DR. CHAIM SAMUEL HÖNIG

SÔBRE UMA GENERALIZAÇÃO DOS NÚMEROS REAIS E SUA APLICAÇÃO NA CLASSIFICAÇÃO DOS GRUPOS SEM TORÇÃO

Tese apresentada no concurso para provimento da Cadeira de Complementos de Matemática da Faculdade Nacional de Filosofia, Ciências e Letras da Universidade do Brasil.

S. PAULO, 1959

Ao amigo e colega Lyra
com os meus agradecimentos
Haim
21. 3013159

Dr. Chaim Samuel Hönig.

SÔBRE UMA GENERALIZAÇÃO DOS NÚMEROS REAIS E SUA APLICAÇÃO NA CLASSIFICAÇÃO DOS GRUPOS SEM TORÇÃO.

Tese apresentada ao concurso para provimento da Cadeira de Complementos de Matemática da Faculdade Nacional de Filosofia, Ciências e Letras da Universidade do Brasil.

S.Paulo - 1959.

INTRODUÇÃO.

Os números reais são obtidos completando-se o corpo dos números racionais Q relativamente à sua topologia habitual. Podemos porém introduzir outras topologias em Q e obter corpos completados diferentes, por exemplo, o corpo dos números p-ádicos. Se apenas exigirmos que a topologia introduzida em Q seja compatível com a sua estrutura de anel e não com a sua estrutura de corpo (isto é, a aplicação $x \longrightarrow x^{-1}$ não é necessàriamente contínua) então obtemos um conjunto abundante de topologias sôbre Q (conjunto êste que tem a potência do contínuo) e para cada uma dessas topologias τ podemos considerar o anel completado $\hat{Q}_\tau$. Temos em vista particularmente as topologias τ de anel sôbre Q nas quais um sistema fundamental de vizinhanças de zero é formado por subgrupos de Q. São os elementos do completado de Q com esta topologia que chamamos de números reais generalizados. Neste trabalho apenas precisamos de uma parte do completado, isto é, o completado do sub-anel Z dos inteiros e os elementos de $\hat{Z}_\tau$ nos servirão na classificação dos subgrupos de Q^n e mais geralmente dos grupos sem torção (a classificação será feita por matrizes de ordem $n \times n$ de elementos de $\hat{Z}_\tau$ ou por matrizes transfinitas no caso geral).

Seria talvez mais acertado chamar os elementos de $\hat{Z}_\tau$ de números inteiros generalizados assim como os elementos do completado de Z no corpo dos números p-ádicos são chamados de inteiros p-ádicos.

Os números reais generalizados nos surgiram naturalmente no problema da classificação dos grupos sem torção substituindo os números p-ádicos que Kurosh havia utilizado para classificar os grupos p-primitivos.

O interêsse pelo estudo e pela classificação dos subgrupos de Q^n e mais geralmente pelos grupos sem torção foi despertado por um exemplo de Pontrjagin (1934) [P], que mostra que um subgrupo de Q^2 não é necessàriamente produto direto, contradizendo assim alguns dos resultados de Alexander e Cohen [AC], de Pietrkowski [Py], de van Dantzig [v.D-1]. Ver p. 43, ou, [P] p. 384.

Os subgrupos G de Q^n não sendo necessàriamente produto direto de subgrupos de Q a sua classificação não se reduz trivialmente à classificação dêstes últimos. Inspirado no exemplo de Pontrjagin, Kurosh estudou os grupos G de pôsto finito e p-primitivos, isto é, tais que existe um subgrupo livre H de G e tal que para qualquer x de G existe um inteiro m tal que $p^m x \in H$. Naturalmente êsses grupos formam uma categoria muito particular de grupos de pôsto finito, mas Kurosh conseguiu uma classificação completa dêsses grupos usando para isso matrizes de ordem n n cujos elementos são inteiros p-ádicos. Para isto, grosso modo, mostrou que o grupo G é reunião de uma sequência estritamente crescente H_r de subgrupos livres de G, subgrupos êstes que têm bases tais que a passágem da base de um para a base do seguinte é essencialmente feita por uma matriz M_r de inteiros cujos elementos $m_{ij}^{(r)}$ satisfazem $0 \leqslant m_{ij}^{(r)} < p$ e reuniu tôdas essas matrizes numa só matriz $\mathfrak{M}$ cujos elementos são inteiros p-ádicos. Kurosh achou condições necessárias e suficien-

entes para que uma matriz $\mathcal{M}$ esteja associada a um grupo G (p-primitivo) e demonstrou a existência de grupos não completamente redutíveis e que êstes constituem a"maioria".

Kurosh suspeitou que os "números ideais de Prüfer" (que são essencialmente os elementos dos aneis $\hat{Z}_c$ apresentados por sistemas de congruências que substituem os ideais) teriam um papel a desempenhar na extensão de seus resultados à classificação de subgrupos quaisquer de pôsto finito.

"Outro desenvolvimento possível na teoria dos grupos abelianos sem torção seria a passágem (do estudo) de grupos p-primitivos ao estudo de grupos quaisquer de pôsto finito. Nesse desenvolvimento os números "ideais" ou "universais" de Prüfer talvez tenham um papel a desempenhar, mas isto não será uma generalização trivial dos resultados do presente artigo". Kurosh, [K] p.177. Parece porém que esta idéia de Kurosh não encontrou éco ou então não deu frutos.

Posteriormente houve duas classificações que tentavam extender a classificação de Kurosh a grupos quaisquer de pôsto finito, isto é, essencialmente , subgrupos de Q^n. Referimo-nos à classificação de Derry [D] e à de Szekeres [Sz]; êste último aliás classificou os grupos enumeráveis e sem torção. Essas classificações também são feitas por meio de matrizes porém não apresentam a simplicidade da classificação de Kurosh no sentido de poder obter de modo simples o grupo a partir das matrizes e recíprocamente.

A classificação de Derry nos faz "sair" do grupo G que queremos classificar. Derry considera G como intersecção de uma infinidade de grupos G_p p-primitivos (p percorrendo

o conjunto dos números primos) e a cada G_p associa uma matriz M_p de elementos p-ádicos e esta família $(M_p)_{p \in P}$ de matrizes (naturalmente satisfazendo certas condições) associa , os grupos G_p e obtem $G = \bigcap_{p \in P} G_p$. Vemos pois que é extremamente difícil ter alguma idéia sôbre o grupo G a partir das matrizes M_p. Aliás, Kurosh suprime, na segunda edição do seu livro [K2], a classificação de Derry, que havia exposto na primeira edição, dizendo textualmente que "O método de apresentar grupos por sistemas de matrizes p-ádicas foi omitido (nesta edição) por ser de pouca ajuda no estudo dêstes grupos". [K 2], p. 8.

A classificação de Szekeres é mais satisfatória no sentido de que o grupo G é obtido como uma reunião de subgrupos $G_{(p)}$ de G. Para isto toma um subgrupo livre H de G com mesmo pôsto que G e define $G_{(p)} = \{x \in G \mid \exists\ p^m x \in H\}$ e a cada um dêstes grupos associa uma matriz M_p de números p-ádicos.

Infelizmente tanto a intersecção qualquer como a reunião qualquer de grupos não goza de nenhuma propriedade privilegiada como gozam os limites indutivos ou os limites projetivos de modo que as classificações de Derry e Szekeres não permitem por exemplo, abordar o estudo dos grupos duais e sua classificação ou outros problemas "naturais".

A classificação que propomos é muito mais simples e generaliza diretamente as idéias e os métodos de Kurosh: enquanto Derry e Szekeres precisam de uma infinidade de matrizes p-ádicas, em nossa classificação basta uma infinidade de matrizes inteiras ou simplesmente uma matriz (q_r)-ádica e além disto a relação entre a matriz e o grupo é muito natural e simples prestando-se à aplicações.

Para realizar esta classificação introduzimos as noções de sequência característica e de sequência crescente de geradores ou, o que é essencialmente equivalente, a noção de sequência principal (q_r) de um grupo G e obtemos o grupo como reunião de uma sequência estritamente crescente de subgrupos livres H_r de G e definimos em cada H_r as chamadas bases canônicas (Hauptsystem de Kurosh) de tal modo que a passágem da base do grupo H_r para o grupo H_{r+1} é feita por uma matriz $M_r = (m_{ij}^{(r)})$ que, entre outras, goza da propriedade de que seus elementos que não estão sôbre a diagonal satisfazem à condição $0 \leqslant m_{ij}^{(r)} < q_r$; reunimos essas matrizes M_r numa só matriz $\mathfrak{M}$ de ordem $n \times n$ (n = pôsto de G) de números (q_r)-ádicos. G é portanto limite indutivo dos subgrupos H_r e então seu grupo dual G é o limite projetivo dos grupos H_r que são toros de dimensão n e de fato a matriz $\mathfrak{M}$ dá êste limite projetivo de modo muito fácil [H 2].

Repetimos: as idéias básicas que nos permitiram associar a subgrupos de Q^n as matrizes são as de característica de um grupo em relação a um subgrupo e a de sequência crescente de geradores, que por sua vez leva a noção de sequência de fatores, de sequência principal e a de número (q_r)-ádico.

Tôdas essas noções giram em torno da mesma ordem de idéias e parte delas (as sequências características) já havia aparecido na classificação dos subgrupos de Q [H 1]. Procuramos então unificar os tratamentos dessas diferentes noções e os o-ideais revelaram-se adequados para isto, permitindo unificar não só o estudo da classificação dos subgrupos de Q e da noção de característica de um grupo em relação a um subgrupo, como ainda serviu para tratar de um modo simples as topologias de ideais sôbre $\mathbb{Z}$.

Façamos alguns comentários sôbre os diversos capítulos desta tese:

Depois de ter recordado ràpidamente no capítulo I as principais noções da teoria dos conjuntos ordenados, da teoria dos grupos, etc. que usamos neste trabalho damos no capítulo II, parágrafo 1º, um estudo detalhado dos o-ideais, das sequências características, dos sistemas crescentes de geradores e sequências principais que vão servir, como já dissemos, para a classificação dos subgrupos de Q, para o estudo de subgrupos de Q^n e das topologias de ideais sôbre Z.

No parágrafo 2º do capítulo II definimos os aneis $Z(\hat{b_n})$ e damos o desenvolvimento de seus elementos como sequências (desenvolvimentos (b_n)-ádicos) pois é sob esta forma que vamos usar êsses elementos. Os números reais generalizados que apresentamos já são bem conhecidos na literatura, sob uma forma ou outra. Parece que a primeira apresentação deles foi feita por Prüfer [Pf]. Os chamados números ideais de Prufer são os elementos "ideais" que são acrescentados a um anel para satisfazer a um sistema de congruências. Pietrkowsky [Py] percebeu que atraz desta idéia de juntar elementos a um anel estava o processo de completação topológica. A primeira formulação em têrmos modernos satisfatórios foi feita por van Dantzig em [D1], o qual essencialmente considera as topologias (em aneis) que têm um sistema fundamental de vizinhanças formado por ideais b_ν (que chamamos simplesmente de topologia de ideais neste trabalho) e considera o completado dêste anel topológico, chamando os elementos do anel completado de números b_ν-ádicos.

Os números reais generalizados são obtidos simplesmente como um caso particular do caso acima quando o anel em questão é

Z. Neste caso particular porém é possível dar uma representação dêstes elementos por sequências, representação esta que chamamos de (b_n)-ádica e que é essencial para o presente trabalho. No caso geral uma representação destas não é possível e por isto nossa classificação não se estende a anéis principais quaisquer. Esta representação generaliza a habitual representação por sequências dos números p-ádicos.

No capítulo III damos agora de modo muito rápido (é verdade que usamos tôda a teoria dos o-ideais) a classificação dos subgrupos de Q que já tínhamos publicado em 1950 [H 1]. Na mesma época também apareceu uma classificação bastante semelhante à nossa [B Z] e posteriormente verificamos que a idéia básica para esta classificação, a de sequência característica, já se encontra em outros autores [B], [L], [Py], que dela fazem interessantes aplicações.

No capítulo IV começamos dando exemplos de subgrupos de Q^2 que não podem ser decompostos em produto direto de grupos de pôsto 1. Apresentamos também um exemplo que é muito mais simples do que os que conhecemos na literatura. No parágrafo 2º, os resultados principais são os teoremas 26 e 28. No § 3º, temos o teorema 29 que é essencialmente de Kurosh [K], p. 185. Outro resultado fundamental é o teorema 36. No §4º, dados os teoremas que permitem associar ao grupo G uma sequência de matrizes que satisfazem determinadas condições e damos os últimos teoremas (teorema 44) que permitirão demonstrar que essas condições também são suficientes para que uma sequência de matrizes esteja associada a um grupo (teorema 46) e completamos nossa classificação nos teoremas 47 e 48.

O têrmo classificação se justifica pois classificar determinados entes, é estabelecer uma correspondência biunívoca entre êstes entes e outros mais simples e dizemos então que êstes últimos classificam os primeiros. Assim para dar exemplos apenas desta tese podemos dizer que as sequências características classificam as topologias de ideais em Z (cap. II, § 2º, teorema 10) ou ainda, no capítulo IV, classificamos os grupos G tais que $Z^n \subset G \subset Q^n$ por meio de matrizes $\mathfrak{M}$ de ordem $n \times n$ cujos elementos estão num determinado anel (dependendo do que chamamos característica do grupo).

A matriz $\mathfrak{M}$ que associamos a um grupo G não é um invariante dêste grupo no sentido de que não é a mesma para qualquer grupo isomorfo a G. A matriz $\mathfrak{M}$ depende da particular imersão de G em Q^n, mas considerando G como subgrupo de Q^n classificamos então completamente êstes grupos pois estabelecemos uma correspondência biunívoca entre êstes grupos e as matrizes e podemos ainda definir a partir das matrizes alguns invariantes do grupo G, o seu tipo e os p-pôstos reduzidos.

Os resultados obtidos ainda se extendem trivialmente a grupos sem torção de pôsto qualquer se os considerarmos como subgrupos de $Q^{(L)}$, L sendo um conjunto bem ordenado (ver o fim do cap. IV, §4º, nº3) mas neste caso não mais sabemos definir invariantes a partir da matriz transfinita associada ao grupo.

A noção de o-ideal é muito familiar na teoria dos reticulados e poderíamos também ter feito seu estudo em aneis principais e tentar extender os resultados obtidos a êste caso, isto é, classificar $\mathcal{A}$-módulos de K^n, onde K é o corpo de quocientes do anel principal $\mathcal{A}$. Esta extensão, porém, não é possível para

um anel principal qualquer. Vamos analisar ràpidamente quais os resultados que podem ser extendidos.

As propriedades de divisibilidade se definem de modo análogo, bem como a decomposição única em produto de números primos (neste caso elementos extremais de $\mathcal{A}$) ver [B. Alg. VII], § 1º, particularmente, proposição 1 e teorema 2. Mas o conjunto $\mathcal{P}$, sistema completo de representantes dos elementos extremais de $\mathcal{A}$ (que vai substituir o conjunto dos números primos positivos no caso geral) não é mais necessàriamente enumerável; exemplo: anel $\mathcal{A} = k[X]$ (dos polinômios na indeterminada X sôbre o corpo k) onde k não é enumerável, de modo que a característica de um o-ideal de $\mathcal{A}$ não mais será uma sequência mas sim uma família $(n_p)_{p \in \mathcal{P}}$. Estas características ainda estão em correspondência biunívoca com os o-ideais de $\mathcal{A}^*$ e de K^*, isto é, valem as prop. 1, teorema 2, prop. 3, prop. 1', teorema 2', proposição 4 e portanto servem para classificar completamente os subgrupos de K. Do mesmo modo ainda temos a noção de tipo e podemos usar a sequência característica para classificar as topologias de ideais sôbre $\mathcal{A}$, isto é, valem as prop. 9, teorema 10, proposições 11 e 12.

Porém para que todo o-ideal tenha uma sistema crescente de geradores é necessário (e suficiente) que $\mathcal{P}$ seja enumerável. Quando esta condição está satisfeita valem todos os resultados do § 1º do Cap. II e podemos, inclusivé, definir a noção de sequência principal. Ainda teremos a noção análoga a de representação (b_r)-ádica para os aneis completados $\hat{\mathcal{A}}$ (relativamente a uma topologia de ideais), os elementos a_n são agora elementos de um sistema completo de representantes R_{p_n} de $\mathcal{A}$ dos restos mod. (p_n), onde $p_n \in \mathcal{P}$. Os teoremas 13 e 16, de-

vidamente formulados são então válidos.

As noções de semibase, pôsto, etc. para $\mathcal{A}$-submódulos de K^n e os teoremas correspondentes subsistem para aneis principais quaisquer, inclusivé, a noção de característica de um $\mathcal{A}$-módulo em relação a um submódulo (teorema 26) bem como o teorema 28. Para extender os resultados do § 3º do Cap. IV e particularmente o teorema 29 é necessário que possamos achar um sistema completo de representantes de restos R_p de $\mathcal{A}$ módulo p tal que se $x,y \in R_p$ então x-y ou y-x também pertencem a R_p; exemplos: $A = k[X]$ e $A = Z$. Esta condição permite extender todos os resultados do §3º do Cap.IV. Se além disso $\mathcal{P}$ for enumerável segue-se que também podem ser extendidos os resultados do § 4º, substituindo-se o anel Z dos inteiros pelo anel principal $\mathcal{A}$ e modificand-se devidamente algumas condições. Pretendemos tratar destas generalizações para aneis principais e possìvelmente para aneis mais gerais (aneis de Dedekind) em outro trabalho.

Mencionaremos ainda alguns problemas que já estudamos ou pretendemos abordar utilizando os resultados do presente trabalho:

1) Mudança da matriz M relativamente a mudanças de semibases de G.

2) Grupos completamente redutíveis de pôsto finito. Demonstramos que o grupo G é completamente redutível se, e sòmente se, pudermos associar-lhe uma matriz $\mathcal{M}$ que é diagonal.

3) Fatores diretos, subgrupos e grupos quocientes.

4) Teoria da dualidade de Pontrjagin. Demonstramos que se ao grupo G de pôsto n está associada a sequência de matrizes M_r então o dual G^* de G é o limite projetivo de uma sequência T_r de toros de dimensão n por aplicações

$$\varphi_{r+1}: \; T_{r+1} \longrightarrow T_r$$

φ_{r+1} sendo definida por

$$(x_1,\ldots,x_n) \in T_{r+1} \longrightarrow M_{r+1}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in T_r$$

onde os x_i são números reais com os quais calculamos módulo 1.

5) Extensão da teoria de dualidade de Pontrjagin para aneis principais.

Quanto às orígens do presente trabalho: nosso interêsse pela teoria dos grupos começou em 1950; nesse ano, publicamos uma classificação dos subgrupos de Q [H 1]; tínhamos ainda diversos outros resultados referentes a subgrupos de Q^n mas não havíamos conseguido generalizar satisfatòriamente a classificação de Kurosh. Abandonamos êste campo e passamos a nos dedicar a outros problemas. Há alguns meses voltamos à teoria dos grupos tendo porém em vista certos resultados topológicos. Estas pesquisas levaram às idéias de sequência crescente de geradores de um o-ideal e de característica de um grupo em relação a um subgrupo pleno e percebemos que estas duas idéias reunidas adequadamente permitiriam generalizar de modo simples a classificação de Kurosh. Efetivamente, em algumas semanas conseguimos a classificação dos subgrupos de Q^n, classificação esta que conseguimos extender a subgrupos de $Q^{(L)}$ e a A-módulos sôbre certos aneis principais.

Nesta tese tratamos de dar demonstrações completas de todos os teoremas, principalmente daqueles que serão usados posteriormente. Também incluimos algumas proposições e corolários de que não fazemos uso neste trabalho, tendo em mente lançar maior luz sôbre o assunto. Usamos uma só numeração para as proposições e teoremas afim de facilitar sua localização.

Dado o grande número de definições de diferentes campos da Matemática que usamos, incluimos na parte final, um índice terminológico e um índice de notações que esperamos, facilitem a leitura da mesma. Êstes índices foram organizados pelo nosso colega Dr. Carlos B. de Lyra ao qual agradecemos calorosamente êsse auxílio e muitos outros que nos prestou.

Terminando esta introdução queremos deixar assinalados aqui os nossos agradecimentos a Dna. Ermilinda de Castro, funcionária do Departamento de Matemática da Faculdade de Filosofia, Ciências e Letras da Universidade de São Paulo, que escreveu à máquina grande parte do manuscrito desta tese e particularmente ao Dr. Luiz Henrique Jacy Monteiro que reviu conosco a maior parte do presente trabalho, sugeriu diversas modificações e ao qual também se deve todo o trabalho de preparação material desta tese. Sem os esforços e a dedicação do Dr. Luiz Henrique Jacy Monteiro esta tese não teria ficado pronta em tempo útil.

S.Paulo, Março de 1959.

ÍNDICE.

CAPÍTULO I.

Noções preliminares.

§ 1º - Teoria dos conjuntos.

1. Neste trabalho usamos as notações e terminologia dos "Éléments de Mathématique" do grupo Bourbaki e em particular de sua teoria dos conjuntos [B.E.].

Com N indicamos o conjunto dos números inteiros estritamente positivos. N_m indica o conjunto dos inteiros de 1 até m, Z o conjunto dos inteiros relativos e Q o conjunto dos números racionais. Z^* e Q^* indicam o conjunto dos números inteiros relativos, respectivamente dos números racionais, que são diferentes de zero. $\bar{N}$ e $\bar{Z}$ indicam respectivamente os conjuntos $N \cup \{\infty\}$ e $Z \cup \{\infty\}$ e consideramos que $\infty > n$ para todo $n \in N$ ou $n \in Z$ respectivamente.

2. A seguir consideraremos stanto sequências finitas $(x_n)_{n \in N_m}$ como sequências infinitas, $(x_n)_{n \in N}$. Na maior parte das vezes dizemos simplesmente "sequência" referindo-nos indiferentemente a sequências finitas ou infinitas, desde que esteja claro de que caso se trata. Aliás escreveremos simplesmente "a sequência (x_n)" ou mesmo "a sequência x_n". Também usamos esta notação simplificada para famílias de elementos, se não houver perigo de confusão.

Indicamos por P o conjunto dos números primos que consideramos ordenado por valores crescentes, de modo que podemos falar no "primeiro número primo", no "segundo número primo" etc. e na "sequência $(p_n)_{n \in N}$ dos números primos", p_n indicando o n-ésimo número primo, quando falamos na sequência $(x_p)_{p \in P}$ de elemen-

tos de um conjunto nos referimos a sequência $(x_{p_n})_{n \in N}$.

Exemplo: as sequências características $(n_p)_{p \in P}$ definidas no Cap. II.

3. Uma família $(x_i)_{i \in I}$ de elementos de Q (ou de um seu subconjunto) é chamada quasi-nula se $x_i = 0$ para todo $i \in I$ com um número finito de exceções apenas, quasi-positiva, se $x_i \geqslant 0$ exceto para um número finito de elementos $i \in I$, positiva, se $x_i \geqslant 0$ para todo $i \in I$. Também usamos a mesma nomenclatura para sequências.

4. Dar uma relação $\mathcal{R}$ sôbre um conjunto E é dar um subconjunto $R \subset E \times E$. Escrevemos $x \mathcal{R} y$ para indicar que $(x,y) \in R$.

Dizemos que uma relação $\mathcal{R}$ sôbre E é uma relação de equivalência se ela goza das seguintes propriedades:

1) Para todo $x \in E$ temos $x \mathcal{R} x$;

2) Se $x,y \in E$ e vale $x \mathcal{R} y$ então vale $y \mathcal{R} x$;

3) Se $x,y,z \in E$ e vale $x \mathcal{R} y$ e $y \mathcal{R} z$ então vale $x \mathcal{R} z$.

Exemplos: a - A relação de igualdade entre elementos de um conjunto E.

b - A relação "x é congruente a y módulo p" entre inteiros, p estando fixado.

c - A relação "x divide y e y divide x" em Z.

O conjunto formado por todos os elementos equivalentes a um elemento x chama-se classe de equivalência.

Dado um conjunto finito I indicamos por $|I|$ o número de seus elementos.

§ 2º - Álgebra.

1. Divisibilidade.

Dados dois elementos q e q' de Q (ou de um seu subconjunto Q^*, Z, Z^* ou N) dizemos que q divide q' e escrevemos $q|q'$, ou que q' é múltiplo de q, escrevemos $q' > q$, se existe um inteiro $m \in Z$ tal que $m.q = q'$.

Dados inteiros $a_1,\ldots,a_n \in Z$ de M.D.C. d, existem inteiros $m_1,\ldots,m_n$ tais que $m_1a_1 + \ldots + m_na_n = d$.

Fazemos a convenção

$$\prod_{i\in\emptyset} m_i = 1.$$

Assim mantemos a propriedade: se $I \subset J$ então $\prod_{i\in I} m_i$ divide $\prod_{i\in J} m_i$.

2. Teoria dos grupos.

Todos os grupos que aparecem neste trabalho são comutativos e usamos para êles a notação aditiva a menos de menção explícita do contrário, como acontece, por exemplo, com o grupo multiplicativo Q^*.

Dado um grupo (comutativo, sempre) G, dizemos que um elemento x G é de ordem finita se existe um $n \in Z^*$ tal que $nx = 0$. O conjunto dos elementos de ordem finita de G formam um subgrupo chamado torção de G. Um grupo sem torção é um grupo cujo único elemento de ordem finita é zero.

Dizemos que um subgrupo H de um grupo G é puro ou G-divisível se $x \in G$ e $nx \in H$, onde $n \in Z^*$, implica $x \in H$. Isto equivale a dizer que G/H é um grupo sem torção. Se K é

um subgrupo puro de H e H um subgrupo puro de G então K é um subgrupo puro de G.

Seja o grupo $G = \prod_{i \in I} G_i$ produto direto de uma família $(G_i)_{i \in I}$ de grupos; se para todo $i \in I$ tivermos $G_i = H$, escreveremos $G = H^I$. O conjunto das famílias quasi-nulas

$$(x_i)_{i \in I} \in H^I$$

é um subgrupo de H^I que indicamos por $H^{(I)}$.

Dado um grupo G, dizemos que um seu subgrupo H é um <u>fator direto</u> de G se existe um subgrupo K de G tal que todo elemento de G se escreve de um e um só modo sob a forma $h+k$, com $h \in H$ e $k \in K$. Então G é isomorfo ao produto direto $H \times K$. Todo fator direto de um grupo sem torção é um subgrupo puro dele.

Um grupo G é chamado <u>livre</u> se existe uma família $(b_i)_{i \in I}$ de elementos de G tal que para todo $a \in G$ existe uma e uma só família quasi-nula $(m_i)_{i \in I}$ de inteiros relativos tal que

$$a = \sum_{i \ I} m_i b_i .$$

Isto equivale a dizer que G é isomorfo ao grupo $Z^{(I)}$. Todo subgrupo de um grupo livre é livre. Idem para o produto direto de um número finito de grupos livres.

3. <u>Aneis e ideais</u>.

Todos os aneis que consideramos são comutativos e com unidade (diferente de zero).

Um subgrupo $\mathfrak{J}$ de um anel A é um <u>ideal</u> (de A) se $x \in \mathfrak{J}$ implica $ax \in \mathfrak{J}$ para todo $a \in A$. Exemplo: o conjunto $(x) = \{ax \mid a \in A\}$ é um ideal de A que chamamos de <u>ideal principal</u> gerado por x em A. No anel Z todo ideal é principal, isto é, gerado por um elemento de Z.

4. <u>Matrizes</u>.

Diz-se que uma matriz M de ordem $m \times n$ formada de elementos de um anel A tem pôsto r se ela tiver um menor de ordem $r \times r$ diferente de zero e se todo menor de ordem $(r+1) \times (r+1)$ for igual a zero.

Dada uma matriz M' de ordem $m \times n$ e uma matriz M" de ordem $n \times s$ temos: pôsto $(M' \times M'') \leq \inf$ [pôsto M', pôsto M"].

Se as matrizes M' e M" são de ordem $n \times n$ e M" é inversível então: pôsto $(M' \times M'')$ = pôsto M'.

Dada uma matriz M de inteiros relativos e um número primo p, o <u>p-pôsto</u> de M é o pôsto, no corpo Z/(p) da matriz $\bar{M}$ formada pelas classes de restos módulo p, $\bar{m}_{ij}$, dos elementos m_{ij} da matriz M. Portanto M tem p-pôsto r se existe um menor de ordem $r \times r$ que não é múltiplo de p mas todo menor de ordem $(r+1) \times (r+1)$ de M é múltiplo de p.

Dada uma matriz $M = (m_{rs})$ de ordem $n \times m$ e dados $I \subset N_n$ e $J \subset N_m$ indicamos por $M_{I \times J}$ a matriz

$$(m_{r,s})_{(r,s) \in I \times J}.$$

§ 3º - Conjuntos ordenados.

1. Relações de ordem e de pré-ordem.

Uma relação de pré-ordem num conjunto E é uma relação $\prec$ que satisfaz as seguintes propriedades:

1) para todo $x \in E$ temos $x \prec x$;

2) para $x,y,z \in E$ as relações $x \prec y$ e $y \prec z$ implicam $x \prec z$.

Se além disto vale a propriedade

1') para todos $x,y \in E$, as relações $x \prec y$ e $y \prec x$ implicam $x = y$;

dizemos que temos uma relação de ordem e o conjunto E munido desta relação será chamado de conjunto ordenado.

Uma relação de ordem será dita total, e E será denominado conjunto totalmente ordenado ou cadeia se vale

3) para todo $x,y \in E$ temos $x \prec y$ ou $y \prec x$.

Exemplos: a - A relação de ordem habitual $x \leqslant y$ em Q ou em qualquer um dos seus subconjuntos é total.

b - A relação $x|y$ (x divide y) em Q (ou nos seus subconjuntos) é uma relação de pré-ordem. Sôbre N esta relação é uma relação de ordem.

c - Dado um conjunto ordenado T, cuja relação de ordem indicamos por $\leqslant$, podemos introduzir uma relação de ordem no conjunto $E = T^I$, I sendo um conjunto qualquer; para isto definimos $(x_i)_{i \in I} \leqslant (x'_i)_{i \in I}$ se e sòmente se $x_i \leqslant x'_i$ para todo $i \in I$ ($x_i, x'_i \in T$). Em geral tomaremos $T = N$, $\bar{N}$ ou $\bar{Z}$ munidos com a ordem habitual e $I = P$ ou N.

Se $\prec$ é uma relação de pré-ordem sôbre E, a relação "$x \prec y$ e $y \prec x$" é uma relação de equivalência. Indicando por

$\mathcal{R}$ esta relação de equivalência, a pré-ordem $\prec$ define naturalmente uma relação de ordem sôbre o conjunto $E/\mathcal{R}$ das classes de equivalência.

2. Reticulados.

Dado um subconjunto A de um conjunto ordenado E dizemos que um elemento $m \in E$ é o extremo superior de A e escrevemos $m = \sup A$ ou $m = \sup \{a \mid a \in A\}$ ou $m = \sup_{a \in A} a$ se

1) para todo $a \in A$ temos $a \prec m$;

2) se $m' \in E$ é tal que para todo $a \in A$ temos $a \prec m'$ então $m \prec m'$.

De modo análogo definimos o extremo inferior de A e escrevemos inf A, etc.. O extremo superior ou inferior nem sempre existe.

Estas noções também podem ser definidas em conjuntos pré-ordenados mas neste caso o extremo superior m de um conjunto A não é mais único: qualquer elemento m' equivalente a m (na relação de equivalência deduzida da relação de pré-ordem) ainda goza das propriedades 1) e 2). Representamos então por sup A qualquer dêstes elementos. Idem para o extremo inferior. Assim quando escrevermos $\sup A \in S$ queremos dizer que qualquer dos elementos representados por sup A pertence a S. Quando escrevermos $\sup A = \sup B$, queremos dizer que existe um elemento da classe de sup A que é igual a um elemento da classe de sup B.

No exemplo b do número precedente sup A é simplesmente o mmc dos elementos de A e inf A o seu MDC (ver Cap. II, § 1º, nº 1) que estão determinados a menos do sinal.

No exemplo c o sup e o inf são ~~simplesmente determinados~~ para cada índice $i \in I$ separadamente.

Dizemos que um conjunto ordenado ou pré-ordenado E é um reticulado se qualquer subconjunto finito de E, tiver extremo superior e extremo inferior (pertencentes a E).

3. o-ideais.

Um subconjunto $A \neq \emptyset$ de um conjunto pré-ordenado reticulado E é um o-ideal (ideal relativamente à pré-ordem) se:

1) $a \in A$ e $b < a$ implica $b \in A$;

2) $a_1, a_2 \in A$ implica $\sup(a_1, a_2) \in A$.

Dada uma família $(A_i)_{i \in I}$ de o-ideais de E tal que $A = \bigcap_{i \in I} A_i \neq \emptyset$ então A é um o-ideal de E.

§ 4º - Topologia geral.

Também em topologia geral seguimos as definições e notações de Bourbaki, precisando de algumas definições e teoremas que se encontram em [B I] ou [B I'].

No Cap. II, § 2º, nº 1 se encontram reunidos os principais fatos sôbre aneis topológicos que usaremos neste trabalho.

CAPÍTULO II.

Os aneis de números reais generalizados.

§ 1º - Os o-ideais.

Começamos este parágrafo lembrando ràpidamente algumas propriedades bem conhecidas da divisibilidade de números racionais (Nº 1) que usaremos no estudo dos o-ideais e de suas sequências características (nº 2). Como já dissemos no prefácio, os o-ideais nos permitem unificar o estudo das topologias sôbre Z definidas por ideais (§ 2º), a classificação dos grupos aditivos de números racionais (Cap. III) e o estudo da característica de um subgrupo de Q^n (Cap. IV). O sistema crescente de geradores de um o-ideal que definimos no nº 4 é um dos instrumentos essenciais para a nossa classificação dos subgrupos de Q^n. O critério de escolha que damos no nº 5 terá aplicação no Cap. IV além de ser importante para lidar com exemplos. A teoria dos tipos (nº 6) terá diversas aplicações nos Capítulos III e IV.

1. Divisibilidade em Q^*.

Todo elemento $q \in Q^*$ se escreve de um e um só modo sob a forma

$$q = \varepsilon \prod_{p \in P} p^{n_p(q)}$$

onde $\varepsilon = 1$ ou $\varepsilon = -1$ e $(n_p(q))_{p \in P}$ é uma sequência quasi-nula de inteiros relativos. Recìprocamente a tôda sequência quasi-nula (m_p) de inteiros relativos corresponde dois elementos

$$q = \varepsilon \prod_{p \in P} p^{m_p} \in Q^*$$

com $\varepsilon = 1$ e $\varepsilon = -1$, $n_p(q) = m_p$.

A seguir q, q', q" indicam sempre elementos de Q^*.

d1 - $q \in N$ se e sòmente se a sequência $(n_p(q))$ for positiva.

d2 - $n_p(q^{-1}) = - n_p(q)$.

d3 - $q|q'$ se e sòmente se $(n_p(q)) \leqslant (n_p(q'))$.

Dados dois elementos q e q' de Q^*, seu m.m.c. e seu M.D.C. são respectivamente os racionais $[q,q']$ e $(q;q')$ tais que:

d4 - $n_p([q,q']) = \sup (n_p(q), n_p(q'))$;

d5 - $n_p((q;q')) = \inf (n_p(q), n_p(q'))$.

Lembremos que êstes elementos são determinados a menos do sinal.

E' imediato que os elementos assim definidos gozam das propriedades habituais dos m.m.c. e M.D.C.:

$[q,q'] \mid q"$ se se sòmente se $q|q"$ e $q'|q"$;

$q"|(q;q')$ se e sòmente se $q"|q$ e $q"|q'$.

E' imediato que

d6 - $[qq',qq"] = q[q',q"]$ e $(qq';qq") = q(q';q")$.

d7 - $n_p(qq') = n_p(q) + n_p(q')$.

d8 - $(q^{-1};q_1^{-1}) = [q,q_1]^{-1}$.

De fato: $n_p((q^{-1};q_1^{-1})) = \inf (n_p(q^{-1}), n_p(q_1^{-1})) =$

$= \inf (-n_p(q), -n_p(q_1)) = - \sup (n_p(q), n_p(q_1)) = - n_p([q,q_1]) =$

$$= n_p([q,q_1]^{-1}).$$

d9 - Dados q e q' existem inteiros m e n, primos entre si, tais que

$$(q;q') = mq + nq'.$$

De fato, r sendo o m.m.c. dos denominadores de q e q' então rq e rq' são inteiros e para êstes é bem conhecida a existência dos inteiros m e n com as propriedades requeridas acima, isto é, tais que

$$(rq;rq') = m.rq + n.rq';$$

usando d6 segue-se portanto a nossa afirmação.

2. Os o-ideais de Q^* e suas sequências caractercterísticas.

Lembremos que dada a relação de pré-ordem $q|q'$ sôbre Q^* um o-ideal de Q^* é um subconjunto $A \subset Q^*$, $A \neq \emptyset$ tal que

I1 - $q \in A$ e $q'|q$ implica $q' \in A$;

I2 - $q \in A$ e $q' \in A$ implicam $[q,q'] \in A$.

Exemplos: a) o conjunto dos números da forma p_o^n/m onde $n \in N$, $m \in Z^*$ e p_o é um número primo fixo.

b) o conjunto dos elementos de Q^* que não são divisíveis por quadrados de números primos.

c) o conjunto dos elementos de Q^* que não são divisíveis pelos números primos de um subconjunto $P_o \subset P$.

d) o conjunto dos divisores de um elemento dado $q_o \in Q^*$.

Dado um o-ideal $A \subset Q^*$ para todo $p \in P$ definimos

$$n_p(A) = \sup \{ n_p(a) \mid a \in A \}$$

(sup em $\bar{Z}$) e a sequência $n_p(A)$ será denominada sequência característica de A. Tomando $a \notin A$ temos portanto

$$(n_p(A)) \gtrdot (n_p(a))$$

e como só um número finito dos $n_p(a)$ pode ser estritamente negativo segue-se que a sequência característica de A é quasi-positiva.

Proposição 1 - Dado um o-ideal A e $q \in Q^*$ então $q \in A$ se e sòmente se $(n_p(q)) \leqslant (n_p(A))$; portanto

$$A = \left\{ q \in Q^* \mid (n_p(q)) \leqslant (n_p(A)) \right\} .$$

Demonstração: Seja $P_1 = \left\{ p \in P \mid n_p(A) < 0 \right\}$. Vimos acima que P_1 é um subconjunto finito de P. Dado

$$q = p_1^{m_1} . p_2^{m_2} \dots p_r^{m_r} \in Q^*$$

onde $p_1, p_2, \dots, p_r$ são números primos diferentes e onde $m_i \leqslant n_{p_i}(A)$, $i = 1,2,\dots,r$, existem elementos $q_i \in A$ tais que

$$m_i \leqslant n_{p_i}(q_i) \leqslant n_{p_i}(A).$$

Tomando $q_o = \prod_{p \in P_1} p^{n_p}$, $q_o \in A$ e $q' = [q_o, q_1, \dots, q_r] \in A$; temos $(n_p(q)) \leqslant (n_p(q'))$ e portanto $q \in A$.

Recìprocamente, dada uma sequência quasi-positiva $(n_p)_{p \in P}$ de elementos de $\bar{Z}$ o conjunto

$$A = \left\{ q \in Q^* \mid (n_p(q)) \leqslant (n_p) \right\}$$

é um o-ideal de Q^* e $n_p(A) = n_p$. Basta demonstrarmos que $A \neq \emptyset$ pois as outras afirmações são triviais; ora, temos

$$q_o = \prod_{p \in P_1} p^{n_p} \in A$$

(ver notação da demonstração precedente).

Demonstramos portanto o

Teorema 2 - A aplicação que a todo o-ideal de Q^* faz corresponder sua sequência característica é uma aplicação biunívoca do conjunto dos o-ideais de Q^* sôbre o conjunto das sequências quasi-positivas de elementos de $\bar{Z}$.

Exemplos: no exemplo a) acima temos $n_{p_o}(A) = \infty$ e $n_p(A) = 0$ se $p \neq p_o$.

No exemplo b) temos $n_p(A) = 1$ para todo $p \in P$.

No exemplo c) temos $n_p(A) = 0$ se $p \in P_o$ e $n_p(A) = \infty$ nos outros casos.

No exemplo d) temos $(n_p(A)) = (n_p(q_o))$.

$n_p(Q^*) = \infty$ para todo $p \in P$.

E' fácil demonstrar a

Proposição 3 - Dados dois o-ideais A e A' de Q^* temos $A \supset A'$ se e sòmente se $(n_p(A)) \geqslant (n_p(A'))$.

Se $(A_i)_{i \in I}$ é uma família de o-ideais de Q^* tal que $\bigcap_{i \in I} A_i \neq \emptyset$ então $n_p(\bigcap_{i \in I} A_i) = \inf_{i \in I} n_p(A_i)$.

Se $\bigvee_{i \in I} A_i$ é o o-ideal gerado pela reunião $\bigcup_{i \in I} A_i$ de uma família $(A_i)_{i \in I}$ de o-ideais então

$$n_p(\bigvee_{i \in I} A_i) = \sup_{i \in I} n_p(A_i).$$

A correspondência do teorema 2 é portanto um isomorfismo de reticulado.

3. Os o-ideais de Z^*.

Considerando a relação de ordem $m|m'$ em Z^*, dizemos que um subconjunto $A \subset Z^*$, $A \neq \emptyset$ é um o-ideal de Z^* se

J1 - $m \in A$ e $m'|m$ implicam $m' \in A$;

J2 - $m \in A$ e $m' \in A$ implicam $[m,m'] \in A$.

Exatamente como antes podemos definir a sequência característica de um o-ideal $A \subset Z^*$ e lembrando a propriedade dl vemos que as sequências características dos o-ideais de N são positivas.

Proposição 1' - Seja A um o-ideal de Z^* e $m \in Z^*$: $m \notin A$ se e sòmente se $(n_p(m)) \leqslant (n_p(A))$; portanto

$$A = \left\{ m \in Z^* \mid (n_p(m)) \leqslant (n_p(A)) \right\} .$$

Teorema 2' - A aplicação que a cada o-ideal de Z^* associa sua sequência característica define uma correspondência biunívoca entre os o-ideais de Z^* e as sequências de elementos de $\bar{N}$.

A demonstração dêstes teoremas é agora trivial bem como a do enunciado correspondente à Proposição 3.

Lembrando que o elemento 1 pertence a todo o-ideal de N temos a

Proposição 4 - Seja A um o-ideal de Q^*; $A \cap Z^*$ é um o-ideal de Z^* se e sòmente se $1 \in A$, isto é, se e sòmente se a sequência característica $(n_p(A))$ for positiva.

4. Sistemas crescentes de geradores de o-ideais.

Os resultados dêste número valem indistintamente para o-ideais de Q^* ou de Z^*.

Chamamos de sistema ou sequência crescente de geradores

de um o-ideal A uma sequência (g_n), ~~finita ou infinita, de e-~~ lementos positivos de A tais que $g_n \neq g_{n+1}$ e $g_n | g_{n+1}$ e tal que para todo $a \in A$ existe um $g_n > a$; temos portanto

$$A = \{ m \mid \text{existe } g_n > m \}.$$

Recìprocamente dada uma sequência (g_n) de elementos (de Q^* ou de Z^*) tais que $g_n | g_{n+1}$ então o conjunto

$$A = \{ m \mid \text{existe } g_n > m \}$$

é um o-ideal (de Q^* se tomarmos $m \in Q^*$, de Z^* se tomarmos $m \in Z^*$ e se os g_n forem inteiros).

Todo o-ideal A tem sempre um sistema crescente de geradores: A como subconjunto de Q^* é enumerável; seja $A = \{a_1, a_2, \ldots\}$; consideremos a sequência $a_1, [a_1, a_2], [a_1, a_2, a_3], \ldots$. Qualquer subsequência positiva estritamente crescente e cofinal desta sequência é um sistema crescente de geradores de A.

Dado um sistema crescente de geradores (g_n) de A e definindo

$$b_1 = g_1 \quad \text{e} \quad b_{n+1} = \frac{g_{n+1}}{g_n}$$

temos $g_n = b_1 . b_2 \ldots b_n$. A sequência (b_n) é chamada <u>sequência ou sistema de fatores</u> da sequência crescente de geradores (g_n) ou sequência de fatores de A. Os b_n são inteiros para $n \geq 2$. Se A tem sequência característica positiva podemos tomar os g_n tais que $b_1 = g_1 \in N$.

Do que precede segue-se imediatamente a

Proposição 5 - Sejam A e A' o-ideais, (g_n) e (g'_n) sistemas crescentes de geradores de A e A' respectivamente; $A \supset A'$ se e sòmente se para todo g_n existe um g'_m tal que $g_n | g'_m$.

Corolário 1 - Duas sequências (g_n) e (g'_m) tais que $g_n | g_{n+1}$ e $g'_m | g'_{m+1}$ definem o mesmo o-ideal A se e sòmente se para todo g_n existe um g'_m tal que $g_n | g'_m$ e para todo g'_m existe um g_n tal que $g'_m | g_n$.

Corolário 2 - Seja A um o-ideal com um sistema crescente infinito de geradores. Então A também tem um sistema crescente de geradores (g_n) tal que, se (b_n) é o sistema de fatores associado temos

$$\frac{b_n}{n} \longrightarrow \infty .$$

Demonstração: Dado um sistema crescente de geradores (g'_n) de A tomemos $g_n = g'_1 \cdot g'_2 \ldots g'_n$. Do corolário 1 segue-se que os dois sistemas de geradores são equivalentes. Temos $b_n = g'_n$ e portanto $b_n/n \longrightarrow \infty$ pois $g'_n = b'_1 b'_2 \ldots b'_n$ e $b'_i \geqslant 2$.

Proposição 6 - Seja A um o-ideal e seja (n_p) sua sequência característica. As seguintes propriedades são equivalentes:

I - A tem um sistema crescente de geradores infinito.

II - $\sum_{p \in P} n_p = \infty$.

III - Não existe $a \in A$ tal que $A = \{ x \mid a \succ x \}$.

Demonstração: I implica II pois

$$\sum_{p\in P} n_p(g_m) < \sum_{p\in P} n_p(g_{m+1}) \leqslant \sum_{p\in P} n_p .$$

II implica III pois se $A = \{x \mid a \succ x\}$ então $n_p(A) = n_p(a)$ portanto $\sum_{p\in P} n_p(A)$ é finito. III implica I pois se $g_1,\ldots,g_r$ é um sistema crescente de geradores de A finito então $A = \{x \mid g_r \succ x\}$.

5. Um critério de escolha de sistemas crescentes de geradores de o-ideais de Z^*.

Dado um o-ideal A podemos associar-lhe de infinitos modos um sistema crescente de geradores (g_n) e por conseguinte o sistema associado de fatores (b_n). Vamos agora dar um procedimento que associa a cada o-ideal A de Z^* um e um só sistema crescente de geradores (g_n) e tal que o sistema associado de fatores (q_n) seja formado por números primos.

Vamos primeiro definir uma sequência u_n de inteiros tais que qualquer inteiro seja divisor de algum u_n e que u_{n+1}/u_n seja primo (portanto um sistema crescente de geradores do o-ideal Z^*). Definimos $u_1 = p_1$ $(= 2)$, $u_2 = p_1^2$ $(=2^2)$, $u_3 = p_1^2.p_2$ $(= 2^2.3)$. Vamos supôr que u_n esteja definido e vamos definir u_{n+1}:

se $u_n = p_1^m.p_2^{m-1} \ldots p_m$ tomamos $u_{n+1} = p_1^{m+1}.p_2^{m-1} \ldots p_m$;

se $u_n = p_1^{m+1}.p_2^m \ldots p_s^{m-s+2}.p_{s+1}^{m-s}.p_{s+2}^{m-s-1} \ldots p_m$ onde $1 \leqslant s < m$ tomamos $u_{n-1} = u_n p_{s+1}$;

se $u_n = p_1^{m+1}.p_2^m \ldots p_m^2$ tomamos $u_{n+1} = u_n.p_{n+1}$.

Dado um o-ideal A de Z^* para todo inteiro $n \in Z^*$ seja h_n o maior elemento positivo de A que divide u_n. E' claro que h_{n+1}/h_n é um número primo ou é igual a 1. Definimos agora g_1 como sendo o primeiro dos elementos h_n que é diferente de 1. E' claro então que g_1 é primo. Suponhamos que $g_n = h_m$ esteja definido. Tomamos então como g_{n+1} o primeiro dos elementos h_{m+1}, h_{m+2},... que é diferente de g_n. Então g_{n+1}/g_n é primo. Se não existe um g_{n+1} com esta propriedade consideremos a sequência finita $g_1, g_2, \ldots, g_n$.

Dado agora $a \in A$ existe um $u_m \geq a$, logo $a \mid h_m$ e portanto os g_n formam uma sequência crescente de geradores de A satisfazendo as condições que queríamos.

A sequência (q_n) de fatores assim associada ao o-ideal A ou a sua sequência característica (n_p) será chamada de sequência principal associada à característica (n_p).

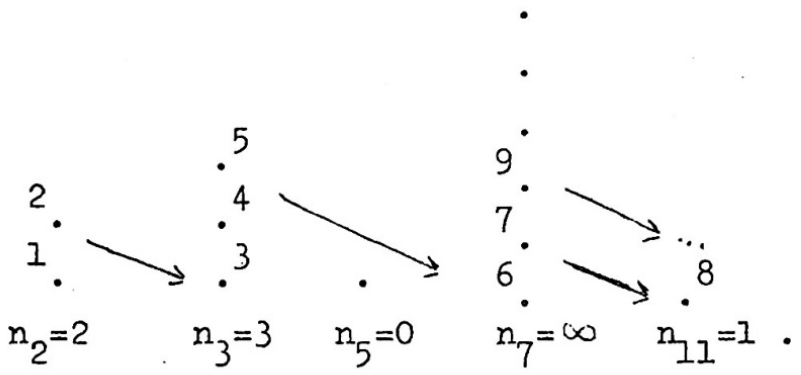
E' evidente que o-ideais diferentes têm sequências principais diferentes e é imediato que os o-ideais A e A' têm o mesmo tipo se, e sòmente se, existem inteiros n_o e m_o tais que tenhamos $q_{n_o+n} = q'_{m_o+n}$ para todo $n \in N$, e que o o-ideal A é de tipo maior que o i-ideal A' se existe um inteiro n_o tal que a sequência principal $(q'_{n_o+n})_{n \in N}$ de A' é uma subsequência da sequência principal (q_n) de A.

O processo acima corresponde exatamente ao processo de "percorrer as diagonais" que se usa na demonstração da teoria dos conjuntos quando se prova que a reunião enumerável de conjuntos enumeráveis é enumerável. Por isto êste processo é de fácil realização. Exemplo: consideremos o o-ideal A de Z^* cujos cinco primeiros têrmos da sequência característica sejam : 2, 3, 0, ∞ e 1. Temos então

$g_1 = 2$, $g_2 = 2^2$, $g_3 = 2^2.3$, $g_4 = 2^2.3^2$

$g_5 = 2^2.3^3$, $g_6 = 2^2.3^3.7$, $g_7 = 2^2.3^3.7^2$

$g_8 = 2^2.3^3.7^2.11$, $g_9 = 2^2.3^3.7^3.11$



. Os nove primeiros têrmos da sequência de fatores são 2, 2, 3, 3, 3, 7, 7, 11, 7.

6. Tipos de o-ideais.

Dado um o-ideal A de Q^* e $q \in Q^*$, $qA = \{qa \mid a \in A\}$ é um o-ideal de Q^* e $n_p(q.A) = n_p(q) + n_p(A)$. Um resultado análogo não vale para o-ideais de Z^*.

Dados dois o-ideais A e A' (de Q^* ou de Z^*) dizemos que A é de tipo maior que A' ou que a sequência característica de A é de tipo maior do que a sequência característica de A' se existe $m \in Z^*$ tal que $(n_p(m)+n_p(A)) \geq (n_p(A'))$; isto equivale a dizer que $n_p(A) \geq n_p(A')$ para todo $p \in P$ com um número finito de exceções e que para estas $n_p(A)$ e $n_p(A')$ são finitos. Para o-ideais de Q^* isto ainda equivale a dizer que $mA \supset A'$.

E' imediato que a relação que acabamos de definir é uma relação de pré-ordem no conjunto dos o-ideais de Q^* ou de Z^*. Ela dá portanto lugar a uma relação de equivalência: dizemos que

dois o-ideais A e A' são do mesmo tipo ou têm o mesmo tipo ou que suas sequências características são do mesmo tipo, se cada um deles é de tipo maior do que o outro; isto equivale a dizer que $n_p(A) = n_p(A')$ para todo $p \in P$ a menos de um número finito de exceções e que para estas $n_p(A)$ e $n_p(A')$ são finitos. Para o-ideais de Q^* isto equivale a dizer que existe um $q \in Q^*$ tal que $A = qA'$.

Proposição 7 - Sejam A e A' dois o-ideais de Q^* ou de Z^*; A e A' são do mesmo tipo se, e sòmente se, existirem inteiros $m, m' \in Z^*$ tais que

$$(n_p(m) + n_p(A)) = (n_p(m)) + n_p(A')).$$

Demonstração: a suficiência da condição resulta das definições acima. Recìprocamente, sejam A e A' do mesmo tipo e sejam

$$P_1 = \{p \in P \mid n_p(A) > n_p(A')\}$$

e

$$P_2 = \{p \in P \mid n_p(A) < n_p(A')\};$$

tomando

$$m' = \prod_{p \in P_1} p^{n_p(A)-n_p(A')} \quad \text{e} \quad m = \prod_{p \in P_2} p^{n_p(A')-n_p(A)}$$

teremos a igualdade procurada.

Corolário - Se A e A' são dois o-ideais de Q^* ou Z^* e se existe $m \in Z^*$ tal que

$$(n_p(A)) \leqslant (n_p(A')) \leqslant (n_p(A) + n_p(m))$$

então A e A' são do mesmo tipo.

O conjunto dos o-ideais está em correspondência biunívoca com o conjunto das sequências características, conjunto êste que tem a potência do contínuo por ser equipotente ao conjunto das aplicações de N em N. Como o conjunto dos pares (m,m') de inteiros é enumerável segue-se da Proposição 7 que o conjunto dos o-ideais do mesmo tipo que um o-ideal dado é enumerável. Portanto temos a

Proposição 8 - O conjunto dos diferentes tipos de o-ideais tem a potência do contínuo.

E' imediato que o conjunto dos tipos de o-ideais ou de suas sequências características formam um conjunto ordenado que é reticulado. Dados os tipos correspondentes a o-ideais A e A' o sup dêstes tipos corresponde ao tipo de o-ideal gerado por $A \cup A'$ e o inf dêstes tipos é o tipo do o-ideal $A \cap A'$.

§ 2º - Os aneis $\widehat{Z(n_p)}$.

Neste parágrafo introduzimos e estudamos os aneis $\widehat{Z(n_p)}$ cujo processo de construção generaliza a construção dos números reais (ver a introdução). Os elementos dêstes aneis aparecerão como elementos das matrizes que classificam os subgrupos de Q^n no cap. IV.

Começamos êste parágrafo recordando ràpidamente os resultados essenciais sôbre aneis topológicos que usamos a seguir. No nº 2 definimos os aneis $\widehat{Z(n_p)}$ e no nº 3 damos a representação (b_n)-ádica dos inteiros positivos que estenderemos por continuidade à representação (b_n)-ádica dos elementos de $\widehat{Z(n_p)}$ (nº 4), representação esta que é essencial para o Cap. IV.

1 - Aneis topológicos.

Dado um anel A e uma topologia sôbre A dizemos que **a topologia é compatível com a estrutura do anel ou que o anel A munido desta topologia é um** anel topológico, se estão satisfeitos os seguintes axiomas:

(AT_I). A aplicação $(x,y) \to x+y$ de $A \times A$ em A é contínua.

(AT_{II}). A aplicação $x \to -x$ de A em A é contínua.

(AT_{III}). A aplicação $(x,y) \to x.y$ de $A \times A$ em A é contínua.

Num anel topológico A se $\mathcal{B}$ é um sistema fundamental de vizinhanças de zero então estão satisfeitos os seguintes axiomas:

(GV'_I). Para todo $V \in \mathcal{B}$ existe um $W \in \mathcal{B}$ tal que $W + W \subset V$.

(GV'_{II}). Para todo $V \in \mathcal{B}$ existe um $W \in \mathcal{B}$ tal que $-W \subset V$.

(GV'_{III}). Zero pertence a todo V de $\mathcal{B}$.

(AV'_I). Para todo $x \in A$ e $V \in \mathcal{B}$ existe $W \in \mathcal{B}$ tal que $x.W \subset V$.

(AV'_{II}). Para todo $V \in \mathcal{B}$ existe $W \in \mathcal{B}$ tal que $W.W \subset V$.

Os conjuntos da forma $x + B$ onde $B \in \mathcal{B}$ formam um sistema fundamental de vizinhanças de x em A. Ver [B III] p. 5, 49 e 4. Recìprocamente, dada uma base de filtro $\mathcal{B}$ em um anel A tal que os axiomas (GV'_I), (GV'_{II}), (GV'_{III}), (AV'_I) e (AV'_{II}) estejam satisfeitos podemos definir em A uma topologia compatível com a sua estrutura de anel tomando como sistema

fundamental de vizinhanças de $x \in A$ os conjuntos da forma $x + B$ onde $B \in \mathcal{B}$. Ver [B III] pg. 4 e 49.

A topologia assim definida é separada se e sòmente se $\bigcap_{B \in \mathcal{B}} B = \{0\}$. Ver [B III], corolário da pg. 6. A topologia assim definida é discreta se e sòmente se $\{0\} \in \mathcal{B}$.

Um anel topológico separado pode ser completado, isto é, ser imerso como sub-anel denso num anel topológico completo. Ver [B III], pg. 51. Um anel topológico separado é metrizável se, e sòmente se, zero (e portanto qualquer outro ponto) tem um sistema fundamental enumerável de vizinhança. Ver [B IX] pg. 35. Neste caso o anel completado $\hat{A}$ de A pode ser definido simplesmente como o conjunto das classes de equivalência de sequências de Cauchy de A (Uma sequência (x_n) de elementos de A é uma sequência de Cauchy se dado $V \in \mathcal{B}$ existe um inteiro $n_o \in N$ tal que para $n,m \geqslant n_o$ temos $x_n - x_m \in V$. Todo elemento $x \in \hat{A}$ é o limite de uma sequência x_n de elementos de A. Duas sequências de Cauchy (x_n) e (y_n) de A são ditas equivalentes se $x_n - y_n \longrightarrow 0$; elas definem portanto o mesmo elemento x de $\hat{A}$).

Exemplo: dado um anel A e uma base de filtro $\mathcal{B}$ formada de ideais de A é trivial verificar que os axiomas acima estão satisfeitos: basta sempre tomar $W = V$. Uma topologia assim definida num anel A chamamos de topologia definida por ideais ou simplesmente topologia de ideais em A. Suporemos sempre que esta topologia seja não discreta, isto é, que $(0) \notin \mathcal{B}$.

2. Os aneis $\hat{Z(n_p)}$.

Dado em Z uma topologia definida por ideais consideremos o conjunto $\mathcal{B}$ de todos os ideais (m) de Z que são vizinhanças de zero nesta topologia.

Proposição 9 - O conjunto $A = \{ m \in Z^* \mid (m) \in \mathcal{B} \}$ é um o-ideal de Z^*.

Demonstração: $n|m$ se, e sòmente se, $(n) \supset (m)$. Portanto se $m \in A$, isto é, se $(m) \in \mathcal{B}$ e se $n|m$ então $(n) \in \mathcal{B}$ isto é, $n \in A$ e está satisfeita a condição J1. Se $m, m' \in A$, isto é, se $(m), (m') \in \mathcal{B}$ então $(m) \cap (m') = ([m,m']) \in \mathcal{B}$, isto é, $[m,m'] \in A$ e está portanto satisfeita a condição J2.

Recìprocamente, todo o-ideal A de Z^* define uma topologia de ideais em Z: basta tomar como sistema fundamental de vizinhança de zero o conjunto $\mathcal{B} = \{ (m) \subset Z \mid m \in A \}$. E' imediato que a o-ideais diferentes de Z^* correspondem topologias diferentes sôbre Z. Temos portanto o

Teorema 10 - A aplicação que a tôda topologia de ideais em Z associa o seu o-ideal definido na proposição 9, é uma aplicação biunívoca do conjunto das topologias de ideais em Z sôbre o conjunto dos o-ideais de Z^*.

Se (n_p) é a sequência característica do o-ideal A associado a uma topologia de ideais em Z indicaremos por $Z(n_p)$ o anel Z munido com esta topologia e por $\widehat{Z(n_p)}$ o seu anel completado; diremos que (n_p) é a sequência característica da topologia de Z ou do anel topológico $Z(n_p)$. Se (g_n) é uma sequência crescente de geradores de A e (b_n) a sua sequência de fatores associada, também usaremos as notações $Z(b_n)$ e $\widehat{Z(b_n)}$ para indicar $Z(n_p)$ e $\widehat{Z(n_p)}$ respectivamente. $N(b_n)$ indica o subconjunto N de Z munido com a topologia induzida por $Z(b_n)$.

Em resumo: se $\mathcal{B}_\tau$ indica o conjunto dos ideais de Z que são vizinhanças de zero de uma dada topologia τ de ideais

de Z temos $n_p = \sup \{ n_p(m) \mid (m) \in \mathfrak{B}_\tau \}$ e $Z_\tau = Z(n_p)$. Reciprocamente, dado $Z(n_p)$ temos: $(m) \in \mathfrak{B}$ se, e sòmente se $(n_p(m)) \leqslant (n_p)$.

Dizer que $g_1, g_2, \ldots$ é uma sequência crescente de geradores de A equivale a dizer que os ideais (g_1), (g_2),... formam um sistema fundamental de vizinhanças de zero em $Z(n_p)$ e que é estritamente decrescente, isto é,

$$(g_1) \supsetneq (g_2) \supsetneq \ldots .$$

Portanto, um anel topológico $Z(n_p)$ é sempre metrizável (se for separado).

Das definições e da proposição 3 segue-se fàcilmente a

Proposição 11 - Sejam τ e τ' duas topologias de ideais sôbre Z e sejam A e A' os seus o-ideais respectivos; a topologia τ é mais fina do que a topologia τ' se, e sòmente se, $A \supset A'$, isto é, se, e sòmente se, $(n_p(A)) \geqslant (n_p(A'))$.

Daí segue-se que a correspondência biunívoca natural do teorema 10 é mesmo um isomorfismo de reticulado.

Proposição 12 - $Z(n_p)$ é um anel topológico separado se e sòmente se

$$\sum_{p \in P} n_p = \infty .$$

Demonstração: Se $\sum n_p$ é finito então $A = \{ a \mid g \succ a \}$ onde $g = \prod_{p \in P} p^{n_p}$ e a topologia de $Z(n_p)$ satisfaz a propriedade $\bigcap_{V \in \mathfrak{B}} V = (g) \neq (0)$; ver a proposição 6. Se $\sum n_p = \infty$ então A tem sequência crescente infinita de geradores (g_n) e

portanto $\bigcap_n (g_n) = (0)$ pois um inteiro diferente de zero não pode ser múltiplo de uma infinidade de inteiros diferentes (os g_n).

De agora em diante suporemos sempre que a topologia de ideais de Z seja separada.

3. Representação (b_n)-ádica dos inteiros naturais.

Seja A um o-ideal de Z^* e (n_p) sua sequência característica, seja (g_n) uma sequência crescente de geradores de A e (b_n) a sequência associada de fatores; estas sequências são infinitas se $\sum n_p = \infty$, isto é, se o anel topológico $Z(n_p)$ for separado (Ver proposições 6 e 12). Nestas condições vamos demonstrar que existe uma correspondência biunívoca entre os elementos de $\widehat{Z(n_p)}$ e o conjunto das sequências

$$(a_1, a_2, \ldots, a_n, \ldots)$$

onde $0 \leq a_n < b_n$, isto é, entre $\widehat{Z(n_p)}$ e $\prod_{n \in N} \{0,1,2,\ldots,b_n-1\}$. Munindo êste último conjunto com a topologia produto (os fatores são supostos discretos) e definindo convenientemente as operações de soma e multiplicação veremos que a aplicação biunívoca mencionada é um isomorfismo de anel topológico. Daí segue-se, em particular, que o anel $\widehat{Z(n_p)}$ é compacto.

Vamos começar definindo a representação (b_n)-ádica dos inteiros naturais. Supomos sempre a seguir que $(b_n)_{n \in N}$ é uma sequência de inteiros naturais, $b_n > 1$.

E' fácil demonstrar por indução sôbre n o

Lema 1 - $b_1 b_2 \cdots b_{n+1} > b_1 + b_1 b_2 + \cdots + b_1 b_2 \cdots b_n$, $n = 2,3,\ldots$.

Lema 2 - Dadas duas sequências quasi-nulas $(a_n)_{n\in N}$ e $(a'_n)_{n\in N}$ de inteiros a_n e a'_n tais que $0 \leqslant a_n < b_n$ e $0 \leqslant a'_n < b_n$ consideremos os inteiros

$$m = \sum_{n\in N} a_n b_1 b_2 \cdots b_{n-1} \quad \text{e} \quad m' = \sum_{n\in N} a'_n b_1 b_2 \cdots b_{n-1};$$

$m < m'$ se, e sòmente se, sendo r o maior dos inteiros n tais que $a_n \neq a'_n$ tivermos $a_r < a'_r$.

Demonstração: Lembrando que $0 \leqslant a_n < b_n$ segue-se do lema 1 que

$$a_1 + a_2 b_1 + a_3 b_1 b_2 + \cdots + a_{r-1} b_1 b_2 \cdots b_{r-2} < b_1 b_2 \cdots b_{s-1}$$

e portanto

$$a_1 + a_2 b_1 + \cdots + a_{r-1} b_1 b_2 \cdots b_{r-2} + a_r b_1 b_2 \cdots b_{r-1} <$$

$$< (a_r+1) b_1 b_2 \cdots b_{r-1} \leqslant a'_r b_1 b_2 \cdots b_{r-1}$$

pois $a_r \leqslant a'_r$. Mas

$$a'_r b_1 b_2 \cdots b_{r-1} \leqslant a'_1 + a'_2 b_1 + a'_3 b_1 b_2 + \cdots + a'_r b_1 b_2 \cdots b_{r-1}$$

e lembrando que $a_n = a'_n$ para $n > 2$ segue-se que $m < m'$. A recíproca segue-se por redução ao absurdo.

Teorema 13 - Todo inteiro $m \geqslant 0$ admite uma e uma só representação

$$m = \sum_{n\in N} a_n b_1 b_2 \cdots b_{n-1}$$

onde (a_n) é uma sequência quasi-nula de inteiros tais que

$$0 \leqslant a_n < b_n.$$

Isto é, existe uma correspondência biunívoca entre o conjunto dos números inteiros positivos e o conjunto das sequências quasi-nulas (a_n) de inteiros tais que $0 \leqslant a_n < b_n$.

Demonstração: E' claro que tôda sequência (a_n) nas condições acima define um inteiro

$$m = \sum a_n b_1 b_2 \cdots b_{n-1}$$

e do lema 2 segue-se que sequências diferentes definem inteiros diferentes. Dado um inteiro $m \geqslant 0$ podemos achar fàcilmente a sequência (a_n) satisfazendo as condições do teorema e tal que

$$m = \sum a_n b_1 b_2 \cdots b_{n-1}:$$

tomamos a_1 como o resto da divisão de m por b_1 e seja q_1 o quociente desta divisão, $m = a_1 + b_1 q_1$ onde $0 \leqslant a_1 < b_1$; se já tivermos definido $a_1, \ldots, a_r$ e q_r definiremos a_{r+1} como sendo o resto da divisão de q_r por b_{r+1}, $q_r = a_{r+1} + b_{r+1} q_{r+1}$, onde $0 \leqslant a_{r+1} < b_{r+1}$. Como $b_n \geqslant 2$ temos $m > q_1 > q_2 > \ldots$ e portanto o processo termina depois de um número finito de divisões, isto é, teremos $a_n = 0$ para n suficientemente grande. Substituindo sucessivamente $q_1, q_2, \ldots$ pelas igualdades $q_r = a_{r+1} + b_{r+1} q_{r+1}$ que achamos nas divisões vem

$$m = \sum a_n b_1 b_2 \cdots b_{n-1}.$$

A sequência (a_n) determinada no teorema precedente é denominada representação (b_n)-ádica do inteiro m. Escrevemos

$a_n(m) = a_n$.

E' de verificação trivial a

Proposição 14 - Dado um inteiro $m \geqslant 0$,

$$m \in (b_1,\ldots,b_n) = (g_n)$$

se, e sòmente se,

$$a_1(m) = a_2(m) = \ldots = a_{n-1}(m) = 0.$$

Consideremos em $B_n = \{0,1,2,\ldots,b_n-1\}$ a topologia discreta e tomemos em

$$\mathcal{T} = \prod_{n\in N} B_n$$

a topologia produto.

Proposição 15 - A aplicação biunívoca

$$\varphi : m \in N(b_n) \longrightarrow (a_n(m)) \in \prod B_n$$

é um homeomorfismo.

Demonstração: em $\mathcal{T}$ os conjuntos

$$V_n = \{(a_r) \in \mathcal{T} \mid a_r = a_r(m) \text{ para } 1 \leqslant r \leqslant n\}$$

formam um sistema fundamental de vizinhanças de $(a_n(m))$. Mas $\varphi^{-1}(V_n) = [m+(b_1 b_2 \ldots b_n)] \cap N$ e êstes conjuntos formam um sistema fundamental de visinhanças de m e $m \in N(b_n)$ donde resulta a nossa afirmação.

E' possível exprimir as operações de adição e de multiplicação de inteiros através de suas representações (b_n)-ádicas. Damos os resultados sem demonstração pois não vamos utilizá-los aqui; as demonstrações, aliás, são fáceis.

Dados dois inteiros positivos m' e m", seja $a'_n = a_n(m')$ e $a''_n = a_n(m")$.

A sequência $a_n = a_n(m+m')$ é definida por indução:

$$(S)\quad \begin{cases} a'_1 + a''_1 = q_1 b_1 + a_1 \quad \text{com} \quad 0 \leqslant a_1 < b_1 \\ \\ a'_{n+1} + a''_{n+1} + q_n = q_{n+1} b_{n+1} + a_{n+1} \quad \text{com} \quad 0 \leqslant a_{n+1} < b_{n+1} \end{cases}$$

A sequência $a_n = a_n(m'.m")$ é definida por indução:

$$(M)\quad \begin{cases} a'_1 a''_1 = q_1 b_1 + a_1 \quad \text{com} \quad 0 \leqslant a_1 < b_1 \\ \\ \sum_{i=1}^{n} (a'_i a''_{n+1} + a'_{n+1} a''_i) b_1 b_2 \ldots b_{i-1} + a'_{n+1} a''_{n+1} = \\ \\ = q_{n+1} b_{n+1} + a_{n+1} \quad \text{com} \quad 0 \leqslant a_{n+1} < b_{n+1}. \end{cases}$$

4. Representação (b_n)-ádica dos elementos de $\widehat{Z(b_n)}$.

As notações são as mesmas que as do número precedente.

Em $Z(b_n)$ todo número negativo $-m$ pode ser aproximado arbitràrimanete por elementos de N. Com efeito, dada uma vizinhança $(b_1 \ldots b_n)$ de zero tomemos $r \in N$ tal que $r \geqslant n$ e tal que $m' = -m + b_1 \ldots b_r > 0$ então

$$m' - (-m) = b_1 \ldots b_r \in (b_1 \ldots b_n).$$

Assim N é denso em $Z(b_n)$ e portanto em $\widehat{Z(b_n)}$ e qualquer elemento de $\widehat{Z(b_n)}$ é então limite de uma sequência (de Cauchy) de elementos de N.

Seja $x \in \widehat{Z(b_n)}$ e uma sequência $(x_n)_{n \in N}$, $x_n \in N$ tal que $x_n \longrightarrow x$. A sequência (x_n) é portanto uma sequência de Cauchy e dada então uma vizinhança $(b_1 \dots b_r)$ de zero existe $n_o \in N$ tal que para $n,m \geqslant n_o$ tenhamos $x_n - x_m \in (b_1 \dots b_r)$. Da proposição 14 segue-se que $a_i(x_n) = a_i(x_m)$ para $1 \leqslant i \leqslant r-1$ e para quaisquer $n,m \geqslant n_o$. Indicando por a_i êste valor comum dos $a_i(x_n)$ para $n \geqslant n_o$ e por $x(r)$ o elemento

$$\sum_{i=1}^{r} a_i b_1 b_2 \dots b_{i-1}$$

então a sequência $(x(n))_{n \in N}$ é uma sequência de Cauchy equivalente à sequência (x_n) dada pois $x(n) - x_n \longrightarrow 0$. Associamos assim a todo elemento $x \in \widehat{Z(b_n)}$ uma sequência

$$(a_n)_{n \in N} \in \Pi = \prod_{n \in N} B_n$$

que chamamos de <u>representação</u> (b_n)-<u>ádica</u> de x. E' claro que a série $\sum_{n \in N} a_n b_1 b_2 \dots b_{n-1}$ converge para x em $\widehat{Z(b_n)}$ (pois as somas parciais finitas, que são os $x(n)$ formam uma sequência de Cauchy que converge para x) e que a representação (b_n)-ádica de um elemento $x \in \widehat{Z(b_n)}$ é única. Elementos $x \neq y$ de $Z(b_n)$ dão lugar a sequências de Cauchy $(x(n)) \neq (y(n))$ e portanto têm representações (b_n)-ádicas distintas.

Recìprocamente, tôda sequência $(a_n) \in \Pi$ dá lugar a uma série convergente

$$\sum_{n \in N} a_n b_1 \dots b_{n-1}$$

cuja soma é um elemento $x \in \widehat{Z(b_n)}$ que tem a sequência (a_n) como representação (b_n)-ádica. Escrevemos $a_n(x) = a_n$.

Teorema 16 - A aplicação biunívoca:

$$\hat{\varphi} : x \longrightarrow (a_n(x))_{n \in N}$$

de $\widehat{Z(b_n)}$ sôbre $\Pi = \prod_{n \in N} B_n$ é um homeomorfismo. $\widehat{Z(b_n)}$ é portanto um anel compacto.

Demonstração: A aplicação $\hat{\varphi}$ acima é simplesmente a prolongada da aplicação φ da proposição 15. A demonstração da bicontinuidade de $\hat{\varphi}$ é análoga à de φ.

Lembremos que dados $x,y \in \widehat{Z(b_n)}$ temos $x(n) \to x$ e $y(n) \to y$ portanto $x(n) + y(n) \longrightarrow x + y$ e $x(n).y(n) \longrightarrow x.y$ o que nos mostra que em Π ainda podemos definir a soma e a multiplicação de sequências usando as relações (S) e (M) do número precedente. Obtemos assim uma estrutura de anel em Π e $\hat{\varphi}$ será então um isomorfismo de anel topológico.

Dado $(0,\ldots,0,a_n,a_{n+1},\ldots,a_{n+r},\ldots)$ com $a_n \neq 0$ temos

$$-(0,\ldots,0,a_n,a_{n+1},\ldots,a_{n+r},\ldots) =$$

$$= (0,\ldots,0,b_n-a_n,b_{n+1}-a_{n+1}-1,\ldots,b_{n+r}-a_{n+r}-1,\ldots).$$

Portanto, temos em particular que dado $x \in \widehat{Z(b_n)}$, x é um inteiro negativo se, e sòmente se, existir $n_o \in N$ tal que para $n \geq n_o$ tenhamos $a_n(x) = b_n - 1$.

CAPÍTULO III.

Grupos sem torção e de pôsto 1.

§ 1º - Subgrupos de Q.

Damos aqui uma classificação dos subgrupos de Q, aplicando os resultados do Cap. II, § 1º. No Cap. IV obtemos esta classificação de um outro modo. Como aplicação dos métodos desenvolvidos no nº 1 estudamos no nº 2 os isomorfismos de subgrupos de Q e no nº 3 o grupo dos automorfismos de um sub-grupo de Q. No nº 4 estendemos a classificação a grupos de pôsto 1 e sem torção.

1. Classificação dos grupos aditivos de números racionais.

Lema - Um conjunto G de números racionais é um subgrupo de Q se, e sòmente se, estiverem satisfeitas as seguintes condições:

I'1 - $q \in G$ e $m \in Z$ implicam $mq \in G$;

I'2 - $q, q' \in G$ implica $(q;q') \in G$.

Demonstração: Se G é um subgrupo de Q, I'1 está evidentemente satisfeita e por d9 (Cap. II, § 1º, nº 1) temos $(q;q') = mq + nq'$ e portanto I'2 está satisfeita se $q, q' \in G$. Recìprocamente, se $G \subset Q$ satisfaz I'1 e I'2, dados $q, q' \in G$ temos $q = n(q;q')$ e $q' = n(q;q')$ onde $n, m \in Z$, portanto $q - q' = (n-m)(q;q') \in G$.

De agora em diante supomos que todos os subgrupos com que lidamos sejam diferentes de $\{0\}$.

Proposição 17 - Dado um subgrupo $G \subset Q$, $G \neq \{0\}$ o conjunto $A = \{q \in Q^* \mid q^{-1} \in G\}$ é um o-ideal de Q^* e portanto $G = \{0\} \cup \{a^{-1} \mid a \in A\}$.

Demonstração: Seja $q \in A$, isto é, $q^{-1} \in G$; se $q_1 | q$ temos $q_1^{-1} > q^{-1}$ e portanto $q_1^{-1} \in G$ por I'1; logo $q_1 \in A$ e vale I1. Dados $q, q_1 \in A$, isto é, $q^{-1}, q_1^{-1} \in G$ temos $(q^{-1}; q_1^{-1}) \in G$ por I'2 e como $(q^{-1}; q_1^{-1}) = [q, q_1]^{-1}$ (d8) segue-se que $[q, q_1] \in A$, isto é, a condição I2 está satisfeita.

Indicamos por $A(G)$ ou por A, se não houver perigo de confusão, o o-ideal de Q^* assim definido a partir de G e o chamamos de o-ideal associado a G ou de G; a sua sequência característica chamamos de sequência característica de G e a indicamos por $(n_p(G))$ ou (n_p). E' imediato que dado $q \in Q^*$, qG é um subgrupo de Q e que $A(qG) = q^{-1} A(G)$, isto é,

Corolário - Se A é o o-ideal de G, $q^{-1}A$ é o o-ideal de qG.

Reciprocamente, dado um o-ideal A de Q^* o conjunto $G = \{0\} \cup \{q \mid q^{-1} \in A\}$ é um subgrupo de Q, $G \neq \{0\}$ e $A(G) = A$. De fato: dados $q, q_1 \in G$ com $q \neq 0$ e $q_1 \neq 0$ obtemos, usando d8, I1 e I2,

$$q - q_1 = \frac{1}{q^{-1}} - \frac{1}{q_1^{-1}} = \frac{m}{[q^{-1}, q_1^{-1}]} = m\,(q; q_1) \in G.$$

As outras afirmações também são triviais.

E' claro que a grupos distintos correspondem o-ideais distintos. Temos portanto o

Teorema 18 - A aplicação que a todo subgrupo $G \subset Q$, $G \neq \{0\}$ associa o seu o-ideal $A(G)$ de Q é uma aplicação biunívoca do conjunto dos subgrupos $G \neq \{0\}$ de Q sôbre o conjunto dos o-ideais de Q.

Temos portanto ainda uma correspondência natural biunívoca entre o conjunto dos subgrupos $G \neq \{0\}$ de Q e o conjunto das sequências quasi-positivas de elementos de $\bar{Z}$ (sequências características):

$$n_p(G) = - \inf \{ n_p(g) \mid g \in G,\ g \neq 0 \}$$

e se G tem sequência característica (n_p) então

$$G = \{0\} \cup \{ q \in Q^* \mid n_p(q) \geqslant - n_p \} .$$

E' imediata a

Proposição 19 - Sejam G e G' subgrupos de Q; $G \supset G'$ se, e sòmente se, $A \supset A'$, isto é, se, e sòmente se, $(n_p) \geqslant (n'_p)$.

Lembrando que $n_p(1) = 0$ para todo $p \in P$ segue-se o

Corolário - $G \supset Z$ se, e sòmente se, a sua sequência característica for positiva.

Exemplos: a - $n_p(Z) = 0$ para todo $p \in P$.
b - $n_p(Q) = \infty$ para todo $p \in P$.
c - $n_p(p_o^m . Z) = -m$ se $p = p_o$, senão é nulo.

E' imediato que à intersecção de grupos corresponde a intersecção dos o-ideais correspondentes e ao grupo gerado por uma reunião de subgrupos de Q corresponde o o-ideal gerado pela reunião dos o-ideais correspondentes.

Da proposição 3 segue-se que se $(G_i)_{i \in I}$ for uma família de subgrupos de Q tal que $\bigcap_{i \in I} G_i \neq \emptyset$ então

$$n_p\left(\bigcap_{i \in I} G_i\right) = \inf_{i \in I} (n_p(G_i)).$$

Se $\bigvee_{i \in I} G_i$ indica o subgrupo de Q gerado por $\bigcup_{i \in I} G_i$ temos

$$n_p\left(\bigvee_{i \in I} G_i\right) = \sup_{i \in I} (n_p(G_i)).$$

A aplicação do teorema 18 é portanto um isomorfismo de reticulado.

2. Isomorfismo entre subgrupos de Q.

Dizemos que dois subgrupos G e G' de Q, têm o mesmo tipo ou são do mesmo tipo se seus o-ideais e portanto suas sequências características são do mesmo tipo. De modo análogo definimos tipo maior.

Lema - Sejam G e G' subgrupos de Q e φ um isomorfismo de G sôbre G'. Existe um elemento $q \in Q^*$ (e um só) tal que $\varphi(g) = q.g$ para $g \in G$ e portanto $G' = q.G$. Recìprocamente, tôda aplicação $g \in G \longrightarrow q.g \in Q$ com $q \in Q^*$ é um isomorfismo de G sôbre o subgrupo $q.G$ de Q.

Demonstração: φ sendo o isomorfismo temos

$$\varphi(x \pm y) = \varphi(x) \pm \varphi(y)$$

e portanto $\varphi(mx) = m.\varphi(x)$ $(m \in Z;\ x,y \in G)$. Dados x e $\frac{m}{n} x$ de G temos

$$\varphi\left(\frac{m}{n} x\right) = \frac{m}{n} \varphi(x)$$

pois

$$\varphi(\frac{m}{n}x) = \frac{n}{n}\varphi(\frac{m}{n}x) = \frac{1}{n}\varphi(mx) = \frac{m}{n}\varphi(x).$$

Dados $x,y \in G$ diferentes de zero seja $\frac{y}{x} = \frac{m}{n}$, isto é, $y = \frac{m}{n}x$; temos então $\varphi(y) = \frac{m}{n}\varphi(x)$ e dividindo esta relação pela precedente (membro a membro) vem

$$\frac{\varphi(y)}{y} = \frac{\varphi(x)}{x} = q \in Q^*,$$

q sendo portanto independente dos x e y particulares de G. Logo $\varphi(x) = q.x$.

A 2ª parte do lema é evidente.

Da definição de tipo de o-ideais e do lema acima segue-se o

Teorema 20 - Dois subgrupos de Q são isomorfos se, e sòmente se, são de mesmo tipo.

Teorema 21 - Dados dois subgrupos G e G' de Q, G é do tipo maior que G' se, e sòmente se, G' for isomorfo a um subgrupo de G.

Demonstração: G é do tipo maior que G' se, e sòmente se, A(G) é do tipo maior que A(G'), isto é, se, e sòmente se, existe $q \in Q^*$ tal que $q.A(G) \supset A'(G)$, isto é (corolário da Prop. 17) $q^{-1}G \supset G'$. A aplicação $x \in G' \longrightarrow qx \in G$ é o isomorfismo procurado.

Dêste teorema e da Proposição 8 segue-se que o conjunto das diferentes classes de subgrupos de Q isomorfos entre si têm a potência do contínuo.

3. Automorfismo de subgrupos de Q.

Do lema precedente segue-se, em particular, que todo automorfismo φ de um subgrupo G de Q (isto é, todo isomorfismo de G sôbre si mesmo) é definido por um elemento $q \in Q^*$: $\varphi(g) = q.g$. Se φ e φ_1 são automorfismos de G definidos por q e q_1 respectivamente então $\varphi_1.\varphi^{-1}$ é um automorfismo de G definido por $q_1 q^{-1}$. E' claro que $q = 1$ se e sòmente se φ for o automorfismo idêntico. Portanto, a aplicação $\varphi \longrightarrow q$ é um isomorfismo do grupo Amf G dos automorfismos de G, sôbre um subgrupo do grupo multiplicativo Q^*. Seja (n_p) a sequência característica de G e φ um automorfismo de G definido por $q \in Q^*$. Temos então $G = q.G$ e portanto $n_p(G) = n_p(G) - n_p(q)$; logo $n_p(q) = 0$ se $n_p(G) \neq \infty$. Portanto

$$\text{Amf } G \cong \left\{ q \in Q^* \mid \text{para todo } p \in P,\ n_p(q) = 0 \text{ se } n_p(G) \neq \infty \right\}.$$

Êste subgrupo de Q^* contém pelo menos dois elementos: 1 e -1; êle terá outros elementos se, e sòmente se,

$$\left\{ p \in P \mid n_p(G) = \infty \right\} \neq \emptyset$$

e neste caso Amf G é um grupo infinito.

E' fácil caracterizar os sub-aneis de Q; ver [H], pg. 45.

4. Grupos de pôsto 1 e sem torção.

Muitas vezes lidamos com grupos isomorfos a subgrupos de Q sem que êste isomorfismo, porém, seja canônico ou natural. Interessa estender os estudos precedentes a êste caso.

Dizemos que um grupo sem torção $G \neq \{0\}$ é de pôsto 1 se dados a e b de G existirem inteiros n e m, não am-

bos nulos, tais que $na = mb$; se $b \neq 0$ podemos tomar $n \neq 0$ e o número racional m/n assim associado ao par (a,b) é bem determinado: se também tivermos $n'a = m'b$ então $nn'a = nm'b = n'mb$ e portanto $(n'm - nm')b = 0$, logo $m/n = m'/n'$. O elemento a tal que $na = mb$ é único (para $b \neq 0$ e n,m dados) pois $na' = mb$ implica $n(a-a') = 0$ e portanto $a = a'$ pois $n \neq 0$. Podemos portanto escrever $a = \frac{m}{n} b$. Portanto fixando $b \neq 0$ de G, a todo elemento $a \in G$ associamos um número racional $\frac{m}{n} \in Q$ e esta aplicação $a \in G \longrightarrow \frac{m}{n} \in Q$ é um isomorfismo de G sôbre um subgrupo de Q que indicamos por $G(b)$. A sequência característica de $G(b)$ é denominada sequência característica de G relativamente a b ou ainda característica de b em G. Indicamo-la por $(n_p(G(b)))$.

Dado um grupo sem torção G e $b \in G$, $b \neq 0$ o conjunto $G_b = \{a \in G \mid \exists\ (n,m) \in Z^* \times Z$ tal que $na = mb\}$ é evidentemente um subgrupo de pôsto 1 de G (se $na = mb$ e $n'a'=m'b$ então $nn'(a - a') = (mn' - nm')b$) que chamamos de subgrupo puro de pôsto 1 gerado por b em G. E' o maior subgrupo de pôsto 1 de G que contém b. A característica de G_b relativamente a b chamamos ainda de característica de b em G. Naturalmente, tomando $b' \in G_b$, $b' \neq 0$, temos $G_{b'} = G_b$ e portanto as características de b e de b' (em G) são do mesmo tipo.

Se H é um subgrupo puro de um grupo sem torção G e se $b \in H$, $b \neq 0$ então a característica de b em G é igual à característica de b em H pois o subgrupo puro de pôsto 1 gerado por b em H é igual ao subgrupo puro de pôsto 1 gerado por b em G.

§ 2º - Soma direta de grupos de pôsto 1.

Sejam $G_1,\ldots,G_q$ grupos de pôsto 1 e sem torção, isto é, grupos isomorfos a subgrupos de Q e seja G seu produto direto (portanto, isomorfo a um subgrupo de Q^q). Neste parágrafo vamos estudar as relações que existem entre o tipo de um subgrupo puro de pôsto 1 de G e os tipos dos grupos $G_1,\ldots,G_q$. Êstes resultados serão aplicados no Cap. IV.

Seja $(b_1,\ldots,b_q) \in G$ com $b_1 \neq 0,\ldots, b_q \neq 0$; com as notações do § precedente temos:

$$G_{(b_1,\ldots,b_q)} =$$

$$= \left\{ (a_1,\ldots,a_q) \in G \mid \exists\, (n,m) \in Z^* \times Z \text{ tal que } n(a_1,\ldots,a_q) = \right.$$

$$\left. = m(b_1,\ldots,b_q) \right\} ;$$

mas $n(a_1,\ldots,a_q) = m(b_1,\ldots,b_q)$ se, e sòmente se, $na_i = mb_i$ para $1 \leqslant i \leqslant q$, isto é, se, e sòmente se $\frac{m}{n} \in G_i(b_i)$ para $1 \leqslant i \leqslant q$ ou ainda, se, e sòmente se

$$\frac{m}{n} \in G_1(b_1) \cap \ldots \cap G_q(b_q).$$

Portanto

$$n_p(G((b_1,\ldots,b_q))) = \inf_{1 \leqslant i \leqslant q} n_p(G_i(b_i)).$$

Se nem todos os b_i são diferentes de zero, seja

$$I = \left\{ i \in N_q \mid b_i \neq 0 \right\} ;$$

então $(b_1,\ldots,b_q)$ pertence ao fator direto $\prod_{i \in I} G_i$ de G e portanto, pelo que precede,

$$n_p(G(b_1,\ldots,b_q)) = \inf_{i\in I} n_p(G_i(b_i)).$$

Demonstramos assim o

Teorema 22 - Se G é produto direto de grupos sem torção de pôsto 1, $G_1,\ldots,G_q$ e se $b = (b_1,\ldots,b_q) \in G$, $b \neq 0$ a característica de b em G é o inf das características dos $b_i \neq 0$ em G_i.

Corolário 1 - Seja α_i o tipo do grupo G_i, $1 \leqslant i \leqslant q$ e $b = (b_1,\ldots,b_q) \in G$; seja $I = \{ i \in N_q \mid b_i \neq 0 \}$ e seja α o tipo do grupo G_b, então $\alpha = \inf_{i\in I} \alpha_i$.

Lembremos que o tipo α de um subgrupo H de pôsto 1 de G é maximal (em G) se não existe um subgrupo H_1 de pôsto 1 de G e do tipo $\alpha_1 > \alpha$. Segue-se então do corolário anterior o

Corolário 2 - Com as notações do teorema 22, G não pode ter mais de q tipos maximais de subgrupos de pôsto 1. Os tipos maximais estão necessàriamente entre os tipos $\alpha_1,\ldots,\alpha_q$.

Vamos usar o corolário 2 para demonstrar no capítulo IV que determinados grupos de pôsto finito não podem ser produto direto de grupos de pôsto 1.

Exemplo: consideramos no plano o grupo G dos elementos da forma $(\frac{n}{2^m}, \frac{r}{3^s})$ onde $n,m,r,s \in Z$, produto direto do grupo dos elementos da forma $n/2^m$ com o grupo dos elementos da forma $r/3^s$ cujas sequências características são respectivamente $(\infty,0,0,\ldots)$ e $(0,\infty,0,0,\ldots)$. Então o subgrupo puro de pôsto 1 gerado por $b = (b_1,b_2) \in G$ com $b_1 \neq 0$, $b_2 \neq 0$ tem o

tipo da sequência característica (0,0,...) isto é, é isomorfo a Z. Portanto: o grupo G é denso no plano mas qualquer reta qua passa pela origem e por um ponto de G e que não coincida com um dos eixos, encontra G segundo um subgrupo discreto isomorfo a Z.

CAPÍTULO IV.

Classificação dos grupos sem torção.

§ 1º - Grupos indecomponíveis.

1. O primeiro exemplo de um grupo de pôsto finito (ver o § 2º, nº 2 para a definição de pôsto) que não é completamente decomponível, isto é, que não é isomorfo ao produto direto de grupos de pôsto 1, é de Pontrjagin, [P], pg. 384. Êste exemplo é o grupo abeliano G gerado por uma infinidade de elementos $y, x_0, x_1, x_2, \ldots$ que estão ligados pelas relações

$$2^{n_i} x_i = x_{i-1} + y,$$

onde $i \in N$ e onde n_i é uma sequência de inteiros que contém elementos arbitràriamente grandes. Identificando x_0 com o elemento (1,0) de Q^2 e y com (0,1) podemos considerar G como subgrupo de Q^2.

Êste exemplo mostrou a não trivialidade do estudo dos grupos sem torção e de pôsto finito, isto é, essencialmente, dos subgrupos de Q^n. Como já dissemos na introdução, o primeiro estudo nesta direção foi feito por Kurosh [K] que classificou uma categoria particular de grupos de pôsto finito, os chamados grupos p-primitivos (isto é, grupos G que contêm um subgrupo livre H tal que para todo $x \in G$ existe um $m \in N$ tal que $p^m x \in H$; p é um número primo fixado). Kurosh classificou êstes grupos por meio de matrizes de ordem $n \times n$ (n = pôsto do grupo) de inteiros p-ádicos. Posteriormente Derry [D] e Szekeres [Sz] fizeram a classificação para grupos quaisquer de pôsto finito, mas estas classificações são insatisfató-

rias, não apresentando a simplicidade da classificação de Kurosh, além de terem outros inconvenientes (Ver a introdução).

Neste capítulo apresentamos uma classificação dos grupos sem torção; fazemos as demonstrações apenas para grupos de pôsto finito, considerados imersos em Q^n. A estensão dos resultados a grupos quaisquer de pôsto finito ou a subgrupos de $Q^{(L)}$, L sendo um conjunto qualquer, é imediata como mostramos no fim do § 4º. Nossa classificação generaliza as idéias e os resultados de Kurosh, substituindo as matrizes de elementos p-ádicos por matrizes de elementos (q_m)-ádicos convenientes. Para êste fim definimos no § 2º as noções de característica e de tipo de um grupo G o que nos permite então determinar a particular sequência principal (q_n) associada a G. No § 3º damos uma série de teoremas preparatórios de caracter algébrico e no § 4º damos finalmente a nossa classificação.

Daremos, a seguir, no nº 2, um outro exemplo de subgrupo de Q^2 que não é completamente decomponível. Êste exemplo é muito mais simples do que o exemplo de Pontrjagin acima reproduzido e também a demonstração de sua indecomponibilidade é estremamente mais simples. Acreditamos que êste exemplo é novo na literatura; êle faz parte de uma categoria de grupos que estudaremos em outro trabalho.

2. Exemplos.

a - Consideremos o subgrupo

$$G = \left\{ \left(\frac{a_1}{2^{b_1}} + \frac{a}{5^b} , \frac{a_2}{3^{b_2}} + \frac{a}{5^b} \right) \in Q \times Q \mid a, a_1, a_2, b, b_1, b_2 \in Z \right\}$$

de Q^2; G é um grupo de pôsto 2. Os seus subgrupos

$$H_1 = \left\{ \left(\frac{a_1}{2^{b_1}} , 0 \right) \mid a_1, b_1 \in Z \right\},$$

$$H_2 = \left\{ \left(0 , \frac{a_2}{3^{b_2}} \right) \mid a_2, b_2 \in Z \right\}$$

e

$$H = \left\{ \left(\frac{a}{5^b} , \frac{a}{5^b} \right) \mid a, b \in Z \right\}$$

são subgrupos puros e de pôsto 1; mostremos esta propriedade para H, por exemplo: seja

$$g = \left(\frac{a_1}{2^{b_1}} + \frac{a}{5^b} , \frac{a_2}{3^{b_2}} + \frac{a}{5^b} \right) \in G$$

e $n \in Z^*$ tal que $ng \in H$; podemos supôr $b_1 \geqslant 0$ e $b_2 \geqslant 0$ e $(2;a_1) = 1$ e $(3;a_2) = 1$. Se então $ng \in H$ devemos ter

$$\frac{na_1}{2^{b_1}} = \frac{na_2}{3^{b_2}} ,$$

isto é, $a_1 . 3^{b_2} = a_2 . 2^{b_1}$ e como $(2;a_1) = 1$ e $(3;a_2) = 1$ segue-se que $b_1 = b_2 = 0$ e portanto $a_1 = a_2$, isto é, $g \in H$. H_1, H_2 e H têm respectivamente o tipo das sequências características $(\infty,0,0,\ldots)$, $(0,\infty,0,0,\ldots)$ e $(0,0,\infty,0,0,\ldots)$ e são portanto tipos dois a dois incomparáveis, o que não pode acontecer num grupo de pôsto 2 que seja produto direto de dois grupos de pôsto 1 (corolário 1 do Teorema 22).

b - De modo análogo pode-se demonstrar que se α_1, α_2 e α_3 são 3 tipos de subgrupos de Q dois a dois incomparáveis (isto é, não vale $\alpha_i \leqslant \alpha_j$ para $i \neq j$) e se H_i é um subgrupo de Q que é de tipo α_i, o subgrupo

$$G = \left\{(x_1+x_3, x_2+x_3) \in Q\times Q \mid x_i \in H_i,\ i = 1,2,3\right\}$$

de Q^2 é indecomponível.

§ 2º - Tipo de um grupo sem torção e de pôsto finito.

Começamos êste parágrafo definindo a noção de semibase de um grupo. Mostramos que duas semibases (finitas) têm sempre o mesmo número de elementos que definimos então como sendo o pôsto do grupo. No nº 2 definimos a noção de característica de um grupo G em relação a certos subgrupos H e no caso em que H é um grupo livre mostramos que o tipo da característica independe do particular H (nº 3), sendo portanto um invariante do grupo G. Estas noções de característica e de tipo de G, são fundamentais no § 4º para classificar subgrupos de Q^n.

Todos os grupos que aparecem a seguir são grupos sem torção.

1. Semibases.

Dizemos que uma família $(b_i)_{i\in I}$ de elementos de um grupo G é linearmente independente ou livre se dada uma família quasi-nula qualquer, $(m_i)_{i\in I}$, de inteiros relativos, a relação

$$\sum_{i\in I} m_i b_i = 0$$

implica $m_i = 0$ para todo $i \in I$. Do teorema de Zorn segue-se que tôda família livre de elementos de G pode ser imersa numa família livre maximal de elementos de G (A demonstração é análoga a do teorema correspondente para espaços vectoriais). Uma

semibase de G é uma família livre maximal, $(b_i)_{i\in I}$, de elementos de G.

Proposição 23 - Dada uma família (b_i) de elementos de um grupo G, as seguintes propriedades são equivalentes:

a - a família (b_i) é uma semibase de G;

b - dado qualquer elemento $a \in G$ existe um inteiro $m \neq 0$ e uma família quasi-nula (m_i) de inteiros relativos tal que

$$ma = \sum_i m_i b_i;$$

além disso, a família $(\frac{m_i}{m})$ de números racionais é univocamente determinada.

Demonstração: Se os (b_i) formam uma semibase e se existisse $a \in G$ tal que não seja verdadeira a relação

$$ma = \sum_i m_i b_i,$$

com $m \neq 0$, a família formada por a e pelos b_i seria livre contra a hipótese de (b_i) ser uma semibase. Se

$$ma = \sum_i m_i b_i \qquad \text{e} \qquad m'a = \sum_i m'_i b_i$$

então

$$mm'a = \sum_i m'm_i b_i = \sum_i mm'_i b_i$$

e portanto

$$\sum_i (m'm_i - mm'_i)b_i = 0,$$

logo $m_i/m = m'_i/m'$ para todo i.

Reciprocamente, se vale a propriedade b, a família b_i é livre pois senão teríamos

$$\sum_i m_i b_i = 0$$

para alguma família m_i de inteiros, com algum $m_i \neq 0$, e zero teria duas representações: a família m_i acima e a família $m'_i = 0$. Os b_i formam uma família livre maximal pois para qualquer elemento $a \in G$ existe uma relação

$$ma = \sum_i m_i a_i$$

com $m \neq 0$.

Proposição 24 - Dada uma semibase $(b_i)_{i \in I}$ de um grupo G, a aplicação φ, definida pela proposição anterior, que a todo elemento $a \in G$ associa a família $(m_i/m)_{i \in I} \in Q^{(I)}$, é um isomorfismo do grupo G no espaço vectorial $Q^{(I)}$.

Demonstração: Dados $a, a' \in G$, seja

$$ma = \sum_i m_i b_i \qquad \text{e} \qquad m'a' = \sum_i m'_i b_i,$$

então

$$mm'(a - a') = \sum_i (m'm_i - mm'_i) b_i.$$

Portanto

$$(a - a') = \left(\frac{m_i}{m} - \frac{m'_i}{m'}\right)_{i \in I} = \left(\frac{m_i}{m}\right) - \left(\frac{m'_i}{m'}\right) = \varphi(a) - \varphi(a'),$$

isto é, φ é um homomorfismo e é biunívoco pois $\varphi(a) = 0$ se e sòmente se $m_i = 0$ para todo $i \in I$, isto é, se e sòmente se

$a = 0$, e portanto φ é um isomorfismo.

Demonstramos também o

Corolário - Todo grupo sem torção pode ser imerso como subgrupo em um espaço vectorial sôbre o corpo Q.

Recìprocamente todo subgrupo de um espaço vectorial sôbre Q é evidentemente um grupo sem torção.

Ainda nas condições da proposição acima: φ leva o elemento b_i no elemento de $Q^{(I)}$ cuja i-ésima coordenada é 1 e cujas outras coordenadas são nulas; logo, o sub-espaço vectorial de $Q^{(I)}$ gerado pelo subgrupo $\varphi(G)$ é o próprio $Q^{(I)}$. Portanto, se G tem uma semibase finita $b_1,\ldots,b_n$, G não pode ter outra semibase $b'_1,\ldots,b'_m$ com $m > n$ elementos pois senão suas imágens $\varphi(b'_1),\ldots,\varphi(b'_m)$ em Q^n formariam uma família linearmente dependente:

$$\sum_{i=1}^{m} \lambda_i \varphi(b'_i) = 0,$$

com $\lambda_i \in Q$ e com nem todos λ_i nulos. Multiplicando esta relação pelo m.m.c. dos denominadores dos λ_i teríamos a relação

$$\sum_{i} m_i \varphi(b'_i) = 0$$

com m_i inteiros não todos nulos. Mas

$$\sum m_i \varphi(b'_i) = \sum \varphi(m_i b_i) = \varphi(\sum m_i b'_i)$$

e φ sendo um isomorfismo, teríamos

$$\sum_{i=1}^{m} m_i b'_i = 0$$

com algum $m_i \neq 0$, contra a hipótese de que a família $b'_1,\ldots,b'_m$ é livre.

Demonstramos portanto a

Proposição 25 - Se o grupo G tem uma semibase finita com n elementos, qualquer outra semibase de G tem o mesmo número de elementos.

Êste número é denominado pôsto do grupo G.

Se G tem pôsto n qualquer família livre de n elementos é uma semibase de G.

E' imediato que o produto direto

$$G = \prod_{k=1}^{m} G_k$$

de grupos G_k de pôsto n_k tem posto

$$\sum_{k=1}^{m} n_k;$$

portanto, o produto direto de n grupos de pôsto 1 é um grupo de pôsto n.

E' evidente que um subgrupo de um grupo de pôsto n, tem pôsto $\leqslant n$.

E' trivial demonstrar o

Lema 1 - Se H é um subgrupo, de pôsto n, de um grupo G de pôsto n, então tôda semibase de H é uma semibase de G.

Daí segue-se imediatamente o

Lema 2 - Dado um grupo G de pôsto n e um seu subgrupo H de pôsto n também, então para todo $x \in G$ existe um $m \in Z$ tal que $mx \in H$.

Lema 3 - Nas condições do lema 2, se $b_1,\ldots,b_n$ é uma semibase de G, existe um inteiro $m \in Z^*$ tal que $mb_1,\ldots,mb_n$ seja uma semibase de H.

Demonstração: conforme o lema 2 existe $m_i \in Z$ tal que $m_i b_i \in H$, $i = 1,2,\ldots,n$. Tomamos então $m = m_1 m_2 \ldots m_n$.

Lema 4 - Dado um grupo G de pôsto n e dois subgrupos H_1 e H_2, de pôsto n, a sua intersecção $H_1 \cap H_2$ tem pôsto n.

Demonstração: Dada uma semibase $b_1,\ldots,b_n$ de G existem inteiros $m',m'' \in Z^*$ tais que $m'b_1,\ldots,m'b_n$ seja uma semibase de H_1 e $m''b_1,\ldots,m''b_n$ seja uma semibase de H_2. Então $m'm''b_1,\ldots,m'm''b_n \in H_1 \cap H_2$ e como esta família é livre e tem n elementos, será uma semibase de $H_1 \cap H_2$.

2. Característica de um grupo em relação a um subgrupo.

Seja G um grupo de pôsto n e H um seu subgrupo de mesmo pôsto; ou mais geralmente, seja G um grupo qualquer (sem torção) e H um subgrupo tal que tôda semibase de H seja uma semibase de G (subgrupo pleno - em relação a êstes subgrupos ainda vale o análogo do lema 2). Dado $x \in G$ o conjunto

$$\{m \in Z \mid mx \in H\}$$

é um ideal $\neq (0)$ de Z (lema 2) que tem portanto um gerador $m_x \in Z^*$, determinado a menos do sinal. Dizemos que o inteiro m_x é a altura de x relativamente a H.

Lema 1 - Se $m' \in Z$ e $m' | m_x$ então $m_{dx} = m'$ onde $d = m_x/m'$; ou ainda: se $d | m_x$ então $m_{dx} = m_x/d$.

Demonstração: $m'.dx = m'd.x = m_x.x \in H$, logo

$$m' \in (m_{dx}).$$

Seja $m \in (m_{dx})$, isto é, $m.dx \in H$; logo $md.x \in H$, isto é, $md \in (m_x) = (m'd)$ e portanto $m' | m$, isto é, $m \in (m')$. Logo $(m') = (m_{dx})$.

De modo análogo pode-se demonstrar que

$$m_{nx} = \frac{m_x}{(n; m_x)} .$$

Lema 2 - Dados $x, y \in G$ existe $z \in G$ tal que

$$m_z = [m_x, m_y].$$

Demonstração: A - Se $(m_x; m_y) = 1$ tomamos $z = x+y$ e teremos $m_z = [m_x, m_y]$ $(= m_x . m_y)$. De fato,

$$[m_x, m_y] = m_x . m_y \in (m_z),$$

pois

$$m_x m_y z = m_y . m_x x + m_x . m_y y \in H.$$

Por outro lado, seja $m \in (m_z)$, isto é, $m.z \in H$; então

$$m_x m z = m . m_x x + m m_x . y \in H$$

e portanto $m m_x y \in H$, isto é, $m m_x \in (m_y)$, ou ainda $m_y | m m_x$ e como $(m_x; m_y) = 1$ segue-se que $m_y | m$. Do mesmo modo mostramos que $m_x | m$ e portanto $[m_x, m_y] \mid m$; logo $m_z = [m_x, m_y]$.

B - Sejam agora m_x e m_y quaisquer; seja

$$P_1 = \left\{ p \in P \mid n_p(m_x) \geqslant n_p(m_y) \right\}$$

e

$$P_2 = \left\{ p \in P \mid n_p(m_x) < n_p(m_y) \right\} .$$

Tomemos

$$m' = \prod_{p \in P_1} p^{n_p(m_x)} \qquad \text{e} \qquad m'' = \prod_{p \in P_2} p^{n_p(m_y)} ;$$

então $m' | m_x$, $m'' | m_y$, $(m';m'') = 1$ e $[m',m''] = [m_x,m_y]$. Tomando $d' = m_x/m'$ e $d'' = m_y/m''$ segue-se do lema 1 que $m_{d'x} = m'$ e $m_{d''y} = m''$; e como $(m';m'') = 1$ resulta da parte A que

$$m_{d'x+d''y} = [m',m''] = [m_x,m_y]. \quad \text{(C.Q.D.)}.$$

Lembrando as condições J1 e J2 (Cap. II, § 1º, nº 3) vemos que com os lemas 1 e 2 demonstramos o

Teorema 26 - Seja G um grupo (sem torção) e H um seu subgrupo pleno. Para todo $x \in G$ existe um inteiro $m_x \in Z^*$ tal que $\{m \in Z \mid m.x \in H\} = (m_x)$. O conjunto $A = \{m_x \in Z^* \mid x \in G\}$ é um o-ideal de Z^*.

A sequência característica (n_p) dêste o-ideal de Z^*, é denominada <u>característica de G relativamente a H</u>. Lembremos que $n_p = \sup_{x \in G} n_p(m_x)$. Notemos que, na parte precedente não supuzemos que H fosse um subgrupo livre de G e efetivamente usaremos o teorema 26 em tôda a sua generalidade para classificar de modo muito simples a categoria de grupos a que aludimos no fim do nº 1, § 1º dêste capítulo. No exemplo a (§ 1º, nº 2) a característica de G relativamente a Z^2 é

$$(\infty,\infty,\infty,0,0,\ldots).$$

E' trivial verificar as seguintes propriedades:

<u>Lema</u> - Seja H_i um subgrupo pleno de G_i, $i = 1,2$; então $H = H_1 \times H_2$ é um subgrupo pleno de $G = G_1 \times G_2$ e dado $x = (x_1,x_2) \in G$ temos $m_x = [m_{x_1},m_{x_2}]$.

<u>Proposição 27</u> - Com as notações do lema precedente, se (n'_p) é a característica de G_1 relativamente a H_1 e (n''_p) a característica de G_2 relativamente a H_2, então a caracterís-

tica (n_p) de G relativamente a H é dada por

$$n_p = \sup (n'_p, n''_p).$$

Observação: propriedades análogas às expressas no lema e na proposição precedente ainda valem para produtos diretos finitos e somas diretas quaisquer.

3. Tipo de um grupo de pôsto finito.

Seja agora G um grupo de pôsto finito n e H um subgrupo livre e pleno (portanto também de pôsto n) de G, por exemplo o subgrupo gerado por uma semibase de G. Vamos mostrar que o tipo da característica de G relativamente a H é independente do particular H que tomamos e é portanto um invariante do grupo G.

Lema 1 - Se $H' \subset H$ são subgrupos livres de G de mesmo pôsto que G, então a característica de G relativamente a H é do mesmo tipo que a característica de G relativamente a H'.

Demonstração: Se $b_1, \ldots, b_n$ é uma base de H existe $m \in Z^*$ tal que $mb_1, \ldots, mb_n$ seja uma semibase de H' (lema 3 do nº 1) e portanto para todo $z \in H$ temos $mz \in H'$, logo $mH \subset H' \subset H$. Se então m_x indica a altura de um elemento $x \in G$ relativamente a H e m'_x sua altura relativamente a H', temos $m_x | m'_x$ e $m'_x | mm_x$. Portanto, se (n_p) é a característica de G relativamente a H e (n'_p) sua característica relativamente a H', temos $n_p \leqslant n'_p \leqslant n_p + n_p(m)$ e o nosso lema resulta do corolário da proposição 7.

Lema 2 - Se H_1 e H_2 são subgrupos livres de pôsto n, de um grupo G de pôsto n, então $H_1 \cap H_2$ é um subgrupo livre de pôsto n de G.

Demonstração: E' um teorema clássico que todo subgrupo livre de um grupo livre é um grupo livre e do lema 4 do nº 1 segue-se que $H_1 \cap H_2$ tem pôsto n.

Teorema 28 - Seja G um grupo de pôsto n e H_1 e H_2 subgrupos livres e de pôsto n de G: a característica de G relativamente a H_1 é do mesmo tipo que a característica de G relativamente a H_2.

Demonstração: de acôrdo com o lema 2 podemos considerar a característica de G relativamente a $H_1 \cap H_2$ e do lema 1 segue-se que a característica de G relativamente a H_1, bem como a característica de G relativamente a H_2, é do mesmo tipo que a característica de G relativamente a $H_1 \cap H_2$.

Corolário 1 - O tipo de G é um invariante do grupo G, isto é, ainda é o mesmo para qualquer grupo G_1 isomorfo a G.

De fato, se φ é um isomorfismo de G_1 sôbre G, φ leva um subgrupo livre H_1, de pôsto máximo, de G_1, sôbre um subgrupo H' de G com as mesmas propriedades e a característica de G relativamente a H' é igual à característica de G_1 relativamente a H_1.

No exemplo b do nº 2, § 1º o tipo de G é

$$\sup (\alpha_1, \alpha_2, \alpha_3).$$

Corolário 2 - Com as notações da Proposição 27: o tipo de $G_1 \times G_2$ é o extremo superior dos tipos de G_1 e G_2 (pôsto finito).

Observações - 1) Para grupos de pôsto 1 o tipo determina o grupo, a menos de isomorfismo (Teorema 20).

2) Para grupos de pôsto ∞ o lema 1 e o teorema 28 não valem: dado o grupo livre $G = Z^{(N)}$ e uma característica qualquer (n_p) existe um subgrupo livre e pleno H de G tal que a característica de G relativamente a H seja (n_p).

§ 3º - Teoremas preliminares.

Neste parágrafo damos os últimos teoremas necessários para poder abordar a nossa classificação dos grupos sem torção. No nº 1 o teorema principal é o que chamamos de Teorema da base canônica, que nos permitirá determinar de modo unívoco uma base de um grupo livre a partir da base de um seu subgrupo pleno. No nº 2 o resultado principal é o Teorema 36 que é essencial para caracterizar, por meio de condições necessárias e suficientes, as matrizes que, no § 4º, serão associadas a grupos sem torção.

1. O teorema da base canônica.

Lema - Dados um grupo G e $p \in N$, sejam elementos $z, b_1, b_2, \ldots, b_r \in G$ tais que

$$pz = \sum_{i=1}^{r} m_i b_i$$

onde $m_i \in Z$ $(1 \leqslant i \leqslant r)$ e $(p; m_r) = 1$. Então existe um elemento $\bar{z} \in G$ tal que

$$p\bar{z} = b_r - \sum_{i=1}^{r-1} m_i' b_i$$

com $0 \leqslant m_i' < p$. $\bar{z}$ é combinação linear inteira de z e dos

$b_1,\ldots,b_r$ e z é combinação linear inteira de $\bar{z}$ e dos $b_1,\ldots,b_r$, isto é, o subgrupo de G gerado pelos $b_1,\ldots,b_r$ e z é igual ao subgrupo de G gerado por $b_1,\ldots,b_r$ e $\bar{z}$.

Demonstração: de $(p;m_r) = 1$ segue-se a existência de inteiros u e v tais que $up + vm_r = 1$, portanto,

$$b_r = upb_r + vm_r b_r,$$

isto é, $vm_r b_r = b_r - pub_r$. Por outro lado

$$vpz = \sum_{i=1}^{r} vm_i b_i = b_r - pub_r + \sum_{i=1}^{r-1} vm_i b_i.$$

Dividindo vm_i por p temos $vm_i = v_i p + m_i'$ com $0 \leqslant m_i' < p$ e portanto

$$p(vz + ub_r - \sum_{i=1}^{r-1} v_i b_i) = b_r - \sum_{i=1}^{r-1} m_i' b_i$$

e basta tomar

$$\bar{z} = vz + ub_r - \sum_{i=1}^{r-1} v_i b_i.$$

De modo análogo achamos z como combinação linear dos b_i e de $\bar{z}$, lembrando que $(p;v) = 1$.

Dado um número primo p e uma matriz $M = (m_{k\ell})$ de ordem $n \times n$, dizemos que ela satisfaz a condição (Dp) se:

1) $m_{kk} = 1$ ou p $(1 \leqslant k \leqslant n)$;

2) $I = \{k \in N_n \mid m_{kk} = p\} \neq \emptyset$;

3) $0 \leqslant m_{k\ell} < p$ se $k \neq \ell$;

4) se $k \neq \ell$ então $m_{k\ell} = 0$ a não ser que $k \in I$, $\ell \in J = \complement I$ e $\ell < k$, isto é, a não ser que

$$(k,\ell) \in \{(i,j) \in I \times J \mid j < i\}.$$

A matriz M tem portanto a forma

$$M = \begin{pmatrix} \cdot & & & & & & \\ \cdot & \cdot & & & & & \\ 0 & 0 & 1 & & & & \\ \cdot & \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & m_{ij} & \cdot & p & & \\ \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \\ \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot \end{pmatrix}$$

Quando temos $p = q_r$ escrevemos

$$M_r = (m_{k\ell}^{(r)}),$$

I_r e J_r em vez de M, I e J.

Dado um grupo (sem torção) H, H[p] indica um grupo (sem torção) que contém H como subgrupo e que é tal que para todo $x \in H[p]$ tenhamos $px \in H$.

Teorema 29 (Teorema da base canônica - Kurosh) - Seja p um número primo, $H \subset H[p]$ um grupo livre de pôsto n e $b_1,\ldots,b_n$ uma base de H. Então existe uma e uma só base $b'_1,\ldots,b'_n$ de H[p] e um subconjunto $I \subset N_n$ tal que

$$\begin{cases} pb'_i = b_i - \sum_{j \in J,\, j<i} m_{ij} b_j & \text{se } i \in I \\ b'_j = b_j & \text{se } j \in J = \complement I \text{ e com } 0 \leqslant m_{ij} < p, \end{cases}$$

os m_{ij} e o conjunto I são também unìvocamente determinados. Em outras palavras: a base $b_1,\ldots,b_n$ de H determina unìvocamente uma base $b'_1,\ldots,b'_n$ de $H[p]$ e uma matriz M de ordem n n que satisfaz a condição (Dp) e tal que

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = M \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix} .$$

Chamamos a base $b'_1,\ldots,b'_n$ de $H[p]$ assim determinada de base canônica de $H[p]$ associada à base $b_1,\ldots,b_n$ de H (que em geral supomos fixada uma vez por tôdas) e a matriz M de matriz de passágem (da base $b'_1,\ldots,b'_n$ à base $b_1,\ldots,b_n$; é claro que ela também determina a transformação inversa, dada acima).

Demonstração do teorema 29: vamos construir sucessivamente os elementos $b'_1,b'_2,\ldots,b'_n$.

(1) - Se existe um elemento $x \in H[p]$ tal que $px = b_1$, êste elemento x com esta propriedade é evidentemente único e definimos então $b'_1 = x$ e teremos $1 \in I$. Se não existe um elemento x com esta propriedade, tomamos $b'_1 = b_1$ e $1 \in J$.

(2) - Suponhamos definidos $b'_1,\ldots,b'_r$ e $I^{(r)} = I \cap N_r$ e $J^{(r)} = J \cap N_r$ (que são conjuntos complementares em N_r); definiremos b'_{r+1}: se existe um elemento $x \in H[p]$ tal que

$$px = b_{r+1} - \sum_{j \in J^{(r)}} m_j b_j$$

com $0 \leqslant m_j < p$, tomamos $b'_{r+1} = x$ e $r+1 \in I$; senão tomamos $b'_{r+1} = b_{r+1}$ e $r+1 \in J$.

(3) - Na primeira hipótese, o elemento x é único. De fato, seja $x' \in H[p]$, $x' \neq x$ tal que

$$px' = b_{r+1} - \sum_{j \in J^{(r)}} m'_j b_j$$

com $0 \leqslant m_j < p$. Então

$$p(x - x') = \sum_{j \in J^{(r)}} (m_j - m'_j) b_j$$

com algum $m_j - m'_j \neq 0$ e seja s o maior dos índices $j \in J^{(r)}$ tais que $q_j = m_j - m'_j \neq 0$; como temos também $-p < q_s < p$ segue-se que $(p; q_s) = 1$ e pelo lema existe portanto $\bar{x} \in H[p]$ tal que

$$p\bar{x} = b_s - \sum_{j \in J^{(s-1)}} q'_j b_j,$$

com 0 q'_j p contra a hipótese de que s J.

(4) - Se $z \in H[p]$ é tal que

$$pz = \sum_{k=1}^{r} q_k b_k \qquad \text{então} \qquad z = \sum_{k=1}^{r} q'_k b'_k.$$

Demonstração para $r = 1$: seja $pz = q_1 b_1$; se $q_1 = pq'_1$ teremos $z = q'_1 b_1$ e portanto $z = q'_1 b'_1$ se $b'_1 = b_1$, ou $z = q_1 b'_1$ se $b_1 = pb'_1$. Se $(p; q_1) = 1$ segue-se do lema que existe um elemento $\bar{z} \in H[p]$ tal que $p\bar{z} = b_1$ e portanto $\bar{z} = b'_1$ e ainda pelo lema z é combinação linear de b_1 e b'_1 e portan

to um múltiplo de b_1' pois $b_1 = pb_1'$.

Suponhamos agora ter demonstrado que se

$$pz = \sum_{k=1}^{s} q_k b_k \qquad \text{então} \qquad z = \sum_{k=1}^{s} q_k' b_k$$

e vamos demonstrar um resultado análogo para $s+1$: seja $z \in H[p]$ tal que

$$pz = q_{s+1} b_{s+1} + \sum_{k=1}^{s} q_k b_k .$$

A - Se $(q_{s+1}; p) = 1$ escrevemos

$$pz = q_{s+1} b_{s+1} + \sum_{i \in I^{(s)}} q_i b_i + \sum_{j \in J^{(s)}} q_j b_j$$

e lembrando que

$$p_i = pb_i' + \sum_{j \in J^{(i)}} m_{ij} b_j'$$

se $i \in I^{(s)}$ e $b_j = b_j'$ se $j \in J^{(s)}$, vem

$$pz = q_{s+1} b_{s+1} + p \sum_{i \in I^{(s)}} q_i' b_i' + \sum_{j \in J^{(s)}} q_j' b_j'$$

ou

$$px = q_{s+1} b_{s+1} + \sum_{j \in J^{(s)}} q_j' b_j'$$

onde

$$x = z - \sum_{i \in I^{(s)}} q'_i b'_i .$$

Pelo lema existe então $\bar{x}$ tal que

$$p\bar{x} = b_{s+1} - \sum_{j \in J^{(s)}} m_j b'_j$$

com $0 \leqslant m_j < p$ e portanto $\bar{x} = b'_{s+1}$ ($b'_j = b_j$ se $j \in J$). z é combinação linear de x e dos b'_i, $i \in I^{(s)}$; x é combinação linear de $\bar{x} = b'_{s+1}$, dos b'_j, $j \in J^{(s)}$, e de b_{s+1} (pelo lema) e b_{s+1} é combinação linear dos b'_{s+1} e dos b'_j, $j \in J^{(s)}$. Daí segue-se que z é combinação linear (inteira) dos b'_k, $1 \leqslant k \leqslant s+1$.

B - Se $q_{s+1} = pq'_{s+1}$ então

$$p(z - q'_{s+1} b_{s+1}) = \sum_{k=1}^{s} q_k b_k$$

e pela hipótese de indução temos

$$z - q'_{s+1} b_{s+1} = \sum_{k=1}^{s} q'_k b_k$$

donde obtemos nosso resultado lembrando que ou $b_{s+1} = b'_{s+1}$, ou

$$b_{s+1} = pb'_{s+1} + \sum_{j \in J^{(s)}} m_{s+1,j} b'_j .$$

(5) - Os elementos $b'_1, \ldots, b'_n$ formam uma base de $H[p]$.

De fato, de (4) segue-se que qualquer elemento é combinação linear dêstes e como o pôsto de $H[p]$ é $\geqslant n$ = pôsto de H, segue-se que a família $b'_1, \ldots, b'_n$ é livre.

(6) - Demonstração da unicidade da base canônica de $H[p]$: Seja $\bar{b}'_1,\ldots,\bar{b}'_n$ outra base canônica, com um subconjunto $\bar{I} \subset N_n$ e $\bar{J}$ seu complementar. Seja r o menor elemento de N_n tal que $b'_r \neq \bar{b}'_r$.

A - Se $r \in I$ e $r \in \bar{I}$, então $J^{(r)} = \bar{J}^{(r)}$, seja

$$pb'_r = b_r - \sum_{j \in J^{(r)}} m_{rj} b_j \qquad \text{e} \qquad p\bar{b}'_r = b_r - \sum_{j \in J^{(r)}} \bar{m}_{rj} b_j .$$

Então indicando por s o maior índice $j \in J^{(r)}$ tal que

$$m_{rj} \neq \bar{m}_{rj}$$

achamos, como em (3) acima, um elemento $\bar{x}$ tal que

$$p\bar{x} = b_s - \sum_{j \in J^{(s-1)}} q_j b_j$$

com $0 \leqslant q_j < p$, contra a hipótese de que $s \in J$.

B - Se $r \in J$ e $r \in \bar{I}$, isto é, se $b'_r = b_r$ e

$$p\bar{b}'_r = b_r + \sum_{j \in J^{(r-1)}} \bar{m}_{rj} b_j$$

temos por (4) que

$$\bar{b}'_r = q_r b'_r + \sum_{k=1}^{r-1} q_k b'_k$$

e portanto

$$p\bar{b}'_r = pq_r b_r + \sum_{k=1}^{r-1} q_k p b'_k = pq_r b_r + \sum_{k=1}^{r-1} q'_k b_k$$

que comparada com a 1ª expressão de $p\bar{b}'_r$ nos dá $pq_r = 1$, o que é impossível. A mesma demonstração vale se $r \in I$ e $r \in \bar{J}$.

(7) - Do que precede segue-se portanto a unicidade do conjunto I e da matriz M e terminamos assim a demonstração do teorema 29.

Vamos passar a indicar por $H[p,M]$ o grupo $H[p]$ acima, ao qual está associado a matriz M; a menos de isomorfismos, êste grupo é completamente determinado pela matriz M (e pela base $b_1,\ldots,b_n$ de H).

Recìprocamente, é evidente que dado um grupo livre H de pôsto n, uma base $b_1,\ldots,b_n$ de H e uma matriz M de ordem n n que satisfaz à condição (Dp), existe um grupo, que indicamos por $H[p,M]$, que contém H como subgrupo e que tem uma base $b'_1,\ldots,b'_n$ tal que

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = M \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix};$$

$H[p,M]$ é único a menos de isomorfismos (que conservam H).

Dado outro número primo q e uma matriz M' de ordem $n \times n$ que satisfaz à condição (Dq) definimos o grupo $H[p,M;q,M']$ como sendo $H[p,M][q,M']$, a segunda extensão, definida por M', sendo feita em relação à base canônica $b'_1,\ldots,b'_n$ de $H[p,M]$.

De modo análogo dados números primos $q_1,\ldots,q_r$ e matrizes M_i, $1 \leqslant i \leqslant r$, de ordens $n \times n$, satisfazendo a condição (Dq_i), definimos

$$H[q_1,M_1;\ldots;q_r;M_r] = H[q_1,M_1] \ldots [q_r,M_r].$$

base fixada $b_1,\ldots,b_n$ de H vai determinando sucessivamente as bases canônicas $b_1^{(1)},\ldots,b_n^{(1)}$ de $H[q_1,M_1]$ até $b_1^{(r)},\ldots,b_n^{(r)}$ de $H[q_1,M_1;\ldots;q_r,M_r]$ e temos

$$\begin{matrix} b_1^{(i-1)} \\ \vdots \\ b_n^{(i-1)} \end{matrix} = M_i \begin{matrix} b_1^{(i)} \\ \vdots \\ b_n^{(i)} \end{matrix}$$

$1 \leqslant i \leqslant r$, onde $b_k^{(o)} = b_k$.

De agora em diante, quando escrevermos

$$G = H[q_1,M_1;\ldots;q_r,M_r]$$

subentenderemos que H é um grupo livre de pôsto n no qual fixamos uma base $b_1,\ldots,b_n$, que os q_i são números primos e que M_i é uma matriz de ordem n n que satisfaz a condição (Dq_i) $(1 \leqslant i \leqslant r)$.

Dado um grupo livre H e uma sua base $b_1,\ldots,b_n$, indicamos por $H^{(r)}$ o subgrupo de H gerado por $b_1,\ldots,b_r$ $(1 \leqslant r \leqslant n)$. Com as notações do teorema 29, definimos

$$H^{(r)}[p] = \{ x \in H[p] \mid px \in H^{(r)} \}$$

e temos a

Proposição 30 - $H^{(r)}[p] = H[p]^{(r)}$.

Demonstração: seja

$$x = \sum_{k=1}^{n} x'_k b'_k \in H^{(r)}[p],$$

isto é, tal que

$$px = \sum_{k=1}^{r} x_k b_k;$$

lembrando que $b_j = b'_j$ se $j \in J$ e

$$b_i = pb'_i + \sum_{j \in J^{(i)}} m_{ij} b'_j.$$

Se $i \in I$ vem

$$px = \sum_{k=1}^{r} m'_k b'_k$$

que comparado com

$$px = \sum_{k=1}^{n} px'_k b'_k$$

mostra que $x'_{r+1} = x'_{r+2} = \ldots = x'_n = 0$, isto é, $x \in H[p]^{(r)}$. De modo análogo mostramos a inclusão no outro sentido.

Corolário 1 - Para todo $r \in N_n$, $b'_1, \ldots, b'_n$ é a base canônica de $H^{(r)}[p] = H[p]^{(r)}$ associada à base $b_1, \ldots, b_r$ de $H^{(r)}$ e a sua matriz de passágem é $M_{N_r \times N_r}$.

Corolário 2 - Se $I^{(r)} = I \cap N_r \neq \emptyset$ então a matriz $M_{N_r \times N_r}$ também satisfaz à condição (Dp). Em caso contrário ela se reduz à matriz unidade.

Com as notações do teorema 29, temos:

Proposição 31 - Seja

$$z' = \sum_{k=1}^{n} z'_k b'_k \in H[p];$$

$z' \in H$ se e sòmente se $z'_i \equiv 0 \pmod{p}$ para todo $i \in I$.

Demonstração: se $z' \in H$ então

$$z' = \sum_{k=1}^{n} z_k b_k = \sum_{i \in I} z_i b_i + \sum_{j \in J} z_j b_j =$$

$$= \sum_{i \in I} z_i (pb'_i + \sum_{j \in J(i)} m_{ij} b'_j) + \sum_{j \in J} z_j b'_j =$$

$$= \sum_{i \in I} pz_i . b'_i + \sum_{j \in J} z'_j b'_j$$

e portanto $z'_i = pz_i$ se $i \in I$. Recìprocamente, se $z'_i = pz_i$ quando $i \in I$, temos

$$z' = \sum_{i \in I} pz_i b'_i + \sum_{j \in J} z'_j b'_j =$$

$$= \sum_{i \in I} z_i . pb'_i + \sum_{j \in J} z'_j b'_j =$$

$$= \sum_{i \in I} z_i (b_i - \sum_{j \in J(i)} m_{ij} b_j) + \sum_{j \in J} z'_j b_j$$

e portanto $z \in H$.

Proposição 32 - Seja $z \in H$ tal que

$$z = \sum_{j \in J} z_j b_j;$$

existe um elemento $z' \in H[p]$ tal que $z = pz'$ se, e sòmente se $z_j \equiv 0 \pmod{p}$, para $j \in J$.

Demonstração: Seja

$$z' = \sum_{k=1}^{n} z'_k b'_k;$$

temos

$$pz' = \sum_{i \in I} z'_i . pb'_i + \sum_{j \in J} pz'_j . b'_j =$$

$$= \sum_{i \in I} z'_i (b_i - \sum_{j \in J,\ j<i} m_{ij} b_j) + \sum_{j \in J} pz'_j . b_j =$$

$$= \sum_{i \in I} z'_i b_i + \sum_{j \in J} (pz'_j + \sum_{i \in I, i>j} z'_i m_{ij}) b_j .$$

Se $pz' = z$ então $z'_i = 0$ quando $i \in I$ e portanto $z_j = pz'_j$. Reciprocamente, se $z_j = pz'_j$ então

$$z = \sum_{j \in J} z_j b_j = \sum_{j \in J} pz'_j b_j = p \sum_{j \in J} z'_j b'_j = pz'$$

onde

$$z' = \sum_{j \in J} z'_j b'_j \in H[p].$$

2. A condição $(q_1 * q_r)$.

Dado um grupo sem torção G, um inteiro $p \in Z^*$ e um subgrupo H de G, definimos $H(p;G) = \{x \in G \mid px \in H\}$ que também indicamos por $H(p)$ se não houver perigo de confusão. Se H é um grupo livre de pôsto n, o mesmo será verdade para $H(p)$ pelo teorema 29 e fixada uma base $b_1,\ldots,b_n$ de H vem a base canônica $b'_1,\ldots,b'_n$ de $H(p)$ com uma matriz de passágem M. Temos então $H(p;G) = H[p,M]$.

Se $q_1,q_2,\ldots,q_r$ são números primos quaisquer definimos $H(q_1,q_2,\ldots,q_r;G) = H(q_1,G)(q_2,G)\ldots(q_r,G)$ e se H for um grupo livre de pôsto n o mesmo será verdade para

$$H(q_1,q_2,\ldots,q_r;G).$$

A base $b_1,\ldots,b_n$ de H determina a base canônica

$$b_1^{(1)},\ldots,b_n^{(1)}$$

de $H(q_1;G)$ com uma matriz de passágem M_1; a base $b_1^{(1)},\ldots,b_n^{(1)}$ por sua vez determina a base canônica $b_1^{(2)},\ldots,b_n^{(2)}$ de $H(q_1,q_2;G)$ com uma matriz de passágem M_2 e assim por diante. Temos portanto

$$H(q_1,q_2,\ldots,q_r;G) = H[q_1,M_1;q_2,M_2;\ldots;q_r;M_r].$$

Proposição 33 - Dado $x \in H[p]$ e $q \in Z$ tal que $(p;q) = 1$ e $qx \in H$ então $x \in H$.

Demonstração: se $(p;q) = 1$ existem inteiros u,v tais que $up + vq = 1$ e portanto $x = upx + vqx \in H$ pois $px \in H$ e $qx \in H$.

Proposição 34 - $H(g_1.g_2;G) = H(g_1,g_2;G)$.

Demonstração: $x \in H(g_1.g_2;G)$ se, e sòmente se, $g_1g_2.x \in H$, isto é, se, e sòmente se, $g_2x \in H(g_1;G)$, isto é, se e sòmente se $x \in H(g_1,g_2;G)$.

Corolário 1 - $H(g_1.g_2 \ldots g_r;G) = H(g_1,g_2,\ldots,g_r;G)$.

Corolário 2 - $H(g_1,g_2,\ldots,g_r;G) = H(g_{\sigma 1},g_{\sigma 2},\ldots,g_{\sigma r};G)$ onde σ é uma permutação qualquer de N_r.

Proposição 35 - Seja $L = K[q_1,M_1;q_2,M_2;\ldots;q_r,M_r]$ com $q_i \neq q_1$ para $i = 2,3,\ldots,r$; então $K(q_1;L) = K[q_1;M_1]$.

Demonstração: é evidente que $K(q_1;L) \supset K[q_1;M_1]$. Por outro lado seja $x \in L$ tal que $x \in K(q_1;L)$, isto é, $q_1x \in K$. Pela definição de L temos $q_2\ldots q_r.x \in K[q_1;M_1]$ e como $(q_1;q_2\ldots q_r) = 1$ podemos aplicar a proposição 33 (tomando $p=q_1$, $q = q_2\ldots q_r$ e $H = K[q_1;M]$) e temos $x \in K[q_1;M_1]$.

Dadas matrizes $M_1,\ldots,M_r$ de ordem $n \times n$, tais que cada M_k satisfaça a condição (Dq_k), ou M_k é a matriz unidade, e além disso, $q_1 = q_r$ e $q_i \neq q_1$ se $1 \leqslant i \leqslant r$, dizemos que elas satisfazem a condição $(q_1 * q_r)$ se a matriz $M_{J_r \times N_n}$ tem q_1-pôsto $|J_1|$ onde $M = M_1 \times \ldots \times M_r$. Lembremos que se $M_1 = (m_k^{(1)})$ então $J_1 = \left\{ k \in N_n \mid m_{kk}^{(1)} = 1 \right\}$.

Teorema 36 - Seja $L = K[q_1,M_1;q_2,M_2;\ldots;q_r;M_r]$ onde $q_1 = q_r$ e $q_i \neq q_1$ se $1 \leqslant i \leqslant r$; $K(q_1;L) = K[q_1;M_1]$ se e sòmente se a condição $(q_1 * q_r)$ estiver satisfeita.

Antes de demonstrar êste teorema vamos demonstrar duas proposições. Conservamos as notações e hipóteses do teorema 36.

P

Proposição 37 - Se existe um elemento $x \in K(q_1;L)$ tal que $x \notin K[q_1,M_1]$, então existe um elemento $\bar{x} \in K(q_1,L)$ tal que $\bar{x} \notin K[q_1,M_1]$ e tal que

$$q_1\bar{x} = \sum_{j\in J_1} \bar{x}_j b_j .$$

Demonstração: se $x \in K(q_1,L)$ então $q_1 x \in K$ e portanto

$$q_1 x = \sum_{k=1}^{n} x_k b_k = \sum_{i\in I_1} x_i b_i + \sum_{j\in J_1} x_j b_j =$$

$$= \sum_{i\in I_1} x_i (q_1 b'_1 + \sum_{j\in J^{(i)}} m''_{ij} b_j) + \sum_{i\in J_1} x_j b_j ;$$

daí segue-se que

$$q_1(x - \sum_{i\in I_1} x_i b'_i) = \sum_{j\in J_1} \bar{x}_j b_j$$

e tomando

$$\bar{x} = x - \sum_{i\in I_1} x_i b'_i$$

temos $\bar{x} \in K(q_1,L)$ e $\bar{x} \notin K[q_1,M_1]$, pois senão teríamos $x \in K[q_1,M_1]$ já que $b'_i \in K[q_1,M_1]$, $i \in I_1$, por serem elementos de sua base canônica. (CQD).

A partir da base $b_1,\ldots,b_n$ de K determinamos a base canônica $b_1^{(1)},\ldots,b_n^{(1)}$ de $K[q_1,M_1]$, que por sua vez determina a base canônica $b_1^{(2)},\ldots,b_n^{(2)}$ de $K[q_1,M_1;q_r,M_r]$ e assim

por diante até chegarmos à base canônica $b_1^{(r)},\ldots,b_n^{(r)}$ de $L = K[q_1,M_1;\ldots;q_r,M_r]$ que, para simplificar a notação, indicaremos por $\bar{b}_1,\ldots,\bar{b}_n$. Temos então

$$\begin{matrix} b_1 \\ \vdots \\ b_n \end{matrix} = M \begin{matrix} \bar{b}_1 \\ \vdots \\ \bar{b}_n \end{matrix}$$

onde $M = (m_{kh}) = M_1 \times \ldots \times M_r$.

Proposição 38 - Seja $x \in L$ tal que

$$q_1 x = \sum_{s=1}^{n} x_s b_s \in K,$$

então temos

$$\sum_{s=k}^{n} x_s m_{sk} = q_1 y_k \equiv 0 \pmod{q_1}$$

para $k = 1,2,\ldots,n$. Recìprocamente, se existem inteiros $x_1,\ldots,x_n$ tais que

$$\sum_{s=k}^{n} x_s m_{sk} = q_1 y_k \equiv 0 \pmod{q_1}$$

para $k = 1,2,\ldots,n$ então

$$x = \sum_{k=1}^{n} y_k \bar{b}_k \in L$$

é tal que

$$q_1 x = \sum_{s=1}^{n} x_s b_s \in K.$$

Demonstração: se $x \in L$ temos

$$x = \sum_{k=1}^{n} y_k \bar{b}_k$$

e portanto

$$q_1 x = \sum_{k=1}^{n} (q_1 y_k) \bar{b}_k .$$

Por outro lado, se $q_1 x \in K$ temos

$$q_1 x = \sum_{s=1}^{n} x_s b_s = \sum_{s=1}^{n} x_s \left(\sum_{h=1}^{s} m_{sk} \bar{b}_k \right) = \sum_{k=1}^{n} \left(\sum_{s=k}^{n} x_s m_{sk} \right) \bar{b}_k$$

que comparado com a relação anterior nos dá

$$\sum_{s=k}^{n} x_s m_{sk} = q_1 y_k ,$$

para $k = 1,2,\ldots,n$. Recìprocamente, dados inteiros $x_1,\ldots,x_n$ tais que

$$\sum_{s=k}^{n} x_s m_{sk} = q_1 y_k \equiv 0 \pmod{q_1}$$

para $k = 1,2,\ldots,n$ tomamos

$$x = \sum_{k=1}^{n} y_k \bar{b}_k$$

e "voltando" as igualdades acima chegamos a

$$q_1 x = \sum_{s=1}^{n} x_s b_s ,$$

isto é, $q_1 x \in K$.

Demonstração do teorema 36: é evidente que

$$K(q_1;L) \supset K[q_1,M_1];$$

portanto $K(q_1;L) \neq K[q_1,M_1]$ se, e sòmente se, existe $x \in K(q_1;L)$ tal que $x \notin K[q_1,M_1]$. Pela proposição 37 isto é verdade se, e sòmente se, existe um elemento $\bar{x} \in K(q_1;L)$ tal que $\bar{x} \notin K[q_1,M_1]$ e tal que

$$q_1\bar{x} = \sum_{j\in J_1} \bar{x}_j b_j.$$

Mas pela proposição 38, se $\bar{x} \in K(q_1,L) \subset L$ e

$$q_1\bar{x} = \sum_{j\in J_1} \bar{x}_j b_j \in K$$

então os $\bar{x}_j$, $j \in J_1$, satisfazem o sistema

$$(\alpha) \qquad \sum_{j\in J_1,\, j\geq k} \bar{x}_j m_{jk} \equiv 0 \pmod{q_1}, \quad k \in N_n$$

e recìprocamente uma solução $(\bar{x}_j)_{j\in J_1}$ do sistema (α) defi um elemento $\bar{x} \in L$ e $\bar{x} \in K(q_1;L)$ pois $q_1\bar{x} \in K$.

Por outro lado, tomando $H = K$, $H[p] = K[q_1,M_1]$, $z' = \bar{x}$ e

$$z = q_1\bar{x} = \sum_{j\in J_1} \bar{x}_j b_j \in K,$$

segue-se da proposição 32 que $\bar{x} \notin K[q_1,M_1]$ se, e sòmente se,

existe um $j \in J_1$ tal que $\bar{x}_j \not\equiv 0 \pmod{q_1}$.

Portanto, existe um elemento $\bar{x} \in K(q_1;L)$ tal que $\bar{x} \notin K[q_1,M_1]$ se, e sòmente se, o sistema

$$(\propto) \qquad \sum_{j\in J_1,\, j\geqslant k} \bar{x}_j m_{jk} \equiv 0 \pmod{q_1}, \quad k \in N_n,$$

tem uma solução $(\bar{x}_j)_{j\in J_1} \not\equiv 0 \pmod{q_1}$. Podemos substituir os $\bar{x}_j$ e os m_{jk} pelas suas classes de restos do corpo $Z/(q_1)$ e considerar o sistema assim resultante de $(\propto)$, sobre o corpo $Z/(q_1)$, pois a tôda solução $(\bar{x}_j) \not\equiv 0 \pmod{q_1}$ de $(\propto)$ corponde uma solução não idênticamente nula do sistema relativamente a $Z/(q_1)$ e recìprocamente. A matriz dêste sistema é de ordem $|J_1| \times n$ e o sistema tem $|J_1|$ incógnitas (as classes de restos dos $\bar{x}_j$, $j \in J_1$). Portanto, o sistema tem uma solução não idênticamente nula se, e sòmente se, a sua matriz tem pôsto $< |J_1|$ e isto equivale a dizer que a matriz $M_{J_1 \times N_n}$ do sistema $(\propto)$ tem q_1-pôsto $< |J_1|$. CQD.

Lembrando os corolários da proposição 30, a demonstração do teorema acima também nos dá o

Corolário 1 - Se $M_1,\ldots,M_r$ satisfazem à condição $(q_1 \ast q_r)$ então para todo $s \in N_n$ as matrizes

$$(M_1)_{N_s \times N_s},\ldots,(M_r)_{N_s \times N_s},$$

de ordem $s \times s$ também satisfazem à condição $(q_1 \ast q_r)$.

Corolário 2 - Sejam $M_1,\ldots,M_r$ matrizes que satisfazem à condição $(q_1 * q_r)$ e sejam

$$I_1 = \{i_1,i_2,\ldots,i_r\} \quad \text{e} \quad I_r = \{i'_1,i'_2,\ldots,i'_t\}.$$

Então $s \geqslant t$ e para todo $k \in N_t$ temos $i_k \leqslant i'_k$.

Demonstração:- Se para algum $s \in N_n$ tivéssemos

$$|I_1^{(s)}| < |I_r^{(s)}|$$

teríamos $|J_1^{(s)}| > |J_r^{(s)}|$ e portanto o q_1-pôsto de $M_{J_1^{(s)}} \times N_s$ seria $|J_r^{(s)}| < |J_1^{(s)}|$ (pois o pôsto de um produto é $\leqslant$ ao menor dos postos dos fatores) contrário ao corolário 1. Daí segue-se que $j_k \geqslant j'_k$ para $j'_k \in J_r$ e portanto o corolário 2.

Corolário 3 - Se $I_1 \supset I_r$ a condição $(q_1 * q_r)$ está satisfeita.

Demonstração: se $I_1 \supset I_r$ então $J_1 \subset J_r$ e dado $j \in J_1$ temos $m_{jj} \equiv 0 \pmod{q_1}$ pois

$$m_{jj} = q_1^{\varepsilon_1} q_2^{\varepsilon_2} \cdots q_r^{\varepsilon_r},$$

onde $\varepsilon_k = 0$ se $k \in J_k$ e $\varepsilon_k = 1$ se $k \in I_k$. Seja h o último elemento de J_1; a última equação do sistema $(\propto)$ se reduz a $\bar{x}_h m_{hh} \equiv 0 \pmod{q_1}$ e como $m_{hh} \not\equiv 0 \pmod{q_1}$ segue-se que $\bar{x}_h \equiv 0 \pmod{q_1}$. Se agora h' é o maior elemento de J_1 que precede h demonstra-se de modo análogo que

$$\bar{x}_{h'} \equiv 0 \pmod{q_1}$$

e assim por diante. Portanto o sistema $(\propto)$ só tem a solução $\bar{x}_j \equiv 0 \pmod{q_1}$, $j \in J_1$, isto é, a condição $(q_1 * q_r)$ está satisfeita como resulta das condições equivalentes que usamos na

demonstração do teorema 36.

§ 4º. Classificação dos grupos sem torção.

Neste parágrafo damos finalmente a classificação dos grupos sem torção. Começamos classificando os grupos de Q^n, associando a cada subgrupo de Q^n (satisfazendo ainda certas condições) uma sequência de matrizes inteiras de ordem $n \times n$ e satisfazendo a condição $(*)$ (teorema 41) ou equivalentemente uma certa matriz de elementos (q_n)-ádicos; recìprocamente, a tô da matriz assim corresponde um subgrupo de Q^n.

No nº 2 consideramos o caso de grupos sem torção de pôsto finito e no nº 3 estendemos a classificação a subgrupos de $Q^{(L)}$, sem restrição de pôsto portanto. No nº 4 abordamos ràpidamente o problema da existência de outros invariantes dos grupos de pôsto finito, além do tipo de sua característica.

1. Classificação dos subgrupos de Q^n.

Vamos classificar os subgrupos G de Q^n que contêm Z^n. Tomemos $H = Z^n$ e seja A o o-ideal associado a G (relativamente a H) (ver o teorema 25), (n_p) a característica de G relativamente a H e (q_n) a sequência principal associada a (n_p). De agora em diante, suporemos que a sequência (q_n) seja infinita, isto é, que

$$\sum_{p \in P} n_p = \infty$$

(prop. 6) ou ainda, que G não seja um grupo livre, caso em que esta classificação fica trivial como teremos ocasião de ver.

Consideremos a sequência

$$H_1 = H(q_1;G),\ldots,H_r = H(q_1,\ldots,q_r;G),\ldots$$

de subgrupos de G. Seja $g_r = q_1 q_2 \ldots q_r$ (sistema crescente de geradores de A). Temos então a

Proposição 39 - $H_r \subsetneq H_{r+1}$.

Demonstração: é evidente que $H_r \subset H_{r+1}$. Como $g_{r+1} \in A$ segue-se do teorema 26 que existe um elemento $x \in G$ tal que $m_x = g_{r+1}$, isto é, tal que $g_{r+1}x \in H$ e tal que $mx \in H$ implica $g_{r+1} | m$. Portanto $x \in H_{r+1}$ e $x \notin H_r$, pois senão $g_r x \in H$ e portanto $g_r | g_{r+1} = g_r \cdot q_{r+1}$ o que é absurdo.

Proposição 40 - $G = \bigcup_{r\in N} H_r$

Demonstração: Dado $x \in G$ temos $m_x x \in H$ e $m_x \in A$; portanto existe um r tal que $g_r > m_x$; logo, $x \in H(g_r;G) = H_r$.

Tomemos agora a base natural $b_1,\ldots,b_n$ de $H=Z^n$ (b_i é o elemento de Z^n cuja i-ésima coordenada é 1 e cujas outras coordenadas são nulas). Do teorema 29 segue-se então que

$$H(q_1;G) = H[q_1,M_1]$$

e

$$H_r = H(g_r;G) = H(q_1,\ldots,q_r;G) = H[q_1,M_1;\ldots;q_r,M_r]$$

e portanto o

Corolário - Todo subgrupo de Q^n é a reunião de uma sequência crescente de grupos livres.

Do teorema 29 segue-se ainda que as matrizes M_r satisfazem as condições (Dq_r); chamamo-las de sequência de matrizes associada ao grupo G.

Seja $q_r = q_{r+s}$ e tal que $q_i \neq q_{p+}$ se $r<i<r+s$. Fa-

zendo $K = H_{r-1}$, $L = H_{r+s} = K[q_r, M_r; \ldots; q_{r+s}, M_{r+s}]$ temos evidentemente

$$K(q_r, L) = H(g_r, L) = H(q_1, \ldots, q_{r-1}; L) =$$

$$= H[q_1, M_1; \ldots; q_{r-1}, M_{r-1}; q_r, M_r] = K[q_r, M_r]$$

e portanto (teorema 36) as matrizes $M_r, M_{r+1}, \ldots, M_{r+s}$ satisfazem à condição $(q_r * q_{r+s})$. Isto nos leva à seguinte definição: dizemos que uma sequência $(M_r)_{r \in N}$ de matrizes de ordem n n satisfaz à condição $(*)$ se: 1) Cada matriz M_r satisfaz uma condição (Dq_r); 2) A sequência (q_r) é principal; 3) Dados $q_r = q_{r+s}$ tais que $q_i \neq q_r$ para $r < i < r+s$ então as matrizes $M_r, M_{r+1}, \ldots, M_{r+s}$ satisfazem à condição $(q_r * q_{r+s})$. Dizemos neste caso que (q_r) é a sequência principal associada à sequência de matrizes (M_r).

Mostramos portanto que a sequência de matrizes (M_r) que associamos ao grupo G satisfaz à condição $(*)$. Se G' é outro subgrupo de Q^n que contém Z^n e se (M'_r) é a sequência de matrizes definida por G', então se $G \neq G'$, seja z o primeiro dos inteiros s tais que

$$H(q_1, \ldots, q_s; G) \neq H(q'_1, \ldots, q'_s; G');$$

teremos $M_r \neq M'_r$ e portanto a sequência (M_s) será diferente da sequência (M'_s). Demonstramos portanto o

Teorema 41 - A aplicação que a todo subgrupo G de Q^n, que contém Z^n e que não é livre, associa (pelo processo acima) uma sequência (M_r) de matrizes (satisfazendo à condição $(*)$) é biunívoca.

Da própria definição da condição $(*)$ vem a

Proposição 42 - Se a sequência $(M_r)_{r\in N}$ satisfaz à condição $(*)$ o mesmo será verdade para a sequência $(M_{m+r})_{r\in N}$ onde $m \in N$.

Proposição 43 - Seja (M_r) uma sequência de matrizes de ordem $n\times n$ que satisfaz à condição $(*)$ e seja (q_r) sua sequência principal associada. Tomemos $H = Z^n$ e definamos

$$K_m = H[q_1, M_1; \ldots; q_m, M_m]$$

e seja $G = \bigcup_{m\in N} K_m$. Para quaisquer $r,m \in N$ temos:

$$K_r(q_{r+1}, \ldots, q_{r+m}; G) = K_r[q_{r+1}, M_{r+1}; \ldots; q_{r+m}, M_{r+m}].$$

Demonstração: por causa da proposição 42 basta fazer a demonstração para $r = 0$ (isto é, $K_o = H$). Temos evidentemente

$$H(q_1, \ldots, q_m; G) \supset K_m = H[q_1, M_1; \ldots; q_m, M_m];$$

vamos mostrar a inclusão inversa. Suponhamos que ela não fosse verdadeira e seja m o primeiro inteiro tal que

$$H(q_1, \ldots, q_m; G) \supsetneq H[q_1, M_1; \ldots; q_m, M_m].$$

Portanto $H_{m-1} = H(q_1, \ldots, q_{m-1}; G) = K_{m-1}$. Seja

$$x \in H(q_1, \ldots, q_m; G) = H_m$$

e seja r o menos dos inteiros j tais que $x \in K_j$ (existe um inteiro j com esta propriedade pois $G = \bigcup_{s\in N} K_s$). Basta então demonstrar que não podemos ter $r > m$. Suponhamos que $r = m+t > m$: A - Se $q_m \neq q_{m+t}$, fazendo

$$K = H(q_1, \ldots, q_{m-1}; G) = H_{m-1} = K_{m-1}$$

e

$$L = K[q_m, M_m; \ldots; q_{m+t}, M_{m+t}] = K_{m+t} = K_r$$

segue-se da proposição 35 que $K(q_m; L) = K[q_m, M_m]$ e como

$$H_m = H(q_1, \ldots, q_m; G) = K(q_m; G) = K(q_m; L)$$

segue-se que $x \in K_m = K[q_m, M_m]$. B - Se $q_m = q_{m+t}$ seja s, o maior inteiro $0 \leqslant s < t$ tal que $q_{m+s} = q_m$; então temos

$$q_{m+s} = q_{m+t} \qquad \text{e} \qquad q_r \neq q_{m+s}$$

se $m+s < i < m+t$. Por hipótese $x \in K_r$ $(r=m+t)$; tomando

$$K = K_{m+s-1} \quad \text{e} \quad L = K[q_{m+s}, M_{m+s}; \ldots; q_{m+t}, M_{m+t}]$$

temos, pelo teorema 36, que

$$K(q_{m+s}, L) = K[q_{m+s}; M_{m+s}].$$

Mas $x \in H_m$ logo $q_m.x \in H_{m-1} \subset K \subset L$ e como $q_m = q_{m+s} = q_{m+t}$ temos

$$x \in K(q_{m+s}, L) = K[q_{m+s}; M_{m+s}] = K_{m+s}$$

contra a hipótese de $r = m + t > m + s$ ser o menor inteiro j tal que $x \in K_j$. CQD.

Recìprocamente, dada uma sequência $(M_r)_{r \in N}$ de matrizes de ordem $n \times n$ e uma sequência principal (q_r) tal que cada M_r satisfaz à condição (Dq_r) definimos

$$K_m = H[q_1, M_1; \ldots; q_m, M_m]$$

e

$$G = \bigcup_{m \in N} K_m \qquad (H = Z^n):$$

se

$$K_m(q_{m+1}, \ldots, q_{m+t}; G) = K_m[q_{m+1}, M_{m+1}; \ldots; q_{m+t}, M_{m+t}]$$

para todos $m,t \in N$, temos também

$$K_m(q_{m+1},\dots,q_{m+t};K_{m+t}) = K_m[q_{m+1},M_{m+1};\dots;q_{m+t},M_{m+t}]$$

(pois

$$K_m(q_{m+1},\dots,q_{m+t};G) \supset K_m(q_{m+1},\dots,q_{m+t};K_{m+t}) \supset$$
$$\supset K_m[q_{m+1},M_{m+1};\dots;q_{m+t},M_{m+t}])$$

e portanto o teorema 36 assegura-nos que vale a condição $(*)$.

Demonstramos portanto o

Teorema 44 - Dada uma sequência principal (q_r) e uma sequência (M_r) de matrizes de ordem $n\times n$ tal que M_r satisfaça a condição (Dq_r) $(r \in N)$, seja

$$K_m = H[q_1,M_1;\dots;q_m,M_m] \quad \text{e} \quad G = \bigcup_{m\in N} K_m \quad (H = Z^n)$$

então a sequência (M_r) satisfaz à condição $(*)$ se, e sòmente se

$$K_r(q_{r+1},\dots,q_{r+t};G) = K_r[q_{r+1},M_{r+1};\dots;q_{r+t},M_{r+t}]$$

para todos os inteiros $r,t \geqslant 0$.

Com as mesmas notações temos a

Proposição 45 - Se a sequência de matrizes (M_r) satisfaz à condição $(*)$ então para todo $r \in N$ existe um elemento $x \in K_r = H[q_1,M_1;\dots;q_r;M_r]$ tal que $m_x = g_r = q_1 \cdots q_r$.

(Ver o teorema 26 para a definição de m_x).

Demonstração: Se $r = 1$ basta tomar $x = b_r^{(1)}$ e $i \in I_1$; suponhamos a proposição demonstrada para $r = s$ e seja $y \in K_s$ tal que $m_y = g_s = q_1 \cdots q_s$. Seja $q_{s+1} = p$ e $g_{s+1} = qp^m$ com

$(q;p^m) = 1$, então $g_s = qp^{m-1}$; para todo $x \in K_{s+1}$ temos $m_x | g_{s+1}$ pois $g_{s+1}x \in H = Z^n$ e tomando um elemento $x \in K_{s+1}$ tal que $x \notin K_s$ temos então $m_x = q'p^m$. Pelo lema 2 do nº2, §2º existe então um elemento $z \in H_{s+1}$ tal que $m_z = [m_x, m_y] = qp^m = g_{s+1}$.

Estamos agora em condições de demonstrar o

Teorema 46 - A tôda sequência (M_r) de matrizes de ordem n n que satisfaz à condição $(*)$ podemos associar um subgrupo de Q^n, que contém Z^n e que não é livre, tal que a característica de G relativamente a Z^n tenha como sequência principal a sequência principal associada a (M_r) e que a sequência de matrizes que corresponde a G, pelo teorema 41, seja a própria sequência (M_r).

Demonstração: tomamos $H = Z^n$ e definimos

$$K_r = H[q_1, M_1; \ldots; q_r, M_r] \quad \text{e} \quad G = \bigcup_{r \in N} K_r;$$

então G é um subgrupo de Q^n que contém Z^n e que não é livre (por ser reunião de uma sequência estritamente crescente de subgrupos de Q^n). Da proposição 45 segue-se que o o-ideal de G relativamente a $H = Z^n$ tem os $g_r = q_1 \ldots q_r$ como sistema crescente de geradores e portanto a sequência principal associada é (q_r) mesmo. Do teorema 44 segue-se (fazendo r = 0, isto é, para $K_o = H = Z^n$) que a sequência de matrizes associada a G é a própria sequência (M_r). CQD.

Reunindo os teoremas 41 e 46 temos o

Teorema 47 - A aplicação que a todo subgrupo de Q^n, que contém Z^n e que não é livre, associa uma sequência (M_r) de matrizes de ordem $n \times n$ é uma aplicação biunívoca do conjunto de todos os grupos não livres G tais que $Z^n \subset G \subset Q^n$ sôbre o conjunto de tôdas as sequências de matrizes de ordem $n \times n$ que satisfazem à condição $(*)$.

Dada uma sequência $M_r = (m_{kh}^{(r)})$ de matrizes de ordem $n \times n$ que satisfazem a condição $(*)$ vamos lhe associar uma matriz $\mathfrak{M} = (m_{kh})$ de números (q_r)-ádicos, onde (q_r) é a sequência principal associada à sequência de matrizes M_r. Se $k \neq h$ tomamos m_{kh} como o elemento de $Z(q_r)$ cujo desenvolvimento (q_r)-ádico é $(m_{kh}^{(1)}, m_{kh}^{(2)}, \ldots, m_{kh}^{(r)}, \ldots)$ e se $k = h$ tomamos m_{kk} como o elemento de $Z(q_r)$ cujo desenvolvimento (q_r)-ádico é $(\bar{m}_{kk}^{(1)}, \bar{m}_{kk}^{(2)}, \ldots, \bar{m}_{kk}^{(r)}, \ldots)$, onde $\bar{m}_{kk}^{(r)} = 1$ se $m_{kk}^{(r)} = 1$, isto é, se $k \in J_r$ e $\bar{m}_{kk}^{(r)} = 0$ se $m_{kk}^{(r)} = q_r$, isto é, se $k \in I_r$. Chamamos $\mathfrak{M}$ de matriz associada ao grupo G.

Esta matriz $\mathfrak{M}$ de ordem $n \times n$ de elementos de $Z(q_r)$ é então tal que, considerando para cada r a matriz M_r formada pelos r-ésimos têrmos do desenvolvimento (q_r)-ádico dos elementos m_{kh} de $\mathfrak{M}$ (onde substituimos os elementos nulos da diagonal por q_r) a sequência M_r satisfaz à condição $(*)$. Dizemos então simplesmente que a própria matriz $\mathfrak{M}$ satisfaz à condição $(*)$.

O teorema 47 então pode ser enunciado:

Teorema 48 - Existe uma aplicação biunívoca do conjunto de todos os grupos não livres G tais que $Z^n \subset G \subset Q^n$, sôbre o conjunto de tôdas as matrizes $\mathfrak{M}$ de ordem $n \times n$ formada de elementos (q_r)-ádicos, que satisfazem à condição $(*)$ ((q_r) per

correndo tôdas as sequências principais infinitas).

Quando temos um subgrupo G de Q^n contendo Z^n e livre então sua característica é finita (basta aplicar o lema 3 do nº 1 do § 2º a uma base de G; teremos então $m > m_x$ para todo $x \in G$ e o resultado segue-se da proposição 6) e portanto a sequência principal associada será uma sequência finita: $q_1,\ldots,q_r$ e teremos $G = H(q_1,M_1;\ldots;q_r,M_r)$. Se $\bar{b}_1,\ldots,\bar{b}_n$ for a base de G associada à base natural de $H = Z^n$, teremos

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = M \begin{pmatrix} \bar{b}_1 \\ \vdots \\ \bar{b}_n \end{pmatrix}$$

onde $M = M_1 \times \ldots \times M_r$ e esta matriz determina completamente G. Naturalmente a sequência finita $M_1,\ldots,M_r$ satisfaz uma condição análoga à condição $(*)$; recìprocamente, dada uma sequência finita $M_1,\ldots,M_r$ de matrizes satisfazendo esta condição, ela determina um e um só subgrupo livre G de Q^n que contém Z^n.

2. Grupos sem torção de pôsto finito.

Se G for um grupo sem torção de pôsto finito n, que não é dado "a priori" como subgrupo de Q^n, então para associar a G uma matriz $\mathfrak{M}$ ou uma sequência de matrizes inteiras (M_r) vamos ter de escolher um subgrupo livre H de G de pôsto n e uma base $b_1,\ldots,b_n$ dêste subgrupo e a matriz $\mathfrak{M}$, ou, a sequência M_r, vai depender de H e da base escolhida, se bem que o tipo da sequência principal associada à sequência M_r só dependa do grupo G.

Neste caso interessaria achar como varia a matriz $\mathfrak{M}$ quando variamos H e a base $b_1,\ldots,b_n$ de H. Êste problema é equivalente ao problema de determinar a partir das matrizes $\mathfrak{M}$, $\mathfrak{M}'$, associadas, respectivamente, a dois subgrupos G e G' de Q^n, condições necessárias e suficientes para que êstes subgrupos sejam isomorfos (uma condição necessária, como vimos, é que a característica de suas sequências principais sejam do mesmo tipo). A solução do problema poderia ser expressa em função de transformações elementares como o faz Kurosh [K], mas esta solução não é satisfatória por não ser simples e nem de manejo fácil. Esperamos abordar êste problema do isomorfismo num outro trabalho com idéias diferentes das de Kurosh.

3. Subgrupos de $Q^{(L)}$.

Consideremos agora grupos G tais que $Z^{(L)} \subset G \subset Q^{(L)}$ onde L é um conjunto qualquer que supomos bem ordenado (isto é, totalmente ordenado e tal que todo seu subconjunto não vazio tem um primeiro elemento). Tomando $H = Z^{(L)}$ o teorema 26 nos permite definir a característica de G relativamente a H, mas agora o tipo desta característica não mais é um invariante de G (ver observação final de § 2º). Considerando a sequência principal (q_s) da característica de G, ainda vale o análogo do teorema 29, substituindo matriz de ordem finita por matrizes transfinitas $M = (m_{kh})_{(k,h) \in L \times L}$ e vamos ter

$$pb'_i = b_i - \sum_{j \in J,\, j<i} m_{ij} b_j$$

quando $i \in I$ e onde $(m_{ij})_{j \in J}$ é uma família quasi-nula de

inteiros tais que $0 \leqslant m_{ij} < p$ e portanto a matriz transfinita M só vai ter um número finito de elementos diferentes de zero em cada linha, condição esta que vamos ter que incluir na condição (Dp) no caso das matrizes transfinitas. A demonstração do teorema 29, assim generalizado, é então exatamente igual a do teorema 29 para grupos de pôsto finito, substituindo-se apenas a indução finita pela indução transfinita; naturalmente qualquer soma finita

$$\sum_{k=1}^{n} z_k b_k$$

será substituida sempre por uma soma da forma

$$\sum_{k \in L} z_k b_k,$$

onde a família $(z_k)_{k \in L}$ é quasi-nula. As proposições 30 a 35 ainda valem. A condição $(q_1 * q_r)$ tem de ser formula do seguinte modo: a matriz $M_{J_1 \times L}$, onde $M = M_1 \times \ldots \times M_r$ deve ter q_1-pôsto máximo, isto é, o sistema

$$(\alpha) \qquad \sum_{j \in J_1} x_j m_{jk} \equiv 0 \pmod{q_1}, \quad k \in L$$

onde (x_j) é uma família quasi-nula de inteiros, só deve ter solução $x_j \equiv 0 \pmod{q_1}$ para todo $j \in J_1$. A multiplicação de matrizes tem sentido, pois cada matriz M_i só tem um número finito de elementos diferentes de zero em cada linha, portanto podemos multiplicar estas matrizes (da direita para a esquerda!: $M_1(M_2[M_3 \times M_4])$). Então ainda valem todos os teoremas do §4º, substituindo naturalmente as matrizes M_r de ordem $n \times n$ por

matrizes transfinitas de inteiros e considerando em $Z^{(L)}$ a base canônica $(b_k)_{k\in L}$ (b_k é o elemento de $Z^{(L)}$ cuja coordenada k-ésima é 1 e cujas outras coordenadas são nulas). No teorema 48, a matriz $\mathfrak{M}$ de ordem $n\times n$ de números (q_r)-ádicos que satisfaz a condição $(*)$ é substituida por uma matriz transfinita $\mathfrak{M} = (m_{kh})_{(k,h)\in L\times L}$ de números (q_r)-ádicos, matriz esta que deve satisfazer à condição $(*)$.

Do mesmo modo, se G é um grupo sem torção de pôsto qualquer podemos considerar um subgrupo livre e pleno H de G, por exemplo, o subgrupo H gerado por uma semibase $(b_k)_{k\in L}$ de G e bem ordenando L, podemos aplicar os resultados acima para associar a G uma matriz relativamente a H e à base $(b_k)_{k\in L}$.

4. p-pôsto reduzido.

Dado o grupo G tal que $Z^n \subset G \subset Q^n$ seja (n_p) sua sequência característica e (q_r) sua sequência principal. Para todo primo p consideremos a subsequência $q_{r_1},\ldots,q_{r_m},\ldots$ finita, ou infinita, ou vazia dos elementos $q_r = p$ e definamos

$$r_p = \lim_{m\to\infty} |I_{q_{r_m}}|$$

que chamamos p-pôsto reduzido: o p-pôsto reduzido é nulo se só existe um número finito de elementos $q_r = p$. $r_p \neq 0$ se e sòmente se $n_p = \infty$.

Pode-se demonstrar que os p-postos reduzidos só dependem de G e não da sequência principal, nem do subgrupo H isomorfo a Z^n de G, sendo portanto invariante de G (que coin-

cide com as noções de mesmo nome definidas por Kursoh e Szekeres).

Êstes invariantes evidentemente ainda não são suficientes para caracterizar G : qualquer grupo com tipo (n_p) onde n_p é finito para todo $p \in P$, tem todos êstes invariantes nulos, mas êstes grupos não são necessàriamente isomorfos entre si.

Para grupos de pôsto infinito o p-pôsto reduzido não é mais um invariante do grupo.

Índice de notações.

ÍNDICE TERMINOLÓGICO.

Referências bibliográficas.

[A-C] - Alexander and Cohen: "A classification of the homology groups of compact spaces", Ann. of Math., vol.33 (1932), pp. 538-566.

[B] - Baer: "Abelian groups without elements of finite order" Duke Math. J., vol.3 (1937), pp. 68-122.

[B. Alg.VII] - Bourbaki: "Algèbre", Chap. VII, Hermann (Paris).

[B-E] - Bourbaki: "Théorie des ensembles" (fascicule de resultats), Hermann (Paris)

[B-I] a [B-IX] - Bourbaki: "Topologie Générale", Chaps. I a IX, 1ª edição, Hermann (Paris).

[B-I'] - Bourbaki: "Topologie Générale", Chaps. I, II (2ª edição) Hermann (Paris).

[B-Z] - Beaumont and Zukermann: "A characterization of the subgroups of the aditive rationals", Pacific J. Math., vol. 1 (1951), pp.169-177.

[D] - Derry - "Uber eine Klasse von Abelschen Gruppen", Proc. London Math. Soc., vol.43(1937), pp.490-506.

[v.D-1]+ - van Dantzig: "Groupes monoboliques et fonctions presque périodiques", C.R.Paris (1933), pp.1074-1076.

[v.D-2] - van Dantzig: "Zur topologischen Algebra", Compositio Math., vol. 2 (1935), pp. 201-223.

[H-1] - Hönig: "Classificação dos grupos aditivos de números racionais", Bol. Soc. Mat. de São Paulo, vol.3 (1951), pp. 37-47.

[H-2] - Hönig: Tese de livre docência à cadeira de Análise Superior da FFCL da USP (em preparação).

[K] - Kurosh: "Primitive torsionsfreie abelsche Gruppen von endlichen Range", Ann. of Math., vol38(1937), pp.175-203.

[K-1] - Kurosh: "Gruppentheorie", Akademie-Verlag, Berlin (1953).

[K-2] - Kurosh: "The theory of groups", vol.1, Chelsea Publ. N. Y. (1955).

[L]+ - Lyapin: "On the decomposition of abelian groups into direct sums of rational groups", Mat. Sbornik, vol.8(1940), pp. 205-237.

[P] - Pontrjagin: "The Theory of Topological Commutative Groups" Ann. of Math., vol.35 (1934), pp.361-388.

[Pr]- Prüfer: "Neue Begründung der algebraischen Zahlentheorie", Math. Annalen, Bd. 94(1925), pp. 198-243.

[Py]- Pietrkowsky: "Zur Theorie der unendlichen Abelschen Gruppen", Math. Annalen, Bd. 1o4(1931),pp.535-569.

[Sz] - Szekeres: "Countable abelian groups without torsion", Duke Math. J., vol.15 (1948), pp. 293-306.

(+) Não temos conhecimento direto dêstes trabalhos.