de G', será

$$(gg')(g'g)^{-1} = gg'(gg')^{-1} = (gg'g^{-1})g'^{-1};$$

e tambem

$$(gg')(g'g)^{-1} = g(g'g^{-1}g'^{-1});$$

mas, como $(g'g^{-1}g'^{-1})$ pertence a G, e $(gg'g^{-1})$ pertence a G', a substituição $(gg')(g'g)^{-1}$ pertence a G e a G' e, portanto a G_1.

Representando por $\alpha_1, \alpha_2 \ldots \alpha_k$ as substituições de G_1, será

$$(gg')(g'g)^{-1} = \alpha_i,$$

ou

$$gg' = \alpha_i(g'g). \tag{1}$$

Dos productos gg', em numero de mn, nem todos sam distinctos. Com effeito, de

$$g_\alpha = \alpha_i g_\beta, \quad g'_\alpha = \alpha_i g'_{\beta'},$$

resulta

$$(2)\begin{cases} g_\alpha g_{\alpha'} = \alpha_i g_\beta \cdot \alpha_{i'} g'_{\beta'} = \\ = \alpha_i(g_\beta \alpha_{i'}) g'_{\beta'} = \alpha_i(\alpha_k g_\beta) g'_{\beta'} = (\alpha_i \alpha_k) g_\beta g'_{\beta'} = \alpha_l g_\beta g'_{\beta'}. \end{cases}$$

Dando a l todos os valores desde 1 até k, a β todos os valores desde 1 até m' e a β' todos os valores desde 1 até n', onde m' e n' representam os indices de G_1 respectivamente em G e em G', as substituições distinctas gg' sam em numero de $km'n' = \frac{mn}{k}$.

Todas estas substituições sam effectivamente distinctas, por

que, se fôr

$$\alpha_l g_\beta g'_{\beta'} = \alpha_\lambda g_\gamma g'_{\gamma'},$$

será

$$g'_{\beta'} g'^{-1}_{\gamma'} = (\alpha_l g_\beta)^{-1} \alpha_\lambda g_{\gamma'};$$

e como estas substituições pertencem a G e a G', ellas pertencerám a G_1, e deverá ser $\beta' = \gamma'$, $\beta = \gamma$ e $l = \lambda$.

As substituições gg' formam um grupo Γ, como mostra a relação (1).

Por outro lado, sendo

$$(gg')^{-1} G (gg') = g'^{-1} g^{-1} G g g' = g'^{-1} G g' = G,$$

e, de um modo analogo,

$$(gg')^{-1} G' (gg') = G',$$

vê-se que G e G' sam subgrupos invariantes de Γ; portanto, sê-lo-ha tambem o seu subgrupo commum G_1.

THEOREMA. — *Se* G *e* G' *sam dois subgrupos invariantes maximos de um mesmo grupo* H *e* G_1 *é um subgrupo commum a* G *e* G', *é* G_1 *um invariante maximo de* G *e de* G', *cujo indice em* G' *é egual ao indice de* G *em* H *e cujo indice em* G *é egual ao indice de* G' *em* H.

Por serem G e G' invariantes de um mesmo grupo, elles serám permutaveis. Sejam, respectivamente, m, n e k as ordens de G, G' e G_1. Os productos distinctos gg' formam, pelo theorema anterior, um grupo Γ de ordem $\frac{mn}{k}$, do qual G e G' sam invariantes.

O grupo Γ é subgrupo invariante em H, pois que, sendo h qualquer substituição de H, teremos

$$h^{-1}(gg')h = h^{-1} g h h^{-1} g' h = (h^{-1} g h)(h^{-1} g' h) = g_i g'_i.$$

Mas, come G e G' sam invariantes maximos em H, o grupo Γ coincidirá com H.

O indice de G em H é $\frac{m'}{k}$, egual ao indice de G_1 em G'. O indice de G' em H é egual a $\frac{m}{k}$, indice de G_1 em G.

Basta provar que G_1 é invariante maximo em G e em G'.

Com effeito, seja A um subgrupo invariante de G, contendo

G_1, e a uma substituição de A; será, pela relação (1) do theorema anterior,

$$ag' = g_i^{(1)}(g'a),$$

sendo $g^{(1)}$ uma substituição de G_1. D'onde,

$$g'^{-1}ag' = (g'^{-1}g_i^{(1)}g')\,a = g_k^{(1)}a = a',$$

por ser $g_k^{(1)}$ uma substituição de A.

Portanto, A é permutavel com G', e, por ser permutavel com G, será invariante em H.

Os grupos G' e A satisfazem á hypothese do theorema anterior.

Se fôr kt a ordem de A, os productos da fórma ag' formam um grupo B de ordem $\frac{kt.n}{k} = tn$, que admitte G' e A como invariantes. O grupo B é invariante em H, porque

$$h^{-1}(ag')\,h = (h^{-1}ah)\,(h^{-1}g'h) = a_i g_i'.$$

Como G' é, por hypothese, invariante maximo em H, B coincidirá com H e A com G, o que mostra que G_1 é invariante maximo em G. Do mesmo modo se mostrava que G_1 é invariante maximo em G'.

11. Um dado grupo G póde conter muitos invariantes maximos; seja G_1 um d'elles. Seja egualmente G_2 um invariante maximo de G_1, G_3 um invariante maximo de G_2, etc.

Á successão G, G_1, G_2 ... 1, cujo ultimo termo é sempre a identidade, chama-se uma *serie de composição* do grupo G.

Os indices i_1, i_2 ..., de cada grupo no precedente, sam os *factores de composição* da serie. Da definição resulta que um mesmo grupo póde admittir diversas series de composição; todas ellas, porém, estam relacionadas pela proposição seguinte, devida a JORDAN:

THEOREMA. — *Em duas series de composição do mesmo grupo, os factores de composição sam os mesmos (por uma ordem, em geral, differente).*

O theorema é verdadeiro, evidentemente, para os grupos de ordem 2 e 3, que sam cyclicos, só admittem por subgrupo a identidade e têem, portanto, uma unica serie de composição. Póde verificar-se egualmente para os grupos de ordem 4, quer

sejam ou não cyclicos. Se G_4 é cyclico, será $G_4 = (1 . \alpha . \alpha^2 . \alpha^3)$ e só admitte o subgrupo $G_2 = (1, \alpha^2)$: tem ainda uma unica serie de composição.

Se G_4 não é cyclico, e fôr $G_4 = (1, \alpha_1, \alpha_2, \alpha_3)$, será

$$\alpha_1 \alpha_2 = \alpha_3 = \alpha_2 \alpha_1 ; \quad \alpha_1 \alpha_3 = \alpha_3 \alpha_1 = \alpha_2 .$$

Portanto, α_1 é permutavel com α_2 e α_3 ; como, além disso, α_1 é de indice 2, o grupo $G_2 = (1, \alpha_1)$ será invariante em G_4 ; bem assim, serám invariantes $(1, \alpha_2)$ e $(1, \alpha_3)$.

O grupo G_4 admitte, pois, tres series de composição; mas em todas ellas os factores de composição sam 2, 2.

Vejamos agora que, se o theorema subsiste para todos os grupos de ordem inferior a m, elle é ainda verdadeiro para os grupos de ordem m.

Seja G um grupo de ordem m e sejam

(1) $\quad G, G_1, G_2 \ldots 1$

(2) $\quad G, G'_1, G'_2 \ldots 1$

duas series de composição do grupo G, com os factores de composição

$$e_1, e_2, e_3 \ldots$$
$$e'_1, e'_2, e'_3 \ldots$$

Como G_1 e G'_1 sam invariantes maximos em G, se fôr Γ o seu subgrupo commum, e

$$\Gamma, \Gamma_1, \Gamma_2 \ldots 1$$

uma serie de composição de Γ, serám

(α) $\quad G, G_1, \Gamma, \Gamma_1 \ldots 1$

(β) $\quad G, G'_1, \Gamma, \Gamma_1 \ldots 1$

duas series de composição de G. Os dois primeiros factores de composição das duas series sam, respectivamente

e_1, e'_1 em (α)

e'_1, e_1 em (β).

Os factores de composição das series (α) e (β) sam, pois, os mesmos.

Como suppomos o theorema verdadeiro para qualquer ordem inferior a m, as series (α) e (1) têem os mesmos factores de composição, porque a ordem de G_1 é inferior a m; as series (β) e (2) têem tambem os mesmos factores de composição, porque a ordem de G'_1 é tambem inferior a m.

Portanto, (1) e (2) têem os mesmos factores de composição.

Do theorema de JORDAN resultam os seguintes corollarios:

1.° *Em todas as series de composição do mesmo grupo, o numero de subgrupos é o mesmo.*

2.° *Dois grupos holoedricamente isomorphos têem os mesmos factores de composição.*

3.° *Se* G *e* G' *sam meriedricamente isomorphos, sendo* G_1 *o subgrupo de* G *correspondente á identidade em* G', *os factores de composição de* G *sam todos os de* G' *e todos os de* G_1.

12. Sendo G um grupo de ordem n e G_1 um seu subgrupo de ordem n_1, diz-se que duas substituições g e g' de G sam *equivalentes* em relação ao subgrupo G_1, quando se verifica a relação

$$g' = g_i^{(1)} g,$$

onde $g_i^{(1)}$ é uma das substituições de G_1.

Duas substituições equivalentes a uma terceira (em relação ao mesmo subgrupo) sam equivalentes entre si. Com effeito, sendo

$$g' = g_i^{(1)} g \quad \text{e} \quad g'' = g_k^{(1)} g,$$

será tambem

$$g' = g_i^{(1)} g_k^{(1)-1} g'' = g_l^{(1)} g''.$$

Portanto, as substituições do grupo G dividem-se, em relação a G_1, em um certo numero de *classes de equivalencia:* em cada classe todas as substituições sam equivalentes entre si:

Seja k o numero de classes de equivalencia, e (1) $g_1, g_2 \cdots g_k$ um systema de k substituições, cada uma d'ellas pertencente a uma classe. Multipliquemos as substituições (1) por uma mesma substituição g de G. No systema

$$(2) \qquad g_1 g, \quad g_2 g, \quad \cdots \quad g_k g$$

não ha duas substituições equivalentes. Com effeito se fôsse $g_i g$ equivalente a $g_k g$, seria, em virtude da definição, g_i equivalente a g_k. Portanto, as substituições (2) sam equivalentes, em geral por outra ordem, ás substituições (1); e a multiplicação por g

das substituições (1) corresponde a uma permutação dos indices de (1) (sob o ponto de vista da equivalencia).

A cada multiplicador g corresponde, pois, uma substituição c, effectuada sobre os elementos (1); ao producto gg' corresponde o producto cc', e ao grupo G corresponde um grupo C de substituições sobre os elementos (1), representantes das classes de equivalencia.

O grupo C é isomorpho com G; diz-se *complementar* á direita, em relação ao subgrupo G_1 e representa-se pelo symbolo $C = \frac{G}{G_1}$. De um modo analogo se podia construir o grupo complementar á esquerda: bastava ter multiplicado á esquerda os elementos (1) para obter os elementos (2).

Sendo k o indice de G_1 em G, e g uma substituição qualquer commum a todos os subgrupos

$$G_1,\ g_2^{-1} G_1 g_2,\ \ldots\ g_k^{-1} G_1 g_k,$$

transformados de G_1 por meio das substituições de G, será

$$g = g_i^{-1} g^{(i)} g_i$$

para todos os valores de i desde 1 até k. Portanto, é $g_i g = g^{(i)} g_i$, ou $g_i g$ equivalente a g_i, para os valores 1, 2 ... k dados a i. Ao multiplicador g corresponde, pois, a identidade em C.

Á identidade no grupo complementar corresponde em G *o subgrupo commum aos transformados de* G_1 *por meio das substituições de* G.

Se G_1 é invariante em G, os transformados coincidem, e *á identidade no grupo complementar corresponde o subgrupo* G_1 *de* G.

13. Posto isto, podemos dar outra fórma ao theorema de JORDAN.

Sendo

$$G,\ G_1,\ G_2\ \ldots\ 1$$

uma serie de composição de G, os grupos complementares

$$C_1 = \frac{G}{G_1},\quad C_2 = \frac{G_1}{G_2}\ \ldots$$

têem uma ordem egual ao respectivo factor de composição.

Chamando aos grupos C grupos *factoriaes*, o theorema de JORDAN póde enunciar-se dizendo que

Em duas series de composição do mesmo grupo, as ordens dos grupos factoriaes sam as mesmas. Os grupos factoriaes sam grupos simples, porque, se C_1, por exemplo, admittisse um invariante, o subgrupo correspondente de G seria invariante e conteria G_1, que corresponde á identidade em C_1. Ora isso é impossivel, por ser G_1 invariante maximo em G.

THEOREMA DE HÖLDER. — *Se*

(1) $C_1, C_2, \ldots$

(2) $C_1', C_2', \ldots$

sam os grupos factoriaes de duas series de composição do mesmo grupo, cada um dos grupos (1) *é isomorpho holoedrico com um dos grupos* (2).

Seja G o grupo dado e

(α) $G, G_1, G_2, \ldots 1$

(β) $G, G_1', G_2', \ldots 1$

as duas series de composição a que correspondem respectivamente os grupos factoriaes (1) e (2).

Seja Γ o subgrupo commum a G_1 e G_1'. Se $g_2, g_3 \ldots g_k$ é um systema de representantes das classes de equivalencia de G_1, em relação a Γ, e $\gamma_1, \gamma_2, \ldots \gamma_l$ sam as substituições de Γ, as substituições de G sam da fórma $\gamma_\alpha g_i$. Do mesmo modo, sendo $g_2', g_3' \ldots g_k'$, um systema de representantes das classes de equivalencia de G_1', em relação a Γ, as substituições de G_1' sam da fórma $\gamma_\alpha g_i'$. Mas as substituições de G sam da forma $\gamma_\alpha g_i g_i'$; portanto, $g_2, g_3 \ldots g_i$ é tambem um systema de representantes das classes de equivalencia de G em relação a G_1'.

Do mesmo modo, $g_2', \ldots g_{k'}$ é um systema de representantes das classes de equivalencia de G em relação a G_1. Isto é, os dois grupos complementares $\frac{G}{G_1'}$ e $\frac{G_1}{\Gamma}$ sam holoedricamente isomorphos, bem como os grupos $\frac{G}{G_1}$ e $\frac{G_1'}{\Gamma}$.

Sendo assim, demonstra-se, como no theorema de JORDAN, que, se o principio subsiste para os grupos de ordem inferior a m, elle é ainda verdadeiro para os grupos de ordem m. Para os

grupos de ordens 2, 3, 4, o theorema é facilmente justificavel: é, portanto, geral.

Numa serie de composição

$$G,\ G_1\ \ldots\ 1,$$

o grupo G_i é invariante maximo em G_{i-1}, mas póde não ser invariante em G. Se todos os termos da serie sam invariantes em G, a serie diz-se *principal*, e os seus factores de composição dizem-se *factores principaes*.

14. 1.º THEOREMA DE SYLOW. — *Se a ordem* m *de um grupo* G *é divisivel por* p^n, *sendo* p *um numero primo, o grupo* G *admitte um subgrupo de ordem* p^n.

Como em todos os grupos figura a identidade, basta demonstrar que, se um grupo, cuja ordem é um multiplo de p^{n-1}, admitte um subgrupo de ordem p^{n-1}, um grupo, cuja ordem é um multiplo de p^n, admitte tambem um subgrupo de ordem p^n.

As substituições de G, que sam permutaveis com todas as substituições do grupo, formam em G um subgrupo, contendo, pelo menos, a identidade. Seja G_1 esse grupo, chamado *commutativo*, e $\gamma_1, \gamma_2 \ldots \gamma_k$ as suas substituições.

1.º Supponhamos, em primeiro logar, que k é multiplo de p.

Nesse caso existe em G_1 uma substituição de periodo p. Com effeito, sendo $i_1, i_2 \ldots i_k$ os periodos das substituições γ de G_1, se formarmos todos os productos da fórma

$$\gamma_1^{\alpha} \cdot \gamma_2^{\beta} \cdots \gamma_k^{\lambda},$$

onde α toma todos os valores desde 1 até i_1, β todos os valores desde 1 até i_2, etc.; esses productos sam em numero de $i_1 . i_2 \ldots i_k$; sam as substituições do grupo commutativo, cada uma repetida o mesmo numero r de vezes.

Portanto

$$i_1 . i_2 \ \ldots\ i_k = rk$$

e um, pelo menos, dos factores i será multiplo de p. Se fôr i_h multiplo de p, a substituição $\gamma = \gamma_h^{\frac{i_h}{p}}$ é de periodo p, como se queria demonstrar.

Consideremos o grupo cyclico Γ sobre a substituição γ, o qual é de ordem p, e o grupo complementar $\frac{G}{\Gamma} = C$. Este grupo

C é de ordem $\frac{m}{p}$, multiplo de p^{n-1} e admitte, por hypothese, um subgrupo C_1, de ordem p^{n-1}. Mas como C é meriedricamente isomorpho com G, sendo p o gráo de meriedria, o subgrupo de G correspondente a C_1 é de ordem p^n, e o theorema fica demonstrado.

2.° Supponhamos agora que k não é multiplo de p.

Duas substituições g e g' de G dizem-se *affins*, quando ha uma substituição no grupo que transforma g em g'. Duas substituições affins de uma terceira sam affins entre si. Podemos, pois, distribuir as substituições de G em *classes de affinidade*, cada uma d'ellas formada por todas as substituições affins entre si duas a duas.

Uma substituição do grupo commutativo Γ não é affim de nenhuma outra substituição de G.

Seja

$$\gamma_1, \quad \gamma_2 \quad \ldots \quad \gamma_k, \quad g_1, \quad g_2, \quad \ldots \quad g_t$$

um systema completo de representantes das classes de affinidade.

Supponhamos que ha em G r_1 substituições affins de g_1, r_2 substituições affins de g_2, etc.

Será

$$m = k + r_1 + r_2 + \ldots + r_t.$$

As substituições de G, permutaveis com g_i, formam em G um subgrupo G_i de ordem m_i. É facil ver que $\frac{m}{m_i} = r_i$. Com effeito, havendo m_i substituições em G que transformam g_i em si mesma, haverá $\frac{m}{m_i}$ substituições que transformam g_i numa substituição differente; e esse numero $\frac{m}{m_i}$ é, por definição, o numero de substituições affins de g_i.

Será, pois,

$$m = k + \frac{m}{m_1} + \ldots + \frac{m}{m_i} + \ldots + \frac{m}{m_t}.$$

Como k não é multiplo de p, um, pelo menos, dos numeros $\frac{m}{m_i}$ não será multiplo de p; portanto, m_i é multiplo de p^n.

Vê-se, pois, que se G não contivesse um subgrupo de ordem p^n, haveria, comtudo, em G um subgrupo G_i, cuja ordem m_i é divisivel por p^n. G_i não conteria tambem nenhum subgrupo de ordem p^n e, comtudo, deveria existir em G_i um subgrupo G_i'

..

cuja ordem m_i' seria divisivel por p^n (como se via por um raciocinio analogo ao precedente).

Teriamos assim uma successão illimitada m_i, m_i' ... de divisores decrescentes de m, todos elles multiplos de p^n, o que é absurdo. Portanto, G deverá conter um subgrupo de ordem p^n.

D'este theorema resulta, como corollario, que, *se* p *é um dos divisores primos da ordem* m *de um grupo* G, *ha sempre em* G *uma substituição de periodo* p.

15. 2.º THEOREMA DE SYLOW. — *Se* p^n *é a mais elevada potencia de* p *contida na ordem* m *de um grupo* G, *todos os subgrupos de ordem* p^n *contidos em* G *sam transformados uns dos outros por meio das substituições de* G. *O numero d'esses subgrupos é um multiplo de* p *mais* 1.

Em G existirá, em virtude do primeiro theorema, um subgrupo de ordem p^n. Seja elle G_1 e sejam

$$(1) \qquad G_1, \quad G_2 \quad \ldots \quad G_k$$

todos os seus k transformados por meio das substituições de G, os quaes sam de ordem p^n e subgrupos de G.

As substituições de G, que transformam G_1 em si mesmo, formam um subgrupo K do qual G_1 é invariante. Sendo m a ordem de G e m' a ordem de K, será $m = \alpha p^n$ e $m' = \beta p^n$; os factores α e β não sam multiplos de p e o quociente $\frac{\alpha}{\beta} = \frac{m}{m'}$ é um numero inteiro.

Distribuindo as substituições de G em relação a K no quadro

$$G \begin{cases} k_1, & k_2 & \ldots & k_{m'} & (K \\ k_1 g_2 & k_2 g_2 & \ldots & k_{m'} g_2 & \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ k_1 g_{\frac{m}{m'}} & k_2 g_{\frac{m}{m'}} & \ldots & k_{m'} g_{\frac{m}{m'}}, & \end{cases}$$

se fôr

$$g_i^{-1} G_1 g_i = G_i,$$

será

$$g_i^{-1} k_i^{-1} G_1 k_i g_i = g_i^{-1} G_1 g_i = G_i,$$

por ser G_1 invariante em K; o que mostra que $\frac{m}{m'} = k$. Portanto:

O numero de grupos transformados de G_1 *é egual ao indice de* K *em* G.

Demonstremos agora que o inteiro k é um multiplo de p mais 1.

Dois grupos G_2 e G_3, da mesma ordem, dizem-se *affins* em relação a um mesmo grupo G_1, quando ha em G_1 uma substituição que transforma G_2 em G_3. Dois grupos affins de um terceiro sam affins entre si.

Distribuamos os grupos (1) em classes de grupos affins em relação a G_1. Em nenhuma classe, a não ser naquella a que pertence G_1, figura um unico grupo. Para verificar que assim é, mostremos, em primeiro logar, que nenhuma substituição de K, não pertencente a G_1, póde ter por periodo uma potencia de p. Com effeito, o grupo $\frac{K}{G_1}$, de ordem β, não póde conter nenhuma substituição de periodo potencia de p; mas como $\frac{K}{G_1}$ é isomorpho meriedrico de gráo p^n com K, se uma substituição k_i de K, não pertencente a G_1, tivesse por periodo uma potencia de p, a substituição correspondente a k_i em $\frac{K}{G_1}$ não seria a identidade, e teria por periodo uma potencia de p, o que é impossivel.

Posto isto, se na classe de affinidade a que pertence

$$G_i = g_i^{-1} G_1 g_i,$$

não existisse nenhum outro grupo, seria, para qualquer substituição γ de G_1,

$$\gamma^{-1} G_i \gamma = G_i,$$

ou

$$\gamma^{-1} g_i^{-1} G_1 g_i \gamma = g_i^{-1} G_1 g_i,$$

ou ainda

$$(g_i \gamma g_i^{-1})^{-1} G_1 (g_i \gamma g_i^{-1}) = G_1;$$

e $g_i \gamma g_i^{-1}$ seria uma substituição de K, pertencente a G_1, por ter por periodo uma potencia de p. Portanto, g_i pertenceria a K, o que não é exacto.

Na classe a que pertence G_i ha, pois, mais de um grupo: vamos ver que o seu numero é uma potencia de p.

Chamando G_1' ao subgrupo de G_1 formado por todas as substituições d'este grupo que sam permutaveis com G_i, vê-se, como acima, que o indice de G_1' em G_1 é egual ao numero de grupos pertencentes á classe de affinidade de G_i; e esse indice é uma potencia de p.

O numero total de grupos transformados de G_1 é pois

$$k = 1 + p^{\alpha} + p^{\beta} + p^{\gamma} + \ldots$$

e, portanto, egual a um multiplo de p mais 1.

Resta finalmente demonstrar que, além dos k subgrupos transformados de G_1, não ha em G mais nenhum subgrupo de ordem p^n.

Seja C um subgrupo G de ordem p^i, com $i \leqq n$.

Distribuindo os grupos (1) em classes de grupos affins em relação a C, como a ordem de C é uma potencia de p, em cada classe haverá um numero de grupos egual a uma potencia de p. Mas como k é egual a um multiplo de p mais 1, haverá uma classe com um unico grupo: isto é, haverá entre os grupos (1), um grupo G_i permutavel com todas as substituições de C. C será, como acima se viu, contido em G_i como subgrupo.

Fazendo $i = n$ fica demonstrado o theorema.

16. Um grupo diz-se *resoluvel* quando os seus factores de composição sam numeros primos.

a) *É resoluvel,* (em virtude dos theoremas precedentes), *todo o grupo cuja ordem é potencia de um numero primo* p.

Todos os seus factores de composição sam eguaes a p.

Com effeito, esses factores de composição deverám ser potencias de *p,* e, como sam ordens de grupos simples (os grupos factoriaes), não podem ser potencias de gráo superior a 1.

b) *É resoluvel todo o grupo de ordem egual ao producto de dois numeros primos* p *e* p'.

Supponhamos $p > p'$.

No grupo G haverá um subgrupo G_1 de ordem p e só um, porque o numero dos subgrupos transformados de G_1 deve ser factor de p' e egual a um multiplo de p mais 1.

Portanto, G_1 é invariante maximo e

$$G, \quad G_1, \quad 1$$

é a serie de composição de G, cujos factores sam p e p'.

Ha ainda outros grupos que á primeira vista se conhece serem resoluveis. A importancia e o nome d'estes grupos resulta do papel que desempenham na theoria das equações algebricas, como veremos.

III

Grupos abelianos

17. Estudaremos agora algumas cathegorias particulares de grupos de que teremos de fazer uso na exposição da theoria das equações algebricas, segundo GALOIS.

Entre essas cathegorias de grupos, a mais simples é a dos grupos *abelianos* que *sam aquelles cujas substituições sam permutaveis duas a duas.*

As principaes propriedades d'estes grupos sam as seguintes:

1.ª *O menor multiplo commum dos periodos das substituições de um producto é multiplo do periodo do producto.*

Com effeito, por ser

$$(gg')^k = g^k g'^k,$$

se k fôr o menor multiplo commum dos periodos de g e g', será

$$(gg')^k = 1,$$

e k multiplo do periodo de gg'.

O theorema extende-se evidentemente a qualquer numero de factores.

COROLLARIO. — *Se os periodos dos factores sam primos entre si dois a dois, o periodo do producto é o producto dos periodos dos factores.*

2.ª *Todo o subgrupo dum grupo abeliano é invariante.* É uma consequencia immediata da definição.

3.ª *Se fôr*

$$m = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

a ordem de um grupo abeliano G, *decomposta nos seus factores*

primos, o grupo G *é um producto de* k *grupos abelianos*

$$G_1, \quad G_2 \quad \ldots \quad G_k$$

respectivamente de ordens

$$p_1^{n_1}, \quad p_2^{n_2} \cdots p_k^{n_k}.$$

Com effeito, G admitte um subgrupo G_1 de ordem $p_1^{n_1}$, que, por ser invariante, é unico d'essa ordem. Bem assim, ha em G um unico subgrupo G_2 de ordem $p_2^{n_2}$ etc.

Formando todos os productos possiveis da fórma

$$(1) \qquad g_1 \cdot g_2 \cdots g_k,$$

onde g_1 é uma substituição qualquer de G_1, g_2 uma substituição qualquer de G_2, etc., estes productos sam todos distinctos, porque, se fôsse

$$g_1 \cdot g_2 \cdots g_k = g_1' \cdot g_2' \cdots g_k'$$

teriamos

$$g_1 g_1'^{-1} = (g_2' g_2^{-1}) \cdots (g_k' g_k^{-1});$$

e como o periodo do primeiro membro é uma potencia de p_1, e o periodo do segundo membro é um producto de potencias de $p_2, p_3 \cdots p_k$, deverá ser

$$g_1 = g_1'; \quad g_2 = g_2' \cdots$$

Os productos 1) sam, pois, em numero de m e sam todas as substituições de G, o que demonstra o theorema.

COROLLARIO 1.° — *Um grupo abeliano tem subgrupos de todas as ordens que sam divisores da ordem do grupo.*

COROLLARIO 2.° — *Todo o grupo abeliano é resoluvel.*

4.ª *Os periodos de todas as substituições de um grupo abeliano sam factores do maior d'elles.*

Seja g a substituição de maior periodo k_1 e supponhamos que o periodo k_2 de g' não era divisor de k_1. Haveria em k_2 um factor primo p com expoente maior que em k_1; seria

$$k_1 = \alpha p^{n_1} \qquad \text{e} \qquad k_2 = \beta p^{n_2}$$

com $n_2 > n_1$.

O periodo de $g^{p^{n_1}}$ será α e o de g'^{β} será p^{n_2}.

Como α e p^{n_2} sam primos, o producto $g^{p^{n_1}} . g'^{\beta}$ teria por periodo $\alpha p^{n_2} > k_1$, o que é contra a hypothese.

Chama-se *periodo relativo* de uma substituição g de um grupo abeliano G, em relação a um seu subgrupo G_1, ao menor expoente k a que é necessario elevar g para que g^k pertença a G_1.

O periodo relativo de uma substituição g é manifestamente egual ao periodo absoluto da sua correspondente no grupo complementar $\frac{G}{G_1}$.

O periodo relativo é, por isso, factor do periodo absoluto.

Duas substituições equivalentes em relação a G_1 *têem o mesmo periodo relativo.*

18. Diz-se que k substituições

$$(1) \qquad g_1, \quad g_2 \ldots g_k$$

de um grupo abeliano G de ordem m sam *independentes,* quando nenhum producto de potencias das substituições (1) póde ser a identidade, sem que cada um dos factores o seja; isto é, sem que os expoentes sejam multiplos dos respectivos periodos.

Sendo $n_1, n_2 \ldots n_k$ os periodos das substituições (1), se no producto

$$g_1^{\alpha} \cdot g_2^{\beta} \ldots g_k^{\gamma}$$

dermos a cada expoente todos os valores inteiros desde 1 respectivamente até

$$n_1 - 1, \quad n_2 - 1, \quad \ldots \quad n_k - 1,$$

obtemos manifestamente um subgrupo G_1 de G de ordem

$$n_1 . n_2 \ldots n_k.$$

Diz-se que as substituições independentes $g_1 g_2 \ldots g_k$ formam uma *base* do grupo abeliano.

Vamos ver como se póde sempre construir uma base de um grupo abeliano.

Sendo g_1 a substituição de maximo periodo k_1 e k_2 o maior dos periodos relativos das substituições de G, em relação ao

subgrupo cyclico sobre g_1, se houver em G uma substituição de *periodo absoluto* k_2, ella será independente de g_1.

Essa substituição existe, porque, sendo g' uma substituição de periodo relativo k_2, tal que

$$g'^{k_2} = g_1^i \, (i \leqq k_1 - 1),$$

teremos

$$g'^{k_1} = g_1^{i\frac{k_1}{k_2}} = 1,$$

por ser k_1 multiplo de todos os periodos e, portanto, $g'^{k_1} = 1$.

Será, pois, $\frac{i}{k_2}$ inteiro, e a substituição

$$g_2 = g' g^{-\frac{i}{k_2}}$$

tem por periodo absoluto k_2, visto que

$$g_2^{k_2} = g'^{k_2} \cdot g_1^{-i} = g_1^i \cdot g_1^{-i} = 1.$$

Com a base $\{ g_1, g_2 \}$ podemos construir um subgrupo G_1 de G de ordem $k_1 . k_2$. Applicando a esse subgrupo um raciocinio analogo ao que empregámos com o grupo cyclico sobre g_1, mostra-se a existencia de uma substituição g_3, independente de g_1 e g_2.

A base $\{ g_1, g_2 \ldots g_i \}$ que assim se constroe, para o grupo abeliano G de ordem m, é tal que os periodos k_1, $k_2 \ldots k_i$ d'estas substituições satisfazem á relação

$$k_1 . k_2 \ldots k_i = m,$$

sendo cada um d'elles multiplo de todos os seguintes, e sendo k_h o maior periodo relativo das substituições de G, em relação ao subgrupo gerado pela base $\{ g_1, g_2 \ldots g_{h-1} \}$.

19. Podem construir-se, por outros processos, bases diversas de um grupo abeliano; mesmo pelo processo indicado, podemos ser conduzidos a bases differentes.

Póde demonstrar-se, porém, (e essa é a principal importancia d'este modo de geração das bases) que *todas as bases geradas pelo processo indicado têem o mesmo numero de substituições com os mesmos periodos.*

Aos periodos das substituições de qualquer base de um grupo abeliano dá-se, por isso, o nome de *invariantes* do grupo.

Se

$$\{ g_1, g_2 \dots g_k \} \quad \text{e} \quad \{ \gamma_1, \gamma_2 \dots \gamma_k \}$$

sam duas bases;

$$n_1, n_2 \dots n_k: \quad \text{e} \quad \nu_1, \nu_2 \dots \nu_k,$$

os periodos das respectivas substituições, será $n_1 = \nu_1$ (o maior periodo das substituições de G).

Basta, pois, demonstrar que, se fôr

$$n_1 = \nu_1, \quad n_2 = \nu_2 \dots, \quad n_{l-1} = \nu_{l-1},$$

será tambem $n_l = \nu_l$.

Representando por α as substituições do grupo que sam potencias n_l de outras substituições do grupo, essas substituições α formam um subgrupo. Se fôr $\alpha = g^{n_l}$,
será

$$\alpha = g_1^{t_1 n_l} \cdot g_2^{t_2 n_l} \dots g_k^{t_k n_l}$$

sendo

$$g_1^{t_1} \cdot g_2^{t_2} \dots g_k^{t_k}$$

a expressão de g nas substituições da primeira base. Mas, como

$$g_l^{n_l} = g_{l+1}^{n_l} = \dots = 1$$

será

$$\alpha = g_1^{t_1 n_l} \cdot g_2^{t_2 n_l} \dots g_{l-1}^{t_{l-1} n_l}. \tag{1}$$

Ás substituições α podemos ainda dar a fórma

$$\gamma_1^{t_1 n_l} \cdot \gamma_2^{t_2 n_l} \dots \gamma_{l-1}^{t_{l-1} n_l},$$

seguindo um raciocinio analogo.

Como uma das substituições α é $\gamma_l^{n_l}$, deverá ser $\gamma_l^{n_l} = 1$, por ser γ_l independente de $\gamma_1, \gamma_2 \dots \gamma_{l-1}$. Portanto, o periodo ν_l de γ_l divide n_l.

Como se provava de um modo identico, que n_l divide ν_l, será

$$n_l = \nu_l$$

e o theorema fica demonstrado.

THEOREMA. — *Se* $n_1, n_2 \ldots n_k$ *fôrem* k *numeros inteiros taes que cada um d'elles é factor do precedente, podemos sempre construir um grupo abeliano que os tenha como invariantes.*

Com effeito, dadas as $n_1 + n_2 + \ldots + n_k$ lettras:

$$\alpha_1, \alpha_2 \ldots \alpha_{n_1}; \quad \beta_1, \beta_2 \ldots \beta_{n_2}; \quad \ldots \lambda_1, \lambda_2 \ldots \lambda_{n_k};$$

as substituições

$$g_1 = (\alpha_1 . \alpha_2 \ldots \alpha_{n_1}), \quad g_2 = (\beta_1 . \beta_2 \ldots \beta_{n_2}),$$
$$\ldots g_k = (\lambda_1 . \lambda_2 \ldots \lambda_{n_k})$$

sam generatrizes de um grupo abeliano de base $\{ g_1, g_2 \ldots g_k \}$ que tem os numeros dados como invariantes.

IV

Grupo metacyclico. — Grupo linear total. Grupo modular

20. Seja G um grupo resoluvel, transitivo sobre m lettras, sendo m um numero primo, e

$$(1) \qquad G, G_1 \ldots G_{p-1}, 1$$

uma serie de composição de G.

Todos os grupos de (1) *sam transitivos sobre* m *lettras*. Basta mostrar que G_k é transitivo se G_{k-1} o fôr.

Supponhamos, com effeito, que G_k não é transitivo e seja

$$(2) \qquad \alpha_1, \alpha_2 \ldots \alpha_i$$

um dos seus systemas de transitividade.

Por ser G_{k-1} transitivo, haverá uma substituição S_1 em G_{k-1} que troca α_i em β_i, sendo β_i uma lettra não pertencente ao systema (2).

No systema $S_1^{-1} G_k S_1$ constituem um systema de transitividade as lettras que S_1 substitue pelas do systema (2).

Mas $S_1^{-1} G_k S_1 = G_k$ e, portanto, o systema de transitividade a que pertence β_i tem, pelo menos, i lettras.

Essas lettras sam i e não mais, porque o raciocinio subsiste trocando α_i por β_i. Logo, todos os systemas de transitividade em G_k têem i lettras e $i = 1$, ou $i = m$, visto que m é primo.

Portanto, G_k ou é a identidade ou é transitivo sobre m lettras.

O subgrupo G_{p-1}, transitivo sobre m lettras, devendo ter uma ordem multipla de m e que seja um numero primo, por ser um dos factores de composição, *será formado pelas* m *potencias de uma substituição cyclica* S; *será o grupo cyclico sobre* S.

Se G_{p-1} é invariante em G_k, tambem o será em G_{k-1}. Com effeito, por ser a ordem de G_k divisor de $m!$, essa ordem contem m á primeira potencia e G_k não contem nenhum outro subgrupo de ordem m além de G_{p-1}. (Theorema de SYLOW).

Portanto, chamando S a uma substituição qualquer de G_{k-1}, e sendo $S^{-1} G_k S = G_k$, será

$$S^{-1} G_{p-1} S = G_{p-1},$$

e G_{p-1} será invariante em G_{k-1}.

Como G_{p-1} é invariante em G_{p-2}, sê-lo-ha em todos os grupos de 1).

O maior grupo M resoluvel, transitivo sobre m lettras, que contenha G_{p-1} como invariante, terá, pois, como subgrupos transitivos todos os grupos transitivos resoluveis sobre m lettras. A esse grupo M dá-se o nome de *grupo metacyclico*.

21. Vamos determinar a ordem do grupo metacyclico sobre m lettras.

Seja

$$G_{p-1} = (1, \alpha, \alpha^2, \ldots \alpha^{m-1})$$

e

$$a_0, \quad a_1, \quad a_2 \ldots a_{m-1}$$

as m lettras sobre as quaes operam as substituições do grupo cyclico G_{p-1}; m é, por hypothese, um numero primo.

Por ser G_{p-1} invariante no grupo metacyclico, toda a substituição g_k do grupo metacyclico transforma α numa sua potencia

$$g_k^{-1} \alpha g_k = \alpha^k. \tag{1}$$

Sendo k e k' dois inteiros positivos inferiores a m, ás duas substituições distinctas α^k e $\alpha^{k'}$ do grupo cyclico G_{p-1} correspondem em (1) substituições diversas g_k e $g_{k'}$ do grupo metacyclico. Para os $m-1$ valores de k teremos, pois, $m-1$ substituições g_k. Mas, se a substituição g pertence ao grupo metacyclico, pertencerám ao mesmo grupo as $m-1$ substituições

$$\alpha g, \quad \alpha^2 g, \quad \ldots \alpha^{m-1} g,$$

todas distinctas, pelo que acima dissemos. Portanto, *a ordem do grupo metacyclico é* $m(m-1)$.

As $m-1$ *substituições* g_k *formam um subgrupo em* M.

Com effeito, distribuindo convenientemente os indices dos elementos

$$a_0, \quad a_1 \quad \ldots \quad a_{m-1},$$

sobre que actuam as substituições de M, a substituição cyclica α póde escrever-se

$$\alpha = (a_0\, a_1\, a_2 \ldots a_{m-1}).$$

Cada uma das substituições cyclicas α^k póde tambem escrever-se *de modo que o respectivo cyclo comece por* a_0. Portanto, as substituições g_k, deixando fixo o elemento a_0, formam em M um subgrupo.

O subgrupo formado pelas substituições g_k *contem as* $m-1$ *potencias distinctas de uma mesma substituição cyclica sobre os* $m-1$ *elementos*

$$a_1, \quad a_2 \quad \ldots \quad a_{m-1}.$$

22. Representemos por (ik) os indices tomados em relação ao modulo (m).

Será

$$\alpha = (a_0 . a_1 \ldots a_{m-1})$$

$$\alpha_k = [a_0\ a_{(k)}\ a_{(2k)} \ldots a_{((m-1)k)}].$$

A substituição g_k, que transforma α em α_k, é a substituição cyclica

$$\beta = (a_1 . a_k\, a_{k^2} \ldots a_{k^{m-2}}),$$

e o grupo das substituições g_k é formado pelas potencias de β.

Vemos, pois, que todas as substituições do grupo metacyclico, que sam da fórma $\alpha^i g_k$, se obtêem a partir das duas substituições α e β, e sam da fórma

$$\alpha^i \beta^l,$$

onde i toma todos os valores inteiros positivos desde 0 até $m-1$, e l todos os valores inteiros positivos desde 0 até $m-2$.

Continuando a representar abreviadamente por $l = (i)$ a congruencia $l = i$ (mod. m), em relação ao modulo m, vejamos qual é a modificação exercida sobre os indices dos elementos a_0, a_1 $\ldots$ a_{m-1} pelas substituições do grupo metacyclico.

O effeito da substituição

$$\alpha^i = [a_0 . a_{(i)}\, a_{(2i)} \ \ldots \ a_{((m-1)\, i)}]$$

é, coms vimos, augmentar em (i) os indices; o effeito da substituição

$$\beta = (a_1\, a_k\, a_{k^2} \ \ldots \ a_{k^{m-2}})$$

sobre α é multiplicar os indices por k. Portanto, o effeito de β^l será multiplicar todos os indices por k^l.

Logo, por effeito da substituição $\alpha^i \beta^l$ do grupo metacyclico, cada indice t se transforma em

$$t' = [(t+i)\, k^l] = (tk^l + ik^l)$$

ou

$$t' = (at + b),$$

$$(\text{pondo } k^l = a \quad \text{e} \quad ik^l = b),$$

onde

$$a = (1,\ 2,\ \ldots\ m-1)$$

$$b = (0,\ 1,\ 2,\ \ldots\ m-1).$$

Quando fôr $a = k^l = 1$, teremos as substituições do grupo cyclico G_{p-1}, as quaes sam de periodo m. As outras substituições do grupo metacyclico têem um periodo divisor de $m-1$.

23. *O grupo metacyclico é duplamente transitivo.*

Com effeito, se fôr

$$a = a' - a'' \quad \text{e} \quad b = a'',$$

mostra a fórmula

$$t' = [(a' - a'')\, t + a'']$$

que os indices 0 e 1 se mudam respectivamente em a' e a''.

Representaremos o grupo metacyclico simplesmente pela notação $t' = (at + b)$, chamando a a o *multiplicador* da substituição.

Como a substituição α é par e β é impar, as substituições $\alpha^i \beta^l$ do grupo metacyclico, em que l é par, sam substituições pares. Ellas formam um subgrupo, chamado *semimetacyclico*.

Além d'este subgrupo, tem o grupo metacyclico duas cate-

gorias de subgrupos de particular importancia na theoria de GALOIS. Vejamos quaes ellas sam.

Se fôrem a_i e a_k os multiplicadores de duas substituições g_i e g_k do grupo metacyclico, é $a_i a_k$ o multiplicador do producto $g_i g_k$. Com effeito, a primeira substituição muda o indice t em

$$t' = (a_i t + b_i),$$

e a segunda muda t' em

$$t'' = [a_k(a_i t + b_i) + b_k] = a_i a_k t + a_k b_i + b_k.$$

Posto isto, seja M_1 um subgrupo do grupo metacyclico M. Se fôrem

(1) $$a_1, \quad a_2 \ldots a_k$$

todos os multiplicadores que figuram nas substituições de M_1, os productos

$$a_1 a_i, \quad a_2 a_i \ldots a_k a_i,$$

de todos esses multiplicadores por um d'elles, sam, em virtude da proposição anterior, os mesmos numeros (1), em geral, por outra ordem. Portanto, a cada multiplicador corresponde uma substituição sobre os elementos (1), e essas substituições formam um grupo de ordem k.

24. *O grupo dos multiplicadores é cyclico.*

Com effeito, seja γ o periodo da substituição correspondente ao multiplicador a_i. Será

$$a_i^{\gamma} = 1 \pmod{m}.$$

Como γ é factor de k, todos os multiplicadores $a_1, a_2 \ldots a_k$ de M_1 sam as raizes da congruencia binomia

$$x^k = 1 \pmod{m}.$$

Todos elles sam, pois, potencias de um, a_i, e o grupo das substituições correspondentes é cyclico.

No subgrupo M_1 considerado póde haver uma ou mais substituições distinctas correspondentes a cada multiplicador.

1.° Supponhamos que ha em M_1 duas substituições com o multiplicador a_i:

$$t' = (a_i t + b_i) \quad \text{e} \quad t' = (a_i t + b_k).$$

Haverá em M_1 a substituição

$$(1) \qquad t' = [t + (b_k - b_i)]$$

que resulta de multiplicar a inversa da primeira pela segunda; e como $b_k - b_i \gtrless 0$, a substituição (1) pertence ao grupo cyclico G_{p-1}, que será um subgrupo de M_1.

Ao grupo M_1 pertencerám todas as substituições que resultam das do grupo cyclico G_{p-1}, por meio dos multiplicadores $a_1, a_2 \ldots a_k$; havendo egual numero de substituições para cada multiplicador. *O grupo* M_1 *será de ordem* mk.

2.° Se em M_1 não houver mais de uma substituição de multiplicador a_i, haverá, em virtude do que fica exposto, uma substituição por cada multiplicador. *O grupo* M_1 *é de ordem* k.

O numero k é sempre factor de $m-1$.

Os subgrupos da primeira categoria sam de ordem superior a $m-1$. *Sam todos os grupos transitivos resoluveis sobre* m *elementos, contendo como invariante o grupo cyclico; e sam todos elles invariantes do grupo metacyclico.*

Os numeros

$$m(m-1), \quad \frac{m(m-1)}{m_1}, \quad \frac{m(m-1)}{m_1 . m_2} \ldots m,$$

onde $m_1, m_2 \ldots$ sam os divisores primos de $m-1$, sam ordens de grupos transitivos resoluveis, e os seus quocientes consecutivos $m_1, m_2 \ldots$ sam numeros primos.

Os grupos que têem essas ordens formam, pela propriedade da invariancia que os caracterisa, uma serie de composição do grupo metacyclico.

Portanto, *o grupo metacyclico é resoluvel, e* $m_1, m_2 \ldots$ *sam os seus factores de composição.*

Os subgrupos de ordem k, da segunda categoria, sam cyclicos, como holoedricamente isomorphos do grupo dos multiplicadores

É fundamental a importancia do grupo metacyclico e dos seus subgrupos na resolução algebrica das equações.

25. Supponhamos agora que sobre os indices t de $m+1$

elementos a_∞, a_0, $a_1 \ldots a_{m-1}$, onde m é ainda um numero primo, se effectuam substituições lineares fraccionarias da fórma

$$(1) \qquad t' \equiv \frac{pt+q}{p't+q'} \pmod{m},$$

sendo p, p', q, q' numeros inteiros, positivos ou negativos, satisfazendo á relação

$$pq'-p'q \gtrless 0 \pmod{m}.$$

O indice ∞ representa as substituições para as quaes

$$p'=q'=0.$$

Sendo k um numero inteiro, que não seja multiplo de m, a substituição

$$t' \equiv \frac{kpt+kq}{kp't+kq'} \pmod{m}$$

é identica a (1).

Inversamente, se as duas substituições

$$t' = \frac{pt+q}{pt'+q'} \pmod{m}$$

e

$$t' \equiv \frac{p_1 t+q_1}{p_1' t+q_1'} \pmod{m}$$

sam identicas, ellas têem coefficientes proporcionaes (mod. m).

Vamos vêr que as substituições (1) formam grupo e determinar a ordem d'esse grupo.

Sendo

$$t'=\left(\frac{pt+q}{p't+q'}\right) \quad \text{e} \quad t_1=\left(\frac{p_1 t'+q_1}{p_1' t'+q_1'}\right)$$

é

$$(2) \qquad t_1=\left(\frac{p_2 t+q_2}{p_2' t+q_2'}\right)$$

onde

$$(3) \qquad \begin{cases} p_2=pp_1+p'q_1; & q_2=q_1 q'+p_1 q \\ p_2'=pp_1'+p'q_1'; & q_2'=p_1' q+q' q_1'. \end{cases}$$

Será (2) uma substituição do systema, porque, de

$$pq' - p'q \gtrless (0) \quad \text{e} \quad p_1 q_1 - p_1' q_1 \gtrless (0),$$

resulta

$$p_2 q_2' - p_2' q_2 \gtrless (0).$$

Portanto, as substituições (1) formam um grupo. Chama-se *o grupo linear total.*

26. Para conhecer a ordem do grupo, é necessario attender a que, quando se multiplicam os coefficientes p, p', q, q' por um factor inteiro k, o determinante

$$\begin{vmatrix} p & p' \\ q & q' \end{vmatrix},$$

da substituição (1), vem multiplicado por k^2. Se fôr

$$\begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \equiv 1 \pmod{m},$$

isto é, se $\begin{vmatrix} p & p' \\ q & q' \end{vmatrix}$ é *residuo quadratico* em relação ao modulo m, podemos fazer

$$r^2 \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \equiv 1 \pmod{m}.$$

Se $\begin{vmatrix} p & p' \\ q & q' \end{vmatrix}$ é *não residuo* será

$$r^2 \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} = \mathrm{S} \pmod{m},$$

sendo S um determinado *não residuo.*

Portanto, as substituições (1) obter-se-ham fazendo tomar a p, p', q, q' todos os valores que satisfaçam ás relações

$$(\alpha) \qquad pq' - p'q \equiv 1 \pmod{m}$$

$$(\beta) \qquad pq' - p'q \equiv \mathrm{S} \pmod{m}.$$

Vamos determinar primeiramente o numero de substituições

cujos coefficientes satisfazem á congruencia

$$(\alpha) \qquad pq' - qp' \equiv 1 \pmod{m}.$$

Fazendo $p = 0 \pmod{m}$ e dando a q' um valor arbitrario, o valor de p' que satisfaz a (α) dependerá do valor dado a q (que não póde ser zero).

Combinando os $m-1$ valores possiveis de q com os m valores distinctos que póde tomar p', temos $(m-1)(m-1)$ substituições com $p = 0 \pmod{m}$.

Accrescentando a este numero as $m-1$ substituições que, na hypothese feita, dam origem ao indice ∞ (que sam as que correspondem a $p' = q' = 0$) temos ao todo $m(m-1)$ substituições, com $p = 0 \pmod{m}$, satisfazendo a (α).

Quando fôr $p \gtrless 0 \pmod{m}$, podemos dar valores quaesquer a q e a p', que o valor de q' fica determinado.

Ha, pois, m^2 substituições por cada valor de $p \gtrless 0 \pmod{m}$.

Para os $(m-1)$ valores de $p \gtrless 0 \pmod{m}$ haverá $m^2(m-1)$ substituições.

Portanto, o numero total de substituições satisfazendo a (α) é

$$m(m-1) + m^2(m-1) = m(m^2-1).$$

Haverá egual numero de substituições satisfazendo a (β). O numero total de substituições assim determinado é $2m(m^2-1)$, mas estas substituições sam duas a duas eguaes, porque duas substituições oppostas dam o mesmo indice em (1).

A ordem do grupo linear total é, pois, $m(m^2-1)$.

27. *As substituições distinctas que satisfazem á congruencia* $pq' - p'q \equiv 1 \pmod{m}$, *em numero de* $\frac{m(m^2-1)}{2}$, *formam um subgrupo invariante do grupo linear total.*

Com effeito, sendo

$$pq' - p'q \equiv 1 \pmod{m} \quad \text{e} \quad p_1 q_1' - q_1 p_1' \equiv 1 \pmod{m},$$

será

$$p_2 q_2' - p_2' q_2 \equiv 1 \pmod{m}$$

quando fôr

$$\begin{cases} p_2 = pp_1 + q'p_1; & q_2 = q_1 q' + p_1 q \\ p_2' = pp_1' + p'q_1'; & q_2' = p_1' q + q' q_1'. \end{cases}$$

Portanto, *as substituições que satisfazem a* (α) *formam um subgrupo.*

Esse subgrupo é invariante, porque, sendo

$$\begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \equiv 1 \pmod{m} \quad \text{e} \quad \begin{vmatrix} p_a & p_a' \\ q_a & q_a' \end{vmatrix} \equiv S \pmod{m}$$

será

$$\begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \times \begin{vmatrix} p_a & p_a' \\ q_a & q_a' \end{vmatrix} \equiv S \pmod{m};$$

e se representarmos, respectivamente, por γ a substituição

$$t' = \frac{pt+q}{p't+q'} \pmod{m}$$

e por g a substituição

$$t' = \frac{p_a t + q_a}{p_a' t + q_a'} \pmod{m},$$

será $g^{-1}\gamma g$ uma substituição cujos coefficientes satisfazem a (α).

Ao subgrupo de ordem $\frac{m(m^2-1)}{2}$ *do grupo linear total, cujas substituições satisfazem a* (α), *dá-se o nome de grupo modular.*

O grupo linear total e o grupo modular têem particular importancia na theoria da transformação das funcções ellipticas e das equações modulares.

28. Os periodos das substituições do grupo linear total sam: m, factores de $m-1$, e factores de $m+1$.

Com effeito, se uma substituição do grupo linear total deixa fixo o indice t_i, será

$$t_i = \frac{pt_i+q}{p't_i+q'} \pmod{m},$$

(se fôrem p, p', q, q' os coefficientes d'essa substituição), ou

$$p' t_i^2 + (q'-p) t_i - q \equiv 0 \pmod{m};$$

ou ainda, suppondo $p' \lesssim 0 \pmod{m}$.

$$(a) \quad [2p' t_i + q' - p]^2 \equiv (q'-p)^2 + 4p'q \pmod{m}.$$

1.° Se

$$(q'-p)^2+4p'q \gtrless 0 \pmod{m}$$

e *é residuo quadratico,* a congruencia (a) tem duas raizes distinctas t_i, e ha dois indices que permanecem invariaveis para a substituição

$$t' \equiv \frac{pt+q}{p't+q'} \pmod{m}.$$

Representemos esta substituição por γ_e, sejam t_i e t_k os dois indices que permanecem invariaveis, e seja g uma substituição do grupo linear total que transforma os indices t_i e t_k em t_0 e t_∞.

A substituição $g^{-1}\gamma_e g$ conserva os indices t_0 e t_∞, é da mesma especie de γ_e e deverá ter a fórma $t' = ct \pmod{m}$, sendo c uma constante. O seu periodo será um divisor de $m-1$, porque esta substituição pertence ao grupo metacyclico, sem pertencer ao grupo cyclico.

Como o periodo de $g^{-1}\gamma_e g$ é o periodo de γ_e, vê-se que:

As substituições do grupo linear total, que deixam fixos dois indices, têem um periodo divisor de $m-1$. Sam chamadas *substituições ellipticas.*

2.° Se

$$(q'-p)^2+4p'q \gtrless 0 \pmod{m}$$

e *não é residuo quadratico,* a congruencia (a) não tem raizes e as substituições, cujos coefficientes satisfazem á condição supra, não deixam fixo indice nenhum.

Seja γ_k uma d'estas substituições e sejam α_1, α_2 ... as substituições cyclicas em que ella se decompõe.

Supponhamos que a ordem k de α_1 era menor que a ordem de α_2 .... A substituição γ_k^k não seria a identidade e deixaria fixas as k lettras sobre que opera o cyclo α_1. Como uma substituição do grupo linear total só póde deixar fixos, quando muito, dois indices, será $k=2$. O cyclo α_1 opera, pois, sobre dois elementos; γ_k será affim e do mesmo periodo de uma substituição que contem o cyclo $(0, \infty)$, representada por

$$(i) \qquad t' = \frac{c_1}{t} \pmod{m},$$

onde c_1 é uma constante.

Como o periodo de (i) é 2, γ_k será de periodo 2, e os periodos dos seus cyclos serám eguaes a 2.

Se toda a substituição γ_h, satisfazendo á desegualdade da hypothese, se decompõe em cyclos do mesmo periodo e não deixa fixo nenhum dos $m+1$ indices, *o seu periodo é um divisor de* $m+1$.

Estas substituições do grupo linear chamam-se hyperbolicas.

3.° Supponhamos finalmente que

$$(q'-p)^2+4p'q=0 \quad (\text{mod. } m).$$

A congruencia (a) tem uma só raiz, e a substituição correspondente deixa fixo um unico indice. Seja t_i o indice que a substituição γ_p conserva, e representemos por g uma substituição que transforma t_i em t_∞.

A substituição affim $g^{-1}\gamma_p g$ conserva t_∞, é da mesma especie de γ_p e será da fórma

$$t'=(t+b).$$

É uma substituição do grupo cyclico G_{p-1}, de periodo m.

A estas substituições do grupo linear total dá-se o nome de parabolicas.

29. As propriedades fundamentaes do grupo *modular* sam as seguintes:

1.ª *O grupo modular póde gerar-se por meio das duas substituições elementares*

$$\alpha)\ t'\equiv t+1 \quad (\text{mod. } m)$$

e

$$\beta)\ t'\equiv -\frac{1}{t} \quad (\text{mod. } m).$$

Seja, com effeito

$$S)\ t'=\frac{pt+q}{p't+q'} \quad (\text{mod. } m)$$

uma substituição qualquer do grupo modular, cujos coefficientes satisfazem, portanto, á congruencia

$$(1) \qquad pq'-p'q\equiv 1 \quad (\text{mod. } m).$$

α) Supponhamos, em primeiro logar, que é $p\equiv 0$ (mod. m).

A relação (1) dá-nos

$$p' \equiv -\frac{1}{q} \pmod{m},$$

e a substituição S póde escrever-se

$$S)\ t' \equiv \frac{q}{-\frac{1}{q}t + q'} \pmod{m},$$

ou

$$S = UV,$$

sendo

$$U)\ t' \equiv t - qq' \pmod{m}$$

$$V)\ t' \equiv \frac{q}{-\frac{1}{q}t} \pmod{m},$$

e U e V pertencentes ao grupo modular.

É facil ver agora que as substituições U e V se obtêem a partir das substituições elementares α e β.

Assim, a substituição U é a potencia $-qq'$ de α.

Formando a substituição

$$\alpha_1 = \beta\alpha^{-1}\beta)\ t' \equiv \frac{t}{kt+1} \pmod{m},$$

será

$$\alpha_1^k)\ t' \equiv \frac{t}{kt+1} \pmod{m};$$

e como

$$\alpha^{k'})\ t' \equiv t + k' \pmod{m},$$

será

$$\alpha^{k'}\alpha_1^k)\ t' \equiv \frac{t+k'}{kt+(1+kk')} \pmod{m}.$$

Tomando k de maneira a ser satisfeita a congruencia

$$kk' \equiv -1 \pmod{m},$$

será

$$\alpha^{k'}\,\alpha_1^{k})\;t' \equiv \frac{t+k'}{-\dfrac{1}{k'}\,t}\,.$$

Multiplicando á direita por

$$\alpha^{k'})\;t' \equiv t + k' \pmod{m},$$

vem

$$\gamma = \alpha^{k'}\,\alpha_1^{k}\,\alpha^{k'})\;t' \equiv \frac{k'}{-\dfrac{1}{k'}\,t} \pmod{m},$$

que, para $k' = q$, é a substituição V.

b) Supponhamos agora que é $q \equiv 0 \pmod{m}$. Uma substituição qualquer

$$\mathrm{S})\;t' \equiv \frac{pt+q}{p't+q'} \pmod{m},$$

satisfazendo a esta condição, toma a fórma

$$\mathrm{S})\;t' \equiv \frac{pt}{p't+\dfrac{1}{p}} \pmod{m},$$

em virtude da relação fundamental (1). Podemos pôr $\mathrm{S} = \mathrm{UV}$ com

$$\mathrm{U})\;t' \equiv \frac{t}{pp't+1} \qquad \text{e} \qquad \mathrm{V})\;t' \equiv \frac{pt}{\dfrac{1}{p}}\,.$$

A substituição $\mathrm{U} = \alpha_1^{pp'}$.

A substituição V é o producto $\gamma\beta$, tomando $k = \dfrac{1}{p}$.

c) Supponhamos finalmente que é $p \gtrless 0 \pmod{m}$ e $q \lesseqgtr 0 \pmod{m}$, sendo

$$\mathrm{S})\;t' \equiv \frac{pt+q}{pt'+q'} \pmod{m}$$

uma substituição do grupo modular.

O producto

$$\alpha^{k}\mathrm{S})\;t'' \equiv \frac{pt+(q+kp)}{p't+(q'+kp')} \pmod{m}$$

será uma substituição do grupo modular, exprimivel em α e β, se determinarmos k pela condição

$$q + kp = 0 \pmod{m},$$

(em virtude do caso *b*). Portanto, a substituição S será tambem elementarmente exprimivel nas mesmas substituições α e β.

2.ª *O grupo modular é duplamente transitivo.*

A substituição

$$S)\ t' \equiv \frac{pt+q}{t+q'},$$

pertencerá, com effeito, ao grupo modular, se fôr $q \equiv pq' - 1$; e transformará os indices ∞ e 0 respectivamente em p e $p - \frac{1}{q}$, *quaesquer que sejam p e q'*, o que mostra ser o grupo modular duplamente transitivo.

3.ª *O grupo modular só contem substituições pares.*

Basta mostrar que sam pares as substituições elementares α e β.

A substituição $\alpha) t' \equiv t + 1 \pmod{m}$ é parabolica, e tem por periodo m: é, portanto par. A substituição $\beta) t' \equiv -\frac{1}{t} \pmod{m}$ é elliptica ou hyperbolica, contendo, no primeiro caso, $\frac{m-1}{2}$ cyclos de duas lettras, e, no segundo caso, $\frac{m+1}{2}$ cyclos de duas lettras; é, pois, tambem uma substituição par.

4.ª *Quando fôr* $m = 3$, *o grupo modular coincide com o grupo alterno sobre 4 elementos:*

$$a_\infty,\ a_0,\ a_1,\ a_2.$$

Com effeito, para $m = 3$, a ordem $\frac{m(m^2-1)}{2}$ do grupo modular é 12; elle é, pois, um subgrupo de indice 2 do grupo total sobre os quatro elementos a_∞, a_0, a_1, a_2.

É formado por todas as substituições pares e coincide, por isso, com o grupo alterno.

5.ª *Para valores de* m *maiores que 3, o grupo modular é simples.*

Representemos por M_0 o grupo modular sobre os $m+1$ ele-

mentos

$$a_\infty,\quad a_0,\quad a_1\quad \ldots\quad a_{m-1};$$

e supponhamos que M_0 admittia um subgrupo invariante $M_0^{(1)}$.

Vamos vêr que $M_0^{(1)}$ não póde conter substituições parabolicas, nem substituições ellipticas.

a) Seja g_i, com effeito, uma substituição de $M_0^{(1)}$, que suppomos parabolica, e seja a_i o elemento que essa substituição conserva. Por ser transitivo o grupo modular M_0, haverá uma substituição g em M_0 que troca a_i por a_∞. A substituição $g^{-1}g_i g$ pertence a $M_0^{(1)}$, por ser $M_0^{(1)}$ invariante em M_0, e conserva o elemento a_∞. Ella será da fórma

$$g^{-1}g_i g)t' \equiv t+k \pmod{m},$$

com

$$k \lesseqgtr 0 \pmod{m}.$$

Em $M_0^{(1)}$ existirá, pois, a substituição

$$(g^{-1}g_i g)k^{-1}]\ t' \equiv t+1 \pmod{m}$$

que é a substituição elementar α.

Por ser β uma substituição de M_0, o subgrupo invariante $M_0^{(1)}$ conterá tambem a substituição

$$S = \beta^{-1}(g^{-1}g_i g)\,\beta]\,t' \equiv \frac{t}{-kt+1} \pmod{m},$$

qualquer que seja o valor de $k \gtrless 0 \pmod{m}$.

Fazendo $k=1$ na substituição S, o grupo $M_0^{(1)}$ conterá a substituição

$$\alpha S\alpha)\ t' \equiv \frac{1}{-t} \pmod{m}$$

Portanto, $M_0^{(1)}$, contendo α e β, coincide com o grupo modular M_0. *Um subgrupo invariante do grupo modular não poderá, pois, conter substituições parabolicas.*

b) Supponhamos que a substituição g_i do subgrupo invariante $M_0^{(1)}$ é elliptica. Como o grupo modular é duplamente transitivo, $M_0^{(1)}$ conterá uma substituição affim de g_i, que conserva

os indices 0 e ∞. Essa substituição será da fórma

$$g_i')\ t' \equiv \frac{kt}{-\frac{1}{k}} \quad (\text{mod. } m).$$

Existirá ainda em $M_0^{(1)}$ a substituição

$$(\alpha^{-1}\, g_i'\, \alpha)\, g_i'^{-1}]\, t' \equiv t + (k^{-2} - 1) \quad (\text{mod. } m).$$

Como esta substituição é parabolica, recaímos no caso anterior; e, portanto, *um subgrupo invariante do grupo modular não póde conter substituições ellipticas.*

c) Se houver algum subgrupo invariante do grupo modular, só poderá, pois, conter substituições hyperbolicas.

Continuemos a representar por $M_0^{(1)}$ esse subgrupo invariante. *A sua ordem deverá ser divisivel por* $m+1$.

Com effeito, sendo o grupo modular duplamente transitivo e g_i uma substituição de $M_0^{(1)}$, contendo o cyclo $(a_i\, a_l \ldots)$, haverá uma substituição g em M_0 que transforma g_i noutra substituição de $M_0^{(1)}$, contendo o cyclo $(a_\infty,\ a_h \ldots)$, *onde* a_h *é um elemento qualquer.*

O grupo $M_0^{(1)}$ será pelo menos uma vez transitivo, e a sua ordem um multiplo do numero $m+1$ dos elementos.

A ordem de $M_0^{(1)}$, será, portanto, um numero *par,* havendo uma substituição g_i de periodo 2, e uma substituição affim de g_i onde figura o cyclo $(0\,\infty)$, da fórma

$$g_i')\ t' = \frac{k}{-\frac{1}{k}\, t} \quad (\text{mod. } m).$$

Pertence tambem a $M_0^{(1)}$ a transformada

$$\beta^{-1}\, g_i'\, \beta)]\, t' = \frac{-\frac{1}{k}}{kt} \quad (\text{mod. } m),$$

e o producto

$$S = \beta^{-1}\, g_i'\, \beta)\, g_i']\, t' = \frac{+\frac{1}{k^2}\, t}{k^2} \quad (\text{mod. } m)$$

que é uma substituição elliptica, excepto quando fôr

$$k^2 \equiv \frac{1}{k^2} \pmod{m} \qquad \text{ou} \qquad k^4 \equiv 1 \pmod{m},$$

porque, nesse caso, é $S = 1$.

Se S fôr uma substituição elliptica, o subgrupo invariante $M_0^{(1)}$ não existe, como vimos no caso *b*).

Sendo $k^4 \equiv 1 \pmod{m}$, como, por outro lado, é $m = 3 \pmod{4}$, (por ser g_i' hyperbolica) será

$$k \equiv \pm 1 \pmod{m}$$

e g_i' coincide com β. Neste caso, sendo

$$\text{U)}\ t' = \frac{pt+q}{p't+q'} \pmod{m}$$

uma substituição qualquer de M_0, existirá em $M_0^{(1)}$ a substituição

$$U^{-1} g_i' U = U^{-1} \beta U,$$

representada por

$$t' \equiv \frac{-(pp'+qq')t+(p^2+q^2)}{-(p'^2+q'^2)t+(pp'+qq')} \pmod{m},$$

cujos coefficientes deverám satisfazer á congruencia

$$pq' - p'q \equiv 1 \pmod{m}.$$

Fazendo $p' = q' = 1$, deverá ser

$$p - q \equiv 1 \pmod{m};$$

determinando p e q de modo a ser tambem satisfeita a congruencia

$$p + q \equiv 0 \pmod{m},$$

será

$$2p = -2q = 1,$$

e a substituição $U^{-1}\beta U$ será representada por

$$t' \equiv \frac{\frac{1}{2}}{-2t} \pmod{m}.$$

Como é $k=2$, deverá ser satisfeita a congruencia

$$2 = \pm 1 \pmod{m},$$

e, portanto, $m=3$.

O grupo modular só admitte subgrupo invariante, formado por substituições hyperbolicas, quando fôr $m=3$.

Adiante se verá que o grupo alterno é tambem sempre um grupo simples, excepto quando opera sobre 4 elementos, coincidindo com o grupo modular sobre $3+1$ elementos:

$$a_\infty, \quad a_0, \quad a_1, \quad a_2.$$

V

Composição do grupo total e do grupo alterno. — Ordens possiveis de grupos simples

30. Vimos que o grupo alterno é um subgrupo de indice 2 do grupo total. Vamos vêr agora que elle é o *unico* subgrupo d'esse indice contido no grupo total.

Demonstremos, para isso, o seguinte

THEOREMA. — *Se um grupo* G *de substituições sobre* n *elementos contem todos os cyclos possiveis de ordem* k, *o grupo* G *coincide com o grupo alterno ou com o grupo total.*

1.° *Seja* $k = 2$. Nesse caso o grupo G contem todas as transposições e, por consequencia, todas as substituições possiveis sobre n elementos: coincide com o grupo total.

2.° *Seja* $k = 3$. O grupo G contem todas as substituições cyclicas sobre 3 elementos. Elle conterá todas as substituições pares. Com effeito, cada substituição par é um producto de um numero par de transposições; e o producto de duas transposições é um cyclo de 3.ª ordem, se as duas transposições tiverem um elemento commum, e é um producto de dois cyclos de 3.ª ordem, se as duas transposições não tiverem elemento commum. Assim

$$(a_1\, a_2)\,(a_1\, a_3) = (a_1\, a_2\, a_3); \quad (a_1\, a_2)\,(a_3\, a_4) = (a_2\, a_3\, a_4)\,(a_1\, a_2\, a_3).$$

Se o grupo G contem todas as substituições pares, coincide necessariamente com o grupo alterno, ou com o grupo total.

3.° *Seja* $k > 3$. Este caso reduz-se ao precedente, porque todo o cyclo de 3.ª ordem é exprimivel pelo producto de *dois* cyclos de ordem $k > 3$.

31. Sejam $\alpha_1, \alpha_2 \ldots \alpha_{\frac{n!}{2}}$ as substituições de um subgrupo G_1, de indice 2, do grupo total $G_{n!}$.

Se fôr g uma substituição de $G_{n!}$ não pertencente a G_1, a substituição g^2 pertence a G_1. Com effeito, sendo

$$\begin{cases} \alpha_1, & \alpha_2 & \ldots & \alpha_{\frac{n!}{2}} \\ \alpha_1 g, & \alpha_2 g & \ldots & \alpha_{\frac{n!}{2}} g \end{cases}$$

todas as substituições de $G_{n!}$, se fôsse

$$\alpha_k g = g^2$$

seria $g = \alpha_i$, o que é contra a hypothese. Todas as potencias pares de g pertencem a G_1, e, portanto, o periodo de g *é par*, porque em G_1, como em todos os grupos, figura a identidade.

Como a substituição g é qualquer, não pertencente a G_1, conclue-se que G_1 *contem todas as substituições de periodo impar.*

Como os cyclos de 3.ª ordem sam de periodo impar, G_1 contem todos os cyclos de 3.ª ordem, e coincide, em virtude do theorema anterior, com o grupo alterno.

O grupo total tem um unico subgrupo de indice 2: o grupo alterno.

* * *

O grupo alterno é subgrupo invariante do grupo total.

Porque, se fôr α_i uma substituição do grupo alterno e g uma substituição impar, a substituição $g^{-1} \alpha_i g$ é par e pertence, portanto, ao grupo alterno.

32. THEOREMA. — *Quando o numero de elementos é differente de 4, o grupo alterno é o unico invariante do grupo total.*

O theorema é manifestamente verdadeiro quando o numero de elementos é 2 ou 3.

Seja n o numero de elementos sobre que opera o grupo $G_{n!}$ e supponhamos que elle admitte um invariante G_1, differente do grupo alterno.

Entre as substituições de G_1 não figura nenhuma substituição

cyclica; porque, se fôsse g_1 um cyclo de ordem k, pertencente a G_1, todos os cyclos de ordem k (transformados de g_1 por meio das substituições de $G_{n!}$) pertenceriam a G_1, e este grupo coincidiria com o grupo alterno ou com o grupo total.

Cada substituição de G_1, decomposta em factores cyclicos, conterá, pois, dois ou mais factores. Seja

$$g_1 = (a_1\, a_2\, \ldots)\,(a_i\, a_{i+1}\, \ldots)\, \ldots$$

a substituição de G_1 (differente de 1) *que troca menor numero de elementos.*

A transformada de g_1

$$g_1' = (a_1\, a_2\, \ldots)\,(a_i\, a_{i+1}\, .\, .)^{-1}\, \ldots$$

pertencerá a G_1, bem como o producto

$$g_1\, g_1' = (a_1\, a_2\, \ldots)^2.$$

Mas este producto deverá ser a identidade, porque de contrario trocaria menos elementos que g_i. O primeiro cyclo de g_i é, pois, uma transposição $(a_1\, a_2)$, e o mesmo se dirá de todos os outros. Será

$$g_i = (a_1\, a_2)\,(a_3\, a_4)\, \ldots$$

As transposições de g_i não podem ser mais de duas; porque, se fôssem tres,

$$g_i = (a_1\, a_2)\,(a_3\, a_4)\,(a_5\, a_6),$$

por exemplo, pertenceria a G_1 a substituição

$$g_i' = (a_1\, a_3)\,(a_2\, a_4)\,(a_5\, a_6),$$

e o producto

$$g_i\, g_i' = (a_1\, a_4)\,(a_2\, a_3)$$

que troca menos elementos que g_i. Será, portanto,

$$g_i = (a_1\, a_2)\,(a_3\, a_4).$$

O grupo G_1 conterá os productos de duas transposições com

elementos diversos; conterá a substituição

$$g_k = (a_1\, a_5)\,(a_3\, a_4),$$

se existirem pelo menos cinco elementos, e, portanto, o producto

$$g_i\, g_k = (a_1\, a_2\, a_5).$$

Mas este producto troca menos elementos que g_i; logo, o grupo G_1, nas condições da hypothese, não póde existir, quando o numero de elementos fôr maior que 4; o que demonstra o theorema.

Se o numero de elementos fôr 4, o grupo G_1 conterá, como vimos, as substituições seguintes:

$$\begin{cases} g_1 = (a_1\, a_2)\,(a_3\, a_4) \\ g_2 = (a_1\, a_3)\,(a_2\, a_4) \\ g_3 = (a_1\, a_4)\,(a_2\, a_3) \\ g_4 = 1 \end{cases}$$

formadas por duas transposições com elementos diversos.

É um grupo de 4.ª ordem, subgrupo *invariante* de indice 6 do grupo total G_{24}. Este grupo tem grande importancia na theoria das equações algebricas de Galois, e foi designado por Klein com o nome de *Vierergruppe*.

33. Theorema. — *O grupo alterno é um grupo simples, quando é differente de 4 o numero de elementos sobre que operam as substituições do grupo.*

Seja $G_{n!}$ o grupo total sobre n elementos, $G_{\frac{n!}{2}}$ o grupo alterno, e supponhamos que $G_{\frac{n!}{2}}$ admittia um subgrupo invariante maximo G_1.

O grupo G_1 não é invariante em $G_{n!}$, porque este grupo admitte como unico invariante o grupo alterno. Portanto, se fôr g uma substituição impar do grupo total, o grupo transformado $G_2 = g^{-1} G_1\, g$ não coincidirá com G_1; mas como

$$G_{\frac{n!}{2}} = g^{-1} G_{\frac{n!}{2}}\, g,$$

por ser $G_{\frac{n!}{2}}$ invariante em $G_{n!}$, será ainda G_2 invariante maximo em $G_{\frac{n!}{2}}$.

Se fôr k a ordem do subgrupo G_3 commum a G_1 e G_2, e k_1 a ordem de G_1 e de G_2, será, em virtude de um theorema demonstrado,

$$\frac{n!}{2} = \frac{k_1^2}{k}, \quad \text{ou} \quad k = \frac{k_1^2}{\frac{n!}{2}}.$$

Mas G_1 e G_2 sam permutaveis e, portanto, qualquer que seja a substituição g_i do grupo total, os grupos (1) $g_i^{-1} G_1 g_i$ e (2) $g_i^{-1} G_2 g_i$ coincidem com G_1 e G_2, ou com G_2 e G_1 respectivamente.

Como $g_i^{-1} G_3 g_i$ é o subgrupo commum a (1) e (2), será $g_i^{-1} G_3 g_i = G_3$ e, portanto, invariante em $G_{n!}$.

A ordem k de G_3 será, pois, a unidade, porque $G_{n!}$ só tem como invariante o grupo alterno, e $k_1^2 = \frac{n!}{2}$, o que é absurdo (1).

Fica assim demonstrado o theorema.

Quando fôr $n = 4$, o *Vierergruppe*, invariante do grupo total e só contendo substituições pares, é invariante do grupo alterno.

Do que fica dito resulta que, em geral, o grupo total admitte a unica serie de composição: 2, $\frac{n!}{2}$ *e não é, portanto, um grupo resoluvel, quando fôr* $n > 4$.

Sendo $n = 4$, a serie unica de composição do grupo total é 2, 3, 2, 2 e *o grupo é resoluvel.*

34. Não ha um criterio geral para verificar se um numero inteiro k póde ser ordem de um grupo simples. Ha criterios particulares, baseados nas propriedades geraes dos grupos, e nas seguintes proposições fundamentaes:

1.ª *Todo o grupo, cuja ordem é um numero primo, é um grupo simples.*

2.ª *Todo o grupo, cuja ordem é potencia inteira e positiva de um numero primo, é um grupo composto.*

3.ª *Todo o grupo cuja ordem é producto de dois numeros primos, é um grupo composto.*

---

(1) Com effeito, os factores primos que figuram na decomposição de k_1^2 têem todos expoente par, e na decomposição de $\frac{n!}{2}$ não póde figurar com expoente superior a 1 o maior numero primo contido em n.

Com effeito, um grupo, cuja ordem satisfaz á hypothese de qualquer das duas ultimas proposições, é resoluvel, com uma serie de composição formada por mais de dois termos.

4.ª Seja G um grupo simples de ordem k e m^r a maior potencia do numero primo m contida em k. Em virtude do 2.º theorema de SYLOW (1), haverá em G mais de um subgrupo de ordem m^r; sejam elles

$$(\alpha) \qquad G_1,\ G_2 \ldots G_s.$$

Os transformados de (α), por meio de uma substituição qualquer de G, sam os mesmos grupos (α) por outra ordem. A cada substituição de G, podemos, pois, fazer corresponder uma substituição h sobre os *elementos* (α).

As substituições h formam um grupo H, isomorpho de G, *cuja ordem não póde ser superior a* k.

O isomorphismo de G *e* H *é necessariamente holoedrico, porque* G *é um grupo simples.*

O grupo isomorpho H *só contem substituições pares, por ser um grupo simples.*

Applicando estes principios, mostra-se que o unico numero composto, menor que 100, que póde ser ordem de um grupo simples é 60.

É a ordem do grupo alterno sobre 5 elementos e do grupo modular sobre $4+1$ elementos.

(1) Porque o numero s d'esses subgrupos é o indice do maior subgrupo de G que os contem como invariantes. E esse indice é maior que 1, por ser G um grupo simples.

VI

Generalisação do conceito de isomorphismo. — Grupos de subtituições lineares de ordem finita

35. O conceito de isomorphismo, estabelecido para os grupos de substituições, é susceptivel de se generalizar a grupos de operações quaesquer (para as quaes tenha sentido a definição dada de grupo).

Se as operações que entram na constituição do grupo A sam de categoria differente da categoria das operações que entram na constituição do grupo B, diz-se que os dois grupos A e B sam *holoedricamente isomorphos,* quando é possivel estabelecer uma correspondencia biunivoca entre as operações do grupo A e as do grupo B, tal que ao producto de duas operações quaesquer a e a' de A *corresponde* o producto das operações b e b' de B, respectivamente correspondentes a a e a'.

Estabelece-se assim a noção de isomorphismo sob um ponto de vista meramente abstracto, que augmenta a sua importancia, pois *permitte substituir um grupo finito de operações quaesquer por um grupo isomorpho de substituições.*

Com effeito, seja

$$(1) \qquad A(a_1, \ a_2, \ \ldots \ a_k)$$

um grupo de operações quaesquer, satisfazendo ás condições da definição.

Se multiplicarmos todas as operações de A por qualquer d'ellas a_h, as operações

$$(2) \qquad a_1 a_h, \ \ a_2 a_h \ \ldots \ a_k a_h$$

figuram todas em (1); de resto, se as operações (1) sam todas

distinctas, as (2) sam tambem distinctas, porque, se fôsse

$$a_i a_h = a_l a_h,$$

seria $a_i = a_l$. Portanto, as operações (2) sam as mesmas operações (1) por outra ordem.

A multiplicação das operações (1) por a_h equivale, pois, a effectuar sobre os *elementos* (1) a *substituição*

$$b_h = \begin{pmatrix} a_1 a_h, & a_2 a_h, & \dots & a_k a_h \\ a_1, & a_2 & \dots & a_k \end{pmatrix}$$

A cada multiplicador a_h corresponde uma substituição b_h. As substituições b_h formam um grupo, porque ao multiplicador $a_h a_l$ corresponde manifestamente a substituição $b_h b_l$, se fôrem b_h e b_l as substituições respectivamente correspondentes aos multiplicadores a_h e a_l.

A dois multiplicadores distinctos correspondem substituições tambem distinctas, e *o grupo* B *das substituições* b_h *é holoedricamente isomorpho com* A, *e, portanto, da mesma ordem* k.

A operação de A, que corresponde á identidade em B, é a *operação identica* em A.

Uniformisa-se assim o estudo dos grupos de operações de ordem finita (1).

36. Uma categoria importante de grupos de substituições, que de certo modo realisa uma transição para os grupos de transformações de Lie, é a dos *grupos de substituições lineares sobre uma variavel.*

---

(1) Entende-se sempre que as operações em questão satisfazem ás condições fundamentaes que figuram na definição de *grupo,* tal como tem sido apresentada. É a definição de grupo que convem ás substituições e que Galois estabeleceu; é a que nos interessa, para o estabelecimento da theoria das equações algebricas.

O conceito de grupo generalizou-se, a noção de grupo invadiu todo o campo da Analyse, deu logar a theorias mais vastas e complexas, como é a theoria dos grupos de transformações de Sophus Lie, mas o *typo* da theoria primitiva conservou-se, orientando as novas investigações e fornecendo até a nomenclatura.

A profunda analogia entre estas theorias, resultante do conceito fundamental de grupo que em todas ellas domina, justifica, de resto, a affinidade de exposição que todas ellas têem com a theoria dos grupos de substituições.

Têem estes grupos uma importancia capital na theoria das equações algebricas de GALOIS, e sam susceptiveis de uma notavel representação geometrica, em que sobresáe com toda a nitidez a noção do grupo.

Seja z uma variavel complexa, e z' outra variavel ligada com z pela relação

$$(1) \qquad z' = \frac{pz+q}{p'z+q'},$$

onde p, q, p', q' sam constantes quaesquer que não annulam a differença $pq'-p'q$, (porque nesse caso z' seria independente de z).

Se fôr z'' uma nova variavel ligada com z' pela relação

$$(2) \qquad z'' = \frac{p_1 z' + q_1}{p_1' z' + q_1'}, \qquad \text{com} \qquad p_1 q_1' - p_1' q_1 \gtrless 0,$$

será

$$z'' = \frac{p_2 z + q_2}{p_2' z + q_2},$$

onde

$$\begin{cases} p_2 = pp_1 + p'q_1\,; & q_2 = qp_1 + q'q_1 \\ p_2' = pp_1' + p'q_1'\,; & q_2' = qp_1' + q'q_1', \end{cases}$$

e portanto

$$p_2 q_2' - p_2' q_2 \gtrless 0.$$

Vemos, pois, que as *operações* (1) sam susceptiveis de se *multiplicar*, conduzinde a uma operação da mesma categoria. Gozam, pois, de todas as propriedades das operações *agrupaveis*, visto que esses productos satisfazem evidentemente á lei associativa.

Podemos considerar as operações (1) como verdadeiras substituições, operando sobre um numero infinito de elementos. Cada ponto z do plano é *substituido* pelo seu correspondente z'. O numero de elementos é, de resto, de secundaria importancia no conceito de substituição.

Vamos vêr que é possivel distribuir todos os grupos finitos de substituições lineares por *cinco* categorias differentes, examinando para isso as propriedades geraes d'esses grupos.

37. Substituindo em

$$(1) \qquad z' = \frac{pz+q}{p'z+q'}$$

a variavel z por outra t, ligada com ella por meio da relação

$$t = \frac{rz+s}{r'z+s'}, \tag{2}$$

onde r, s, r', s' sam constantes quaesquer que não annullam a differença $rs'-r's$; e substituindo a variavel z' por outra t' ligada com ella pela relação

$$t' = \frac{rz'+s}{r'z'+s'} \tag{3}$$

cujos coefficientes sam os mesmos de (2), ficará t' ligada com t por uma relação linear que se diz *transformada* de (1).

Se a substituição (1) fizer parte de um grupo G, as transformadas das substituições do grupo G por (2) e (3) formam um grupo G', que se diz *transformado* de G pelos parametros r, s, r', s'.

Consideramos pertencentes ao mesmo typo de G *todos os seus transformados.*

Chamam-se *pólos* de uma substituição linear (1) os valores de z que a substituição conserva, e que satisfazem, portanto, á equação

$$z = \frac{pz+q}{p'z+q'},$$

ou

$$p'z^2+(q'-p)z-q=0. \tag{4}$$

Os pólos de uma substituição linear sam dois; quando fôr $p'=0$, *um d'elles será* $z=\infty$ *e o outro será* $z=\frac{q}{q'-p}$.

Os pólos da transformada de uma substituição linear (1) sam os pontos transformados dos pólos da substituição primitiva (1).

Uma substituição que tem por pólo o infinito é da fórma

$$z' = \frac{pz+q}{q'} = kz+k'.$$

Se o segundo pólo fôr tambem o infinito, será $p=q'$ e a substituição será da fórma

$$z' = z+k' \tag{5}$$

Uma substituição linear da fórma (5) *não póde fazer parte de um grupo finito,* porque o seu periodo é infinito: nenhuma potencia de (5) reproduz a identidade.

Não póde, pois, fazer parte d'esse grupo finito nenhuma transformada de (5), isto é, *nenhuma substituição com pólos eguaes.*

38. THEOREMA. — *Se* k *substituições lineares de um grupo finito* G *tiverem um pólo commum, ellas têem tambem o segundo pólo commum e formam em* G *um subgrupo cyclico.*

Sejam

$$(1)\quad z_1' = \frac{p_1 z + q_1}{p_1' z + q_1'},\quad z_2' = \frac{p_2 z + q_2}{p_2' z + q_2'},\quad \ldots\quad z_k' = \frac{p_k z + q_k}{p_k' z + q_k'},$$

k substituições de um grupo G, tendo todas o polo a. Será

$$a = \frac{p_1 a + q_1}{p_1' a + q_1'} = \frac{p_2 a + q_2}{p_2' a + q_2'} = \ldots = \frac{p_k a + q_k}{p_k' a + q_k'}.$$

As substituições (1) formam um grupo, porque o producto das substituições z_i' e z_h' será

$$(2)\qquad z_{i,h}' = \frac{p_h z_i' + q_h}{p_h' z_i' + q_h'};$$

fazendo $z = a$, vem

$$z_{i,h}' = a,$$

e a substituição (2) pertence, portanto, a (1).

Effectuando uma transformação linear da variavel, de modo a transportar para o infinito o pólo a, o grupo transformado de (1) será

$$(2)\qquad z_1' = z,\quad z_2' = b_2 z + b_2',\quad \ldots\ z_k' = b_k z + b_k',$$

onde a primeira substituição representa a identidade, que necessariamente existe em todos os grupos, e que admitte por pólo a, como qualquer outro ponto do plano.

O periodo de qualquer substituição de (2) é um factor da ordem k do grupo, e portanto, a potencia k de qualquer d'ellas será a identidade; d'onde

$$b_2^k = b_3^k = \ldots = b_k^k = 1,$$

o que mostra que b_2, b_3 ... b_k sam raizes de gráo k da unidade. Essas raizes sam todas distinctas; porque, se fôsse $b_2 = b_3$, o producto da substituição $z_2' = b_2 z + b_2'$ pela inversa

$$z = \frac{z_3' - b_3'}{b_2} \quad \text{de} \quad z_3' = b_2 z + b_3',$$

seria uma substituição

$$(c) \qquad z' = \frac{b_2 z + b_2' - b_3'}{b_2} = z + \frac{b_2' - b_3'}{b_2}$$

do grupo (2). Como as duas substituições z_2' e z_3' sam distinctas, não póde ser tambem $b_2' = b_3'$; a substituição (c) seria, pois, de periodo infinito e pertenceria a um grupo finito, o que é absurdo.

Sendo distinctas, b_2 ... b_k sam todas as raizes de gráo k da unidade, e as substituições

$$(3) \qquad z_1' = z, \quad z_2' = b_2 z, \quad \ldots \; z_k = b_k z$$

formam manifestamente um grupo cyclico de ordem k, *tendo cada substituição os dois pólos* 0 *e* ∞.

Mas *o grupo* (3) *é transformado de* (2). Com effeito, pela transformação linear

$$(\alpha) \qquad z' = z - \frac{b_2'}{b_2^1},$$

as substituições

$$z_2' = b_2 z + b_2' \quad \text{e} \quad z_3' = b_3 z + b_3'$$

do grupo (2) convertem-se respectivamente nas substituições

$$z_2' = b_2 z$$

e

$$(\beta) \qquad z_3' = b_3 z - \frac{b_3 b_2'}{b_2} + b_3' = b_3 z + d_3$$

do grupo transformado de (2) por meio de (α). A este mesmo grupo pertencerám as substituições

$$z_{3,2}' = b_2 b_3 z + b_2 d_3$$

$$z_{2,3}' = b_2 b_3 z + d_3.$$

Estas duas substituições, pelo que fica dicto, não poderám ser distinctas e deverá, portanto, ser $b_2 d_3 = d_3$; como $b_2 \gtrless 1$, será $d_3 = 0$. A substituição (β) pertence, pois, ao grupo (3), e o mesmo se mostraria de qualquer substituição do grupo transformado de (2) por meio de (α).

O grupo (3) é egualmente transformado de (1) e este será um grupo cyclico, *cujas substituições têem todas o segundo pólo commum.*

39. Seja G_1 o subgrupo cyclico formado por todas as substituições do grupo G que têem a como pólo commum, e

$$g')\ z' = \frac{p_e z + q_e}{p_e' z + q_e'}$$

uma substituição qualquer de G, não pertencente a G_1.

As substituições do subgrupo transformado de G_1 por meio de g' admittem, como pólo commum,

$$a' = \frac{p_e a + q_e}{p_e' a + q_e'}.$$

Os pólos a e a' dizem-se *equivalentes;* cada um d'elles é commum a um mesmo numero k de substituições de G, (incluindo a identidade).

Se fôr n a ordem de G, o numero de pólos distinctos da mesma classe de equivalencia de a é manifestamente $\frac{n}{k}$, e, como cada um d'elles é commum a $k-1$ substituições (não contando a identidade), será $(k-1)\frac{n}{k}$ o total de pólos d'esta classe, contando cada um d'elles tantas vezes quantas as substituições a que pertence.

Por outro lado, admittindo cada substituição dois pólos distinctos, os pólos das substituições do grupo G de ordem n serám em numero de $2(n-1)$, não contando a identidade. Sendo s o numero de classes de equivalencia dos pólos de G, terá logar a relação

$$(1) \qquad \sum_{i=1}^{s} \frac{n}{k_i}(k_i - 1) = 2(n-1)$$

que permitte estabelecer, como nos propuzemos, a existencia de

cinco categorias possiveis de grupos finitos de substituições lineares.

40. *O numero de classes de equivalencia não póde ser superior a 3, nem inferior a 2.*

Com effeito, escrevendo a relação (1) do paragrapho anterior sob a fórma

$$(1) \qquad \sum_{i=1}^{s}\left(1-\frac{1}{k_i}\right)=2-\frac{2}{n}$$

vê-se que, se fôsse $s \geqq 4$, o primeiro membro seria maior ou egual a 2 (por ser $k_i \geqq 2$), sendo o segundo membro menor que 2; se fôsse $s=1$, o primeiro membro seria menor que 1 e o segundo maior ou egual a 1.

a) *Para* $s=2$, a equação fundamental toma a fórma

$$(2) \qquad \frac{1}{k_1}+\frac{1}{k_2}=\frac{2}{n}.$$

Como k_1 e k_2, ordens de subgrupos de G, ham de ser divisores de n, teremos necessariamente $k_1=k_2=n$.

Como k_1 é a ordem de um grupo cyclico, ha em G uma substituição de periodo $k_1=n$, e *o grupo* G *é um grupo cyclico.*

Todas as suas substituições têem os mesmos dois pólos; effectuando uma transformação linear conveniente, esses dois pólos coincidirám, respectivamente, com 0 e ∞ e as substituições do grupo transformado (egualmente cyclico) serám da fórma

$$z_i=\alpha^i z \,(i=0,\ 1\ \ldots\ n-1)$$

onde α é uma raiz primitiva de gráo n da unidade.

b) *Para* $s=3$, a equação fundamental toma a fórma

$$(3) \qquad \frac{1}{k_1}+\frac{1}{k_2}+\frac{1}{k_3}=1+\frac{2}{n}.$$

Os numeros k_1, k_2, k_3 não podem ser simultaneamente maiores que 2, porque o 1.º membro de (3) seria menor ou egual a 1. Supponhamos $k_1=2$; a equação (3) toma a forma

$$(4) \qquad \frac{1}{k_2}+\frac{1}{k_3}=\frac{1}{2}+\frac{2}{n}.$$

Os numeros k_2 e k_3 não podem ser ambos maiores que 3, porque o 1.º membro seria então menor ou egual a $\frac{1}{2}$.

Fazendo $k_2 = 2$, a equação (4) toma a fórma

$$(5) \qquad \frac{1}{k_3} = \frac{2}{n}; \quad \text{d'onde} \quad k_3 = \frac{n}{2}.$$

Fazendo $k_2 = 3$, a equação (4) toma a fórma

$$(6) \qquad \frac{1}{k_3} = \frac{1}{6} + \frac{2}{n}; \quad \text{d'onde} \quad k_3 < 6.$$

Temos, pois, os seguintes casos possiveis, satisfazendo a (3)

$$b') \qquad k_1 = 2, \quad k_2 = 2, \quad k_3 = \frac{n}{2}$$

$$b'') \qquad k_1 = 2, \quad k_2 = 3, \quad k_3 = 3 \quad (n = 12$$

$$b''') \qquad k_1 = 2, \quad k_2 = 3, \quad k_3 = 4 \quad (n = 24$$

$$b^{IV}) \qquad k_1 = 2, \quad k_2 = 3, \quad k_3 = 5 \quad (n = 60.$$

Estes quatro typos de grupo formam com o *typo cyclico* as unicas cinco categorias possiveis de grupos finitos de substituições lineares. Sam todas distinctas, como vamos vêr.

11. Seja G um grupo de ordem n, do typo (b'):

$$k_1 = k_2 = 2, \quad k_3 = \frac{n}{2}.$$

O grupo G é necessariamente de ordem par, admittindo um subgrupo cyclico G_1 de ordem $k_3 = \frac{n}{2}$.

Se fôr g' uma substituição de G, não pertencente a G_1, e

$$G_1 = (1, \quad g, \quad g^2, \quad g^{n-1}),$$

as substituições

$$(1) \qquad G' \begin{cases} 1, & g, & g^2, & \dots & g^{n-1} \\ g', & gg', & g^2g', & \dots & g^{n-1}g' \end{cases}$$

sam todas distinctas, pertencentes a G, e em numero de n; sam todas as substituições do grupo G.

As substituições do subgrupo cyclico G_1 já vimos que se póde dar a fórma normal

$$z' = \alpha^i z \left(i = 0,\ 1,\ 2,\ \ldots\ \frac{n}{2} - 1 \right),$$

onde α é uma raiz primitiva do gráo $\frac{n}{2}$ da unidade.

Resta determinar a fórma das substituições da 2.ª linha de (1).

As substituições

$$(g',\quad gg',\quad \ldots\ g^{n-1}g')$$

devem coincidir, por outra ordem, com as substituições

$$(g',\quad g'g,\quad \ldots\quad g'g^{n-1}),$$

e, portanto, deverá ser

$$(2) \qquad gg' = g'g^k \qquad (k \leqq n-1).$$

Representando g' por $z' = \frac{pz+q}{p'z+q'}$, a egualdade (2) toma a fórma

$$\frac{p\alpha z+q}{p'\alpha z+q'} = \alpha^k \frac{pz+q}{p'z+q'},$$

que só póde ser satisfeita por

$$p = q' = 0, \qquad \text{ou} \qquad p' = q = 0,$$

A ultima solução deve pôr-se de parte, porque daria a g' a fórma

$$z' = \frac{pz}{q'} = cz;$$

todas as substituições de G teriam os mesmos dois polos communs, e o grupo G seria cyclico.

A primeira solução dá a g' a fórma

$$z' = \frac{q}{p'\alpha z} = \frac{c}{z}.$$

Effectuando a transformação linear $z' = -cz$, as substituições do grupo G podem pôr-se sob a fórma

$$\text{II} \qquad \begin{cases} z' = \beta^i z \\ z' = -\dfrac{\beta^i}{z} \end{cases} (i = 0, 1, 2 \ldots n-1).$$

Os grupos das duas categorias estudadas sam os unicos que podem admittir invariantes cyclicos.

Com effeito, se um grupo G admitte um invariante cyclico G_1, que supporemos maximo, cujas substituições sam da fórma $z' = \alpha^i z$, só poderá haver em G substituições g da fórma

$$z' = cz \quad \text{ou} \quad z' = \frac{c}{z},$$

para que a transformada $g^{-1} g_1 g$ de qualquer substituição g_1 de G_1 seja ainda uma substituição de G_1 e, portanto, da fórma

$$z' = \alpha^i z.$$

Se houvesse em G substituições da fórma $z' = cz$, além das de G_1, G_1 não seria um invariante maximo, como suppozemos, porque haveria em G um invariante cyclico contendo G_1.

Se as substituições de G, não pertencentes a G_1, fôrem da fórma $z' = \frac{c}{z}$, o producto de duas quaesquer d'ellas,

$$z' = \frac{c}{z}, \quad z' = \frac{c'}{z},$$

será uma substituição $z' = \frac{c}{c'} z$ de G_1. O grupo G será, pois, formado pelas substituições de G_1, potencias de uma mesma substituição g_1, e pelos productos das substituições de G_1 por uma mesma substituição $z' = \frac{c}{z}$. É um grupo da segunda categoria.

42. Seja G_{12} um grupo do typo

$$b'')\ n=12,\quad k_1=2,\quad k_2=3,\quad k_3=3.$$

Para determinar a fórma das substituições do grupo G_{12}, vamos mostrar que elle *é holoedricamente isomorpho com um grupo alterno de substituições sobre quatro elementos.*

Em virtude do 2.º theorema de SYLOW, o numero n' de subgrupos de 3.ª ordem de G_{12} será um divisor de 12, satisfazendo á congruencia $n'=1$ (mod. 3), e teremos, portanto, $n'=1$, ou $n'=4$.

Como n' é o indice em G_{12} do maior subgrupo que contem como invariante um d'aquelles subgrupos de terceira ordem, não poderá ser $n'=1$, porque então o grupo G_{12} conteria invariantes cyclicos.

Serám, pois, 4 os subgrupos de 3.ª ordem de G_{12}, que representaremos por

$$(1)\qquad G_3^1,\quad G_3^2,\quad G_3^3,\quad G_3^4,$$

e que sam, ainda em virtude do 2.º theorema de SYLOW, transformados uns dos outros por meio das substituições de G_{12}.

Sendo g uma substituição qualquer de G_{12}, os grupos

$$(2)\quad g^{-1}G_3^1 g,\quad g^{-1}G_3^2 g,\quad g^{-1}G_3^3 g,\quad g^{-1}G_3^4 g$$

serám, pois, os mesmos subgrupos (1), por outra ordem. A cada substituição linear g de G_{12} corresponde uma substituição sobre os *elementos* (1) e ao grupo G_{12} corresponde um grupo transitivo A de substituições sobre os elementos (1) com o qual G_{12} é isomorpho.

Chamando k ao gráo de meriedria d'esse isomorphismo, será $k'=\frac{12}{k}$ a ordem de A, que deve ser um multiplo de 4. Portanto, será $k=1$, ou $k=3$. A ultima solução é impossivel, porque á identidade em A corresponderia em G_{12} um subgrupo cyclico *invariante* de 3.ª ordem. Os dois grupos G_{12} e A sam, pois, como se queria demonstrar, holoedricamente isomorphos, e o grupo A, de ordem 12, é o grupo alterno sobre os quatro elementos

$$G_3^1,\quad G_3^2,\quad G_3^3,\quad G_3^4.$$

Todas as substituições de A se obtêem a partir das tres ge-

neratrizes

$$\alpha_1 = (G_3^1\, G_3^4)\,(G_3^2\, G_3^3)$$

$$\alpha_2 = (G_3^1\, G_3^2)\,(G_3^3\, G_3^4)$$

$$\alpha_3 = (G_3^1\, G_3^2\, G_3^3).$$

Representando por g_1, g_2, g_3 as substituições de G_{12}, respectivamente correspondentes a α_1, α_2, α_3, todas as substituições de G_{12} se poderám egualmente obter a partir das generatrizes g_1, g_2, g_3.

As substituições α_1 e α_2 sam de periodo 2; portanto, uma das substituições g_1 ou g_2, (supponhamos g_1), será da fórma

$$z' = -z,$$

(depois de reduzida á fórma normal).

A fórma de g_2 fica immediatamente determinada, pois que, sendo $\alpha_2^{-1}\,\alpha_1\,\alpha_2 = \alpha_1$, será tambem $g_2^{-1}\,g_1\,g_2 = g_1$, o que exige que g_2 tenha qualquer das fórmas

$$z' = cz, \quad \text{ou} \quad z' = \frac{c}{z},$$

onde c é uma constante. Por ser g_2 de periodo 2, ella coincidiria com g_1 (depois de reduzida á fórma normal), se fôsse $g_2)\,z' = cz$.

Deverá, pois, ser $g_2)\,z' = \dfrac{c}{z}$, ou, depois de reduzida á fórma normal, $g_2)\,z' = \dfrac{1}{z}$.

Para achar a fórma de g_3, basta attender a que, existindo entre α_1, α_2, α_3 as relações

$$\alpha_2^{-1}\,\alpha_3\,\alpha_1 = \alpha_3 \quad \text{e} \quad \alpha_1^{-1}\,\alpha_3\,\alpha_1\,\alpha_2 = \alpha_3,$$

deverám existir egualmente entre as suas correspondentes em G_{12} as relações

$$g_2^{-1}\,g_3\,g_1 \;\; = g_3 \qquad (\gamma)$$

$$g_1^{-1}\,g_3\,g_1\,g_2 = g_3 \qquad (\gamma').$$

Suppondo g_3 da fórma geral

$$g_3)\,z' = \frac{pz+q}{p'z+q'},$$

..

as relações (γ) e (γ') conduzem ás seguintes identidades:

$$-\frac{p+qz}{p'+q'z}=\frac{pz+q}{p'z+q'} \quad (\gamma)$$

$$-\frac{q'-p'z}{q-pz}=\frac{pz+q}{p'z+q'} \quad (\gamma');$$

d'onde

$$p'=\pm ip, \quad q'=\pm iq=\mp ip, \quad q=\pm p.$$

Podemos, pois, tomar para g_3 uma das quatro fórmas

$$z'=\pm i\frac{z+1}{z-1}, \quad z'=\pm i\frac{z-1}{z+1} \quad (\delta).$$

Dando a g_3 a fórma

$$z'=+i\frac{z+1}{z-1},$$

o producto $g_1 g_3$, (tambem pertencente a G_{12}), é da fórma

$$z'=-i\frac{z+1}{z-1};$$

e facil é verificar que todas as substituições (δ) pertencem a G_{12}, por serem combinações de qualquer d'ellas com g_1 e g_2. Podemos agora escrever todas as substituições de G_{12}, que sam:

$$\text{III}\begin{cases} z'=\pm z, \quad z'=\pm\frac{1}{z}, \quad z'=\pm i\frac{z+1}{z-1}, \quad z'=\pm i\frac{z-1}{z+1} \\ \qquad\qquad z'=\pm\frac{z+i}{z-i}, \quad z'=\pm\frac{z-i}{z+i}, \end{cases}$$

sendo as quatro ultimas as inversas das quatro substituições (δ).

43. Seja G_{24} um grupo do typo

$$(b''') \qquad k_1=2, \quad k_2=3, \quad k_3=4, \quad n=24.$$

Uma analyse analoga á precedente vae indicar-nos a fórma das substituições dos grupos d'este typo. Assim:

Todo o grupo d'esta categoria é holoedricamente isomorpho com o grupo total sobre 4 elementos.

Com effeito, o numero n' de subgrupos de 3.ª ordem de G_{24} será um divisor de 24, satisfazendo á congruencia

$$n' = 1 \pmod 3,$$

e, portanto, só poderá ser $n' = 1$, ou $n' = 4$. A primeira hypothese não póde verificar-se, porque G_{24} conteria invariantes cyclicos de 3.ª ordem, e só os grupos dos dois primeiros typos podem admittir, como vimos, invariantes cyclicos. Será, pois, $n' = 4$.

Sejam

$$(1) \qquad G_3^1,\ G_3^2,\ G_3^3,\ G_3^4$$

os quatro subgrupos possiveis de 3.ª ordem, que sam transformados uns dos outros por meio das substituições de G_{24}. Existirá, analogamente ao que succedia no caso anterior, um grupo transitivo A de substituições sobre os *elementos* (1), isomorpho com G_{24}. Seja k o gráo de meriedria d'esse isomorphismo: a ordem

$$k' = \frac{24}{k}$$

do grupo A deve ser um multiplo de 4, e portanto,

$$k = 1, \quad k = 2, \quad k = 3 \quad \text{ou } k = 6.$$

Se fôsse $k = 6$, seria esta a ordem do subgrupo G_6 de G_{24} correspondente á identidade em A; e como o unico factor s de 6 que satisfaz á congruencia $s = 1 \pmod 3$ é a unidade, o grupo G_6 conteria, em virtude do theorema de SYLOW, um unico subgrupo de 3.ª ordem, cyclico, que seria invariante em G_6 e em G_{24}, o que é impossivel.

Se fôsse $k = 2$, ou $k = 3$, seria cyclico e invariante em G_{24} o subgrupo correspondente á identidade em A. Só póde, pois, ser $k = 1$; o isomorphismo de G_{24} e A é holoedrico, e A é o grupo total sobre os 4 elementos (1).

O grupo G_{24} conterá um subgrupo invariante G_{12}, holoedri-

camente isomorpho do grupo alterno sobre 4 elementos. *Esse subgrupo, que não póde ser cyclico, não póde tambem ser do typo* (II).

Com effeito, se G_{12} fôsse do typo (II), conteria um unico subgrupo cyclico de 6.ª ordem que seria invariante em G_{12} e em G_{24}.

O grupo G_{12} é, pois, necessariamente do typo (III).

Como o indice de G_{12} em G_{24} é 2, basta determinar a fórma de uma substituição g de G_{24}, não pertencente ao subgrupo G_{12}, para obter todas as substituições de G_{24}, que sam as substituições III (n.º 42) e os seus productos por g.

Seja g a substituição de G_{24} correspondente ao cyclo

$$\alpha_4 = (G_3^1\, G_3^2\, G_3^3\, G_3^4)$$

do grupo total, não pertencente ao grupo alterno: g não pertencerá a G_{12}.

Conservando a α_1, α_2, α_3, g_1, g_2, g_3 o significado do n.º 42, verifica-se a relação

$$\alpha_1^{-1}\,\alpha_4\,\alpha_1 = \alpha_4\,; \qquad (\varepsilon)$$

e, portanto,

$$g_1^{-1}\,g\,g_1 = g. \qquad (\varepsilon')$$

A substituição g será da fórma $z' = cz$, ou $z = \frac{c}{z}$. Só a primeira fórma convém, porque todas as substituições $z' = \frac{c}{z}$ sam de periodo 2 e g, correspondente a α_4, é de periodo 4.

Reduzida á forma normal, effectuando uma transformação linear que não altera a fórma normal das substituições III (n.º 42), será

$$g)\; z' = iz.$$

Podemos agora escrever todas as substituições de G_{24}:

$$\text{IV}\begin{cases} z' = \pm z, \quad z' = \pm\frac{1}{z}, \quad z' = \pm i\frac{z+1}{z-1} \\ z' = \pm i\frac{z-1}{z+1}, \quad z' = \pm\frac{z+i}{z-i}, \quad z' = \pm\frac{z-i}{z+i} \\ z' = \pm iz, \quad z' = \pm\frac{i}{z}, \quad z' = \pm\frac{z+1}{z-1} \\ z' = \pm\frac{z-1}{z+1}, \quad z' = \pm i\frac{z+i}{z-i}, \quad z' = \pm i\frac{z-i}{z+i}. \end{cases}$$

44. Seja, finalmente G_{60} um grupo do typo (V):

$$n = 60, \quad k_1 = 2, \quad k_2 = 3, \quad k_3 = 5.$$

O grupo G_{60} *é um grupo simples.*

Não póde, com effeito, conter invariantes cyclicos, como nenhum grupo dos typos (III), (IV), (V). Não terá egualmente invariantes do typo (II) (pondo por emquanto de parte o caso d'esse invariante ser de ordem 4), porque um subgrupo G_1 de G_{60}, do typo (II) e de ordem n, differente de 4, conteria um unico invariante de ordem $\frac{n}{2}$, cyclico, e que seria tambem invariante em G_{60}. Portanto, se G_{60} contiver algum subgrupo invariante, será necessariamente de ordem 12, e do typo (III) [excepto, talvez, no caso de ser do typo (II) e de ordem 4].

Mas esse subgrupo G_{12} de G_{60} só póde conter um subgrupo de ordem 4 e do typo (II), em virtude do segundo theorema de SYLOW, o qual será tambem invariante em G_{60}. Fica assim incluida no caso geral a excepção ha pouco feita.

As substituições d'esse subgrupo G_4 do typo (II), invariante em G_{12} e em G_{60}, serám

$$(1) \qquad z' = \pm z, \quad z' = \pm \frac{1}{z}.$$

Por ser $k_3 = 5$, haverá em G_{60} uma substituição g de periodo 5, que deve ser permutavel com o subgrupo G_4.

A substituição g, ou permuta entre si as substituições (1), o que é impossivel porque não ha uma substituição de periodo 5 sobre tres elementos [as tres substituições (1), não contando a identidade], ou é permutavel com cada uma das substituições (1). Este ultimo caso é egualmente impossivel, porque, sendo g de periodo 5 e permutavel com $z' = -z$, não poderia ser permutavel com $z' = \frac{1}{z}$, porque seria da fórma $z' = \alpha z$, onde α é raiz quinta da unidade.

Portanto, o subgrupo G_{12}, invariante em G_{60}, não póde existir, e o grupo G_{60} é simples, como se queria provar.

O grupo G_{60} *é holoedricamente isomorpho com o grupo alterno sobre 5 elementos.*

Basta mostrar que este isomorphismo existe entre o grupo alterno sobre 5 elementos, *e qualquer grupo simples de ordem 60.*

Com effeito, todo o grupo simples de ordem $60 = 2^2 \times 3 \times 5$

contem subgrupos de ordem 5; o numero d'estes subgrupos será um factor n' de 60, satisfazendo á congruencia $n' = 1 \pmod 5$.

Deverá, pois, ser $n = 6$. Sejam

$$(2) \qquad G_5^1,\ G_5^2,\ G_5^3,\ G_5^4,\ G_5^5,\ G_5^6$$

esses subgrupos, transformados uns dos outros por meio das substituições de G_{60}. Transformando os subgrupos (2) por meio de qualquer substituição de G_{60}, obteremos os mesmos *elementos* (2), em geral, por outra ordem.

Podemos, assim, por um processo identico ao que varias vezes tem sido empregado, construir um grupo A de substituições sobre os elementos (2), isomorpho do grupo G_{60}. Esse isomorphismo é holoedrico, por ser G_{60} um grupo simples.

O grupo A_{60}, transitivo sobre os seis elementos (2), só contem substituições pares, e é, portanto, um subgrupo do grupo alterno G_{360} sobre 6 elementos.

O grupo complementar

$$B = \frac{G_{360}}{A_{60}}$$

é holoedricamente isomorpho com G_{360}, porque o gráo k de meriedria de B em relação a G_{360} é egual á ordem do subgrupo commum a A_{60} e a todos os seus transformados em G_{360}; e esse subgrupo reduz-se á identidade, por ser G_{360} um grupo simples.

Se fôrem (3) $g_1, g_2 \ldots g_6$ os representantes das classes de equivalencia de G_{360}, em relação a A_{60}, será B_{360} o grupo alterno sobre os elementos (3). O subgrupo B' de B_{360}, correspondente a A_{60}, será tambem de ordem 60, e as suas substituições conservam o elemento g_1, representante da classe de equivalencia a que pertencem as substituições de A_{60}. Portanto, B' é o grupo alterno sobre os 5 elementos $g_2, g_3, \ldots g_6$, e, sendo holoedricamente isomorpho com A_{60}, é-o tambem com G_{60}, como se queria demonstrar.

Podemos agora determinar a fórma das substituições do grupo G_{60}.

Todas as substituições do grupo alterno B'_{60}, sobre os cinco elementos $g_2, g_3 \ldots g_6$, se podem obter a partir das substituições generatrizes

$$b'_1 = (g_3\ g_4)\ (g_5\ g_6)$$

$$b'_2 = (g_2\ g_3\ g_4\ g_5\ g_6).$$

Com effeito, todo o grupo formado com b'_1 e b'_2 conterá a substituição

$$b'_3 = (g_3 g_6)(g_5 g_4) = b'^2_2 b'_1 b'^3_2 b'_1 b'^2_2 b'_1,$$

e o subgrupo

$$(4) \qquad 1, \quad b'_1, \quad b'_3, \quad b'_1 b'_3.$$

A sua ordem deverá ser multipla de 5 (periodo de b'_2), de 4 (ordem do subgrupo 4) e de 3 [ordem de $b'_1 b'_2 = (g_2 g_3 g_5)$]; será, portanto, 60.

Representemos por g, g', g'' as substituições de G_{60} respectivamente correspondentes a b'_1, b'_2 e b'_3.

Como a substituição b'_2 é cyclica, de periodo 5, a sua correspondente g' em G_{60} é, depois de reduzida á fórma normal,

$$g') \; z' = \alpha z,$$

onde α é raiz quinta da unidade.

Para determinar a fórma de g'' basta attender a que, entre as substituições b'_2 e b'_3 de B'_{60}, existe a relação

$$(\beta) \qquad b'^{-1}_3 b'_2 b'_3 = b'^4_2.$$

Existirá, portanto, entre as suas correspondentes no grupo holoedricamente isomorpho G_{60}, a relação

$$(\gamma) \qquad g''^{-1} g' g'' = g'^4, \qquad \text{ou} \qquad g' g'' = g'' g'^4.$$

Se representarmos, de um modo geral, g'' por

$$z' = \frac{pz+q}{p'z+q'},$$

a relação (γ) dará

$$(\delta) \qquad \frac{paz+q}{p'az+q'} = \alpha^4 \frac{pz+q}{p'z+q'}.$$

Da relação (δ) concluem-se as seguintes:

$$(\varepsilon) \qquad pp' = 0, \quad qq' = 0, \quad pq' = 0.$$

Como, por outro lado, se deve verificar a relação funda-

mental

$$pq' - qp' \lesseqgtr 0,$$

deverá ser, necessariamente,

$$p = 0, \quad q' = 0.$$

A substituição g'' será, portanto, da fórma

$$g'') \; z' = \frac{q}{p'z}, \quad \text{ou} \quad z' = \frac{c}{z},$$

onde c é uma constante.

Effectuando uma transformação linear, que não altera a fórma de g', podemos dar a g'' a fórma normal

$$g'') \; z' = -\frac{1}{z}.$$

Resta determinar a fórma de g.

Como a substituição g é permutavel com g'', (por ser b_1' permutavel com b_3'), verificar-se-ha a relação

$$(\theta) \qquad gg'' = g''g;$$

ou (representando g, de um modo geral, por

$$g) \; z' = \frac{p_1 z + q_1}{p_1' z + q_1'}\Big),$$

$$(\theta') \qquad \frac{q_1 z - p_1}{q_1' z - p_1'} = -\frac{p_1' z + q_1'}{p_1 z + q_1}.$$

A identidade (θ') equivale ás seguintes:

$$(k) \qquad p_1 q_1 + p_1' q_1' = 0, \quad p_1^2 + p_1'^2 = q_1^2 + q_1'^2.$$

Como, por outro lado, a substituição g é de periodo 2, será

$$g^2) \; z' = \frac{(p_1^2 + q_1 p_1') z + q_1 (p_1 + q_1')}{p_1' (p_1 + q_1') z + p_1^2 + q_1 p_1'}$$

a identidade; e, portanto,

$$p_1 = -q_1'.$$

As identidades (k) equivalem, pois, ás seguintes

(k') $\qquad p_1 = -q_1' \quad$ e $\quad p_1' = q_1$;

e a substituição g é da fórma

$$g)\ z' = \frac{p_1 z + q_1}{q_1 z - p_1}.$$

Podemos exprimir os coefficientes p_1 e q_1 em α (raiz primitiva do gráo 5 da unidade).

Como entre b_1', b_2' e b_3' se verifica a relação

$$b_3' = b_2'^2 b_1' b_2'^3 b_1' b_2'^2 b_1',$$

dar-se-ha tambem, entre as suas correspondentes em G_{60}, a relação

(μ) $\qquad g'' = g'^2 g\, g'^3 g\, g'^2 g.$

Substituindo g, g' e g'' pelas suas expressões, a identidade (μ) converter-se-ha na seguinte:

(μ') $\qquad \dfrac{p_1 - q_1 z}{p_1 z + q_1} = \dfrac{(p_1^2 \alpha^3 + q_1^2 \alpha^4) z + (1 - \alpha^2) p_1 q_1}{(1 - \alpha^2) p_1 q_1 z + (\alpha^3 q_1^2 + p_1^2)}$;

ou ainda

(ν) $\qquad p_1^2 (1 + \alpha^2) + q_1^2 (\alpha^3 + \alpha^4) = 0.$

Por ser α raiz quinta da unidade, será

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha = -1;$$

e a egualdade (ν) poderá escrever-se

$$\frac{p_1^2}{q_1^2} = \frac{(\alpha^4 - \alpha)^2}{(\alpha^2 - \alpha^3)^2}.$$

Portanto, á substituição g podemos dar a fórma

$$g)\ z' = \frac{(\alpha^4 - \alpha)z + (\alpha^2 - \alpha^3)}{(\alpha^2 - \alpha^3)z - (\alpha^4 - \alpha)}.$$

Conhecida a fórma das substituições g, g', g'', ficam determinadas todas as substituições do grupo G_{60}, de que ellas sam generatrizes.

Fazendo

$$\alpha^4 - \alpha = u, \quad \alpha^2 - \alpha^3 = v,$$

as substituições de G_{60} serám

$$\mathrm{V}\begin{cases} z' = z, \quad z' = \alpha z, \quad z' = \alpha^2 z, \quad z' = \alpha^3 z, \quad z' = \alpha^4 z \\ z' = -\dfrac{1}{z}, \quad z' = -\dfrac{\alpha}{z}, \quad z' = -\dfrac{\alpha^2}{z}, \quad z' = -\dfrac{\alpha^3}{z}, \quad z' = -\dfrac{\alpha^4}{z}, \\ z' = \alpha^t \dfrac{u\alpha^r z + v}{v\alpha^r z - u} \\ z' = \alpha^t \dfrac{u\alpha^r z - v}{v\alpha^r z + u} \end{cases} \begin{pmatrix} r = 0,\ 1,\ 2,\ 3,\ 4 \\ t = 0,\ 1,\ 2,\ 3,\ 4 \end{pmatrix}.$$

VII

Representação geometrica dos grupos finitos de substituições lineares: grupos dos polyedros regulares

45. Acabamos de vêr que ha cinco categorias possiveis de grupos finitos de substituições lineares sobre uma variavel. É possivel fazer-lhes corresponder, por isomorphismo holoedrico, outros tantos typos de grupos de movimentos (rotações), effectuados sobre determinados polyedros.

Obtem-se assim, por isomorphismo, uma representação geometrica dos grupos finitos de substituições lineares, que ao mesmo tempo explica a nomenclatura, que usualmente os designa, de *grupos dos polyedros regulares*.

46. Sejam Ox e Oy os dois eixos do plano da variavel complexa $z = x + iy$ a que se acham referidos os valores d'esta variavel.

Consideremos um terceiro eixo Ot, orthogonal aos outros dois, e uma esphera de centro em O e de raio egual a 1.

Projectando stereographicamente a esphera, a partir do pólo

$$x = 0, \quad y = 0, \quad t = 1,$$

sobre o plano da variavel z, a cada ponto da esphera corresponde, por projecção, um ponto unico sobre o plano. Ao pólo da projecção correspondem no plano os pontos no infinito.

Estabelece-se assim uma correspondencia biunivoca entre os pontos dos dois logares geometricos.

Supponhamos que a esphera gira sobre si mesma, em volta do seu centro.

Os movimentos da esphera sobre si mesma sam operações agrupaveis.

Com effeito, dois movimentos successivos podem compôr-se num movimento unico, *producto* dos dois movimentos elementares, verificando-se para tres ou mais movimentos successivos a lei associativa.

Qualquer movimento da esphera sobre si mesma é o producto de tres rotações elementares em torno dos tres eixos Ox, Oy, Oz.

Supponhamos que a esphera soffre um movimento M, sobre si mesma, que conduz o pólo (0,0,1) ao ponto (x, y, t), ou, em projecção, o ponto $z = \infty$ ao ponto z'. Podemos reconduzir novamente o ponto z' ao pólo, por meio de duas rotações elementares: uma, R_x, em torno do eixo Ox, que conduz z' ao plano xz; e outra, R_y, em torno de Oy, que conduz z' ao pólo.

Portanto, o producto

$$MR_x R_y$$

deixa fixo o pólo $z = \infty$ e egualmente o pólo opposto $z = 0$; é uma rotação em torno de Ot:

$$MR_x R_y = R_t.$$

D'onde, $M = R_t R_y^{-1} R_x^{-1}$, como se queria demonstrar.

47. Cada *movimento* M da esphera sobre si mesma corresponde a uma *substituição* S sobre a variavel z. A substituição S será a representação analytica do movimento M.

Theorema. — *Qualquer que seja o movimento* M *da esphera sobre si mesma, a substituição correspondente* S *é linear da fórma*

$$(1) \qquad S)\, z' = \frac{pz + q}{p'z + q'}.$$

Demonstrado que qualquer movimento da esphera sobre si mesma é o producto de tres rotações em volta, respectivamente, de cada um dos tres eixos coordenados, basta mostrar que:

Uma rotação da esphera, em torno de qualquer dos eixos coordenados, corresponde a uma substituição linear sobre a variavel z.

a) Seja M uma rotação de amplitude θ, em torno do eixo O_x, no sentido positivo.

Representemos por (x, y, t) as coordenadas de um ponto qualquer P da esphera, antes da rotação, e por (x, y, 0) as coorde-

nadas da sua projecção stereographica P', a partir do pólo (0, 0, 1), sobre o plano xy. Sejam, respectivamente, (x', y', t') e $(x', y', 0)$ as coordenadas de P e P', depois de effectuada a rotação.

O movimento M equivale á substituição da variavel $z = x + iy$ por $z' = x' + iy'$.

Vamos achar a expressão de z' em z.

Como a recta PP' passa pelo pólo, verificar-se-ham as relações

$$(2)\quad x = \frac{x}{1-t};\quad y = \frac{y}{1-t};\quad z = x + iy = \frac{x+iy}{1-t};$$

e egualmente

$$(2')\quad x' = \frac{x'}{1-t'};\quad y' = \frac{y'}{1-t'};\quad z' = x' + iy' = \frac{x'+iy'}{1-t'}.$$

Substituindo, na expressão de z', as coordenadas x', y', t' pelas suas expressões em x, y, t, dadas pelas equações

$$(3)\quad \begin{cases} x' = x \\ y' = y\cos\theta + t\,\mathrm{sen}\,\theta \\ t' = y\,\mathrm{sen}\,\theta + t\cos\theta, \end{cases}$$

vem

$$(4)\quad z' = \frac{x - iy\cos\theta + it\,\mathrm{sen}\,\theta}{1 - y\,\mathrm{sen}\,\theta - t\cos\theta}.$$

A partir das equações (2) obtêem-se as expressões de x, y, t em x, y, que, substituidas na expressão de z' conduzem, depois de posta em evidencia a variavel $z = x + iy$, á relação

$$(5)\quad z' = \frac{z\cos\frac{\theta}{2} + i\,\mathrm{sen}\,\frac{\theta}{2}}{iz\,\mathrm{sen}\,\frac{\theta}{2} + \cos\frac{\theta}{2}},$$

que é linear, como se queria provar.

b) Seja agora M uma rotação de amplitude θ, no sentido positivo, em torno de Oy.

As equações de transformação das coordenadas sam agora:

$$(6)\qquad \begin{cases} x' = x\cos\theta + t\,\mathrm{sen}\,\theta \\ y' = y \\ t' = -x\,\mathrm{sen}\,\theta + t\cos\theta, \end{cases}$$

e, portanto, em virtude da ultima equação (2'),

$$(7)\qquad z' = \frac{x\cos\theta + iy + t\,\mathrm{sen}\,\theta}{1 + x\,\mathrm{sen}\,\theta - t\cos\theta}.$$

Substituindo x, y, t, pelos seus valores em x e y, dados por (2), e pondo z em evidencia, vem

$$(8)\qquad z' = \frac{z\cos\frac{\theta}{2} - \mathrm{sen}\,\frac{\theta}{2}}{z\,\mathrm{sen}\,\frac{\theta}{2} + \cos\frac{\theta}{2}};$$

z' é expresso linearmente em z, como no 1.° caso.

c) Supponhamos, finalmente, que o movimento M da esphera, sobre si mesma, é uma rotação em torno de Oz, no sentido positivo e de amplitude θ.

As equações de transformação sam agora:

$$(9)\qquad \begin{cases} x' = x\cos\theta - y\,\mathrm{sen}\,\theta \\ y' = x\,\mathrm{sen}\,\theta + y\cos\theta \\ t' = t \end{cases}$$

e, portanto,

$$(10)\qquad z' = \frac{x\cos\theta - y\,\mathrm{sen}\,\theta + i\,(x\,\mathrm{sen}\,\theta + y\cos\theta)}{1 - t}$$

$$= z\,(\cos\theta + i\,\mathrm{sen}\,\theta).$$

α) Os coefficientes das substituições lineares correspondentes a cada uma das rotações elementares, expressas por (5), (8) e (10), verificam a relação

$$(11)\qquad pq' - p'q = 1.$$

A esta mesma relação satisfazem, portanto, os coefficientes da substituição linear correspondente a qualquer movimento da esphera sobre si mesma.

β) Nas mesmas substituições (5), (8) e (10), os coefficientes p e q' sam conjugados; bem assim p' e $-q$.

Toda a substituição linear (1), cujos coefficientes satisfazem ás duas condições (α) e (β), é chamada uma *substituição de* CAYLEY.

Todo o movimento da esphera sobre si mesma corresponde, pois, analyticamente a uma substituição linear de CAYLEY sobre a variavel z.

Os dois pólos de uma tal substituição sam as raizes da equação

$$p'z^2+(q'-p)z-q=0;$$

da condição (β) resulta que, se uma d'ellas fôr z, a outra será $-\frac{1}{z_1}$, onde z_1 representa o conjugado de z.

É facil vêr que os pontos da esphera, projectados em z e $-\frac{1}{z_1}$, sam diametralmente oppostos; portanto, o movimento da esphera sobre si mesma, analyticamente representado por uma substituição de CAYLEY, é uma rotação em torno de um diametro.

48. Sendo operações agrupaveis os movimentos da esphera sobre si mesma, haverá tambem cinco typos de *grupos finitos* de rotações, holoedricamente isomorphos dos cinco typos possiveis de substituições lineares sobre uma variavel.

Vamos construir directamente esses grupos de rotações.

Inscrevendo ou circunscrevendo á esphera um polyedro regular, *as rotações que sobrepõem o polyedro a si mesmo formam um grupo*. Essa sobreposição póde effectuar-se, fazendo coincidir um vertice com cada um dos outros, podendo obter-se a coincidencia dos vertices a e b por duas rotações distinctas.

A ordem n do grupo de rotações relativo ao polyedro P, com v angulos solidos e m arestas em cada angulo solido, será, pois,

$$n=vm.$$

Dois polyedros polares um do outro, o octaedro e o cubo, o dodecaedro e o icosaedro, não originam, manifestamente, grupos distinctos.

Dos cinco polyedros regulares, só tres, portanto, conduzem a grupos finitos differentes de rotações: o *tetraedro*, o *octaedro* e o *icosaedro*.

Consideremos mais os dois polyedros seguintes:

1.º Uma pyramide regular tendo por base um polygono de qualquer numero de lados, inscripto num circulo maximo qualquer da esphera e o vertice no pólo d'esse circulo;

2.º Uma dupla pyramide, formada pela anterior e pela symetrica em relação ao plano da base.

Sam estes, como vamos vêr, os cinco polyedros que dam origem aos cinco grupos finitos de rotações, holoedricamente isomorphos dos grupos finitos de substituições lineares.

1.º *Grupo da pyramide regular ou cyclico.* — A pyramide regular sobrepõe-se a si mesma por um grupo de rotações em torno do seu eixo. Esse grupo é constituido pelas potencias de uma mesma rotação, de amplitude $\frac{2\pi}{n}$, se fôr n o numero de lados da base da pyramide: é um *grupo cyclico*, holoedricamente isomorpho de um grupo de substituições lineares do typo I.

Se o plano da base da pyramide fôr o plano xy, e o vertice o pólo (0, 0, 1), as substituições do grupo isomorpho correspondente têem a fórma *normal* $z' = \alpha^i z$.

Qualquer que seja a orientação da pyramide, podemos conduzi-la á orientação *normal*, por meio de uma rotação conveniente, *o que equivale a uma transformação linear da variavel z.*

2.º *Grupo da dupla pyramide ou diedral.* — Sobrepõem a dupla pyramide a si mesma as rotações do grupo anterior e mais n rotações de amplitude π, em torno, respectivamente, dos raios e apothemas da base.

O grupo da pyramide regular é, portanto, um subgrupo de indice 2 do grupo diedral. Se fôr M uma rotação de amplitude π, e S uma rotação do grupo cyclico, será

$$M^{-1}SM = S,$$

o que mostra que o subgrupo cyclico é invariante no grupo diedral.

O grupo isomorpho de substituições lineares, correspondente ao grupo diedral pela fórmula de Cayley, é o grupo do typo II.

Se o plano da base da pyramide fôr o plano xy e um dos vertices da base fôr o ponto $z = i$, as substituições do grupo isomorpho correspondente têem a fórma normal II. Aquella será, portanto, a *orientação normal* da dupla pyramide.

3.° *Grupo do tetraedro.* — A ordem d'este grupo é

$$n = vm = 4 \times 3 = 12.$$

Tem 8 rotações de periodo 3, em torno dos 4 eixos de symetria ternaria do tetraedro, e 3 rotações de periodo 2, em torno dos 3 eixos de symetria binaria (passando cada um d'elles pelos meios de duas arestas oppostas).

Os 8 pólos das rotações de periodo 3 dividem se por duas classes de equivalencia: a dos 4 vertices e a dos 4 pólos oppostos. Os 6 pólos das rotações de periodo 2 pertencem todos á mesma classe.

Admitte o grupo tetraedral 4 subgrupos cyclicos de 3.ª ordem, cada um d'elles formado pelas rotações em torno de um mesmo eixo ternario; e 6 subgrupos de 2.ª ordem, cada um d'elles formado pelas rotações em torno de cada eixo binario.

Todas as rotações do grupo se podem obter a partir de tres rotações generatrizes: duas de periodo 2, em torno, respectivamente, de dois quaesquer dos eixos binarios, e uma de periodo 3 em torno de um dos eixos ternarios.

Por todas estas propriedades se verifica que o grupo do tetraedro é holoedricamente isomorpho com o grupo de substituições lineares do typo III.

Demos ao tetraedro uma orientação tal que um dos eixos binarios coincida com o eixo Ot e os planos determinados por esse eixo e por cada uma das arestas que elle encontra sejam os bissectores dos diedros formados pelos planos xt e yt.

As tres rotações elementares serám então representadas, por exemplo, por

$$z' = -z, \quad z' = \frac{1}{z} \quad \text{e} \quad z' = i\frac{z+1}{z-1}.$$

Aquella é, portanto, a *orientação normal* do tetraedro.

4.° *Grupo do octaedro.* — A ordem deste grupo de rotações é

$$n = vm = 6 \times 4 = 24.$$

Ha no octaedro tres categorias de eixos de rotação, respectivamente de symetria quaternaria, ternaria e binaria; o grupo octaedral contem, por isso, rotações de periodos 4, 3 e 2. Cada uma das rotações do grupo octaedral corresponde a uma substituição sobre os 4 eixos de symetria ternaria. *Essas substituições*

..

sam todas distinctas e o grupo octaedral é, por isso, holoedricamente isomorpho com o grupo total sobre 4 elementos.

Ha 12 rotações no grupo octaedral, formando um subgrupo de indice 2, que sobrepõem a si mesmo cada um dos dois tetraedros hemiedricos do octaedro; as 12 restantes permutam os dois tetraedros. O grupo tetraedral é, portanto, *invariante* no grupo do octaedro.

Todas estas propriedades do grupo octaedral verificam o seu isomorphismo holoedrico com o grupo de substituições lineares do typo IV.

Determinada a *orientação normal* do tetraedro (3.°), a do octaedro fica egualmente conhecida: os tres eixos de symetria quaternaria do octaedro deverám coincidir com os tres eixos coordenados. Das tres generatrizes do grupo octaedral, duas sam tambem generatrizes do grupo do tetraedro; a terceira é uma rotação cyclica de periodo 4, em torno de Ot, correspondente, pela fórmula de CAYLEY, á generatriz

$$g)\ z' = iz$$

do grupo de substituições lineares do typo IV.

5.° *Grupo do icosaedro.* — A ordem d'este grupo é

$$n = vm = 12 \times 5 = 60,$$

visto que o icosaedro tem 12 angulos solidos pentaedros.

Sam eixos de rotação os 6 diametros do icosaedro, os 10 eixos que passam pelos centros das faces oppostas, e os 15 eixos que unem os meios das arestas oppostas.

As rotações do grupo relativas a estes eixos sam, respectivamente, de periodos 5, 3 e 2.

Podemos distribuir os 15 eixos de symetria binaria (passando pelos meios de duas arestas oppostas) em 5 systemas, cada um d'elles formado por 3 eixos orthogonaes entre si. Sejam

$$(1) \qquad e_1,\ e_2,\ e_3,\ e_4,\ e_5$$

esses systemas.

Uma rotação R de amplitude $\frac{2}{5}\pi$, em torno de um diametro do icosaedro, corresponde a uma *substituição cyclica* α sobre os elementos (1):

$$\alpha = (e_1\, e_2\, e_3\, e_4\, e_5).$$

Uma rotação R′ de amplitude π, em torno de um eixo de symetria binaria, por exemplo, um eixo do systema e_1, corresponde á substituição

$$\alpha' = (e_2\, e_3)\,(e_4\, e_5)$$

sobre os elementos (1).

Como todas as substituições do grupo icosaedral se podem obter a partir das duas generatrizes R e R′, este grupo será isomorpho do grupo de substituições que tem como generatrizes α e α', *que é o grupo alterno sobre os 5 elementos* (1).

Isto basta para verificar o isomorphismo holoedrico do grupo do icosaedro com o grupo de substituições lineares do typo V, e com o grupo modular sobre $4+1$ elementos.

Os tres eixos binarios do systema e_1 sam os eixos de um octaedro regular inscripto no icosaedro. Se considerarmos uma rotação de amplitude π, em torno de cada um d'esses eixos, essas tres rotações formam com a identidade um subgrupo do typo II, de ordem 4, do grupo icosaedral: é um *Vierergruppe,* na nomenclatura de KLEIN. Sam 5, portanto, os *Vierergruppen* subgrupos do grupo do icosaedro.

A *oriéntação normal* do icosaedro obtem-se, fazendo coincidir um dos diametros com Ot e levando uma das arestas que concorrem no pólo (0, 0, 1) a coincidir com o plano xt, do lado dos xx positivos. Com effeito, á rotação R corresponderá a substituição

$$z' = \alpha z, \tag{2}$$

(onde α é raiz quinta da unidade).

Seja agora $z = k$ a projecção do vertice do icosaedro que existe no plano xt, com coordenadas positivas: será k real e positivo. A rotação R′ de amplitude π, em torno do eixo binario que une os meios das duas arestas existentes no plano xt, corresponde, como facilmente se vê, a substituição

$$z' = \frac{(\alpha^4 - \alpha)z + (\alpha^2 - \alpha^3)}{(\alpha^2 - \alpha^3)z - (\alpha^4 - \alpha)}. \tag{3}$$

Sam (2) e (3) as *fórmas normaes* das substituições generatrizes do grupo do typo V.

49. Os cinco typos de grupos finitos de *rotações,* representando geometricamente os grupos de substituições lineares,

não sam os grupos mais geraes de *transformações* da esphera em si mesma. Além dos movimentos da esphera até aqui considerados (rotações), cumpre attender áquelles em que a figura primitiva e a transformada sam *inversamente eguaes:* sam os chamados *movimentos de 2.ª especie.* Se fôr z_1 o conjugado de z, a substituição $z = z_1$ corresponde geometricamente a uma transformação da figura dada na sua symetrica em relação ao plano xt.

Combinando a substituição $z = z_1$ com a substituição de CAYLEY

$$z' = \frac{pz + q}{p'z + q'} \quad (pq' - p'q = 1),$$

(onde sam conjugados p e q', p' e $-q$), a qual representa o movimento mais geral de 1.ª especie (rotação), obtemos a representação analytica

$$z' = \frac{pz_1 + q_1}{p'z_1 + q'} \quad (pq' - p'q = 1)$$

de um movimento qualquer de 2.ª especie.

É possivel considerar grupos finitos de movimentos de 1.ª e 2.ª especie da esphera em si mesma: esses grupos conterám como invariantes de indice 2 os grupos dos polyedros regulares.

INDICE

ERRATAS

Pag.	linha	onde se lê:	leia-se:
10	11	g'	G'
11	21 e 23	g'_α	$g'_{\alpha'}$
12	4	$g_{\gamma'}$	g_γ
»	30	$\frac{m'}{k}$	$\frac{n}{k}$
14	7	indice	periodo
22	7	subgrupo G	subgrupo de G
26	10	$g'g^{-\frac{i}{k_2}}$	$g'g_1^{-\frac{i}{k_2}}$
29	16	systema	grupo
31	19	α_k	α^k
»	20	α_k	α^k
37	23	em (1).	em (1) (n.º 25).
37	33	$q'p_1$	$p'q_1$
44	16	$(g^{-1}g_ig)k^{-1}$	$(g^{-1}g_ig)^{k^{-1}}$
51	7, 10, 11, 13	g_1 ou g'_1	g_i ou g_i
63	12	grupo	grupos

Mira Fernandes

THEORIA de GALOIS