APROXIMAÇÃO FORTE EM GRUPOS CLÁSSICOS

Laercio Luiz Vendite

Prof. Dr. Nelo da Silva Allan

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática.

Este trabalho foi realizado com apoio financeiro da Fundação de Amparo à Pesquisa do Estado de São Paulo FAPESP

JUNHO 1978

Para Shirley que me fêz...

e Sandra com quem farei...

Agradecimentos

A todos que colaboraram na realização deste trabalho, a minha sincera gratidão.

Em especial ao meu orientador Professor Nelo da Silva Allan pelo apoio e incentivo, ao Professor Antonio Paques pelas discussões de alguns tópicos, ao colega Walter Alexandre Carnielli pelo apoio sempre frequente e à FAPESP cujo auxilio financeiro a tornou possível.

Laercio Luiz Vendite

I N D I C E

I N T R O D U Ç Ã O

No início deste século Meyer provou que toda matriz $(n \times n)$ A simétrica, unimodular, indefinida, com coeficientes inteiros e $n \geq 5$ pode ser diagonalizada.

Nos meados da década de 20 Hasse introduziu o processo da localização, afim de estudar a relação entre as formas quadráticas localmente e globalmente, determinando completamente uma classe de invariantes para formas quadráticas. No início da decada de 50, Kneser refez a prova do teorema de Meyer usando um refinamento da tecnica de Hasse. O problema foi somente reformulado geometricamente em termos de teoria local. A principal parte da prova consiste em mostrar que só existe uma classe no genus espinorial de A e a reformulação desta proposição é o teorema da aproximação forte. Desse resultado conclui-se também que o número de classe em cada genus é finito. Esses resultados podem ser extendidos a várias classes de grupos.

O objetivo deste trabalho é demonstrar o teorema da aproximação forte para o grupo espinorial com o minimo de detalhes possível, dai a restrição às dimensões maiores ou iguais a 5. Para não prolongar demais o trabalho e evidenciar as ideias en

volvidas cujo objetivo principal é a aproximação dos geradores , decidimos omitir algumas provas, as quais o leitor poderá, depois de compreendido o global, consultar [0].

No capítulo I introduzimos a noção de corpos com valorização e completamento e demonstramos os teoremas da aproximação fraca e da aproximação forte para o completado F_p de um corpo F.

No capítulo II apresentamos uma geometria ortogonal para um espaço vetorial de dimensão finita e estudamos certos grupos de transformações lineares; mais especificamente o grupo Ortogonal, seus principais subgrupos e sua geração por simetrias.

No capítulo III estudamos o grupo ortogonal sobre corpos com valorizações e sobre corpos globais, como também o teorema da aproximação fraca para rotações.

E, finalmente no capítulo IV apresentamos o teorema da aproximação forte para rotações, para dimensões maiores ou iguais a 5.

CAPITULO I

CORPOS P.ADICOS

§1. CORPOS COM VALORIZAÇÕES

O conceito de valorização é utilizado com a finalidade de introduzir uma estrutura de espaços métricos em corpos e daí obter novos corpos através do completamento. Serão considerados conhecidos os resultados mais elementares de espaços métricos e grupos topológicos.

VALORIZAÇÃO

Seja F um corpo. Uma valorização de F é uma aplicação $|\ |: F \to \mathbb{R}$ que satisfaz

(i) $|\alpha| > 0$ se $\alpha \neq 0$ e $|0| = 0$

(ii) $|\alpha\beta| = |\alpha| \cdot |\beta|$.

(iii) $|\alpha+\beta| \leq |\alpha|+|\beta|$

Se $|\ |: F \to \mathbb{R}$ é uma aplicação que satisfaz as condições i), ii) e mais

iv) $|\alpha+\beta| \leq \max(|\alpha|, |\beta|)$

então $|\ |$ também é uma valorização. Isto acontece pois se $|\ |$ satisfaz iv) então $|\ |$ satisfaz iii).

A valorização será trivial quando $|\alpha| = 1$ para todo $\alpha \in \dot{F}$; será não-arquimediana quando satisfaz a condição iv) e arquimediana caso contrário.

Quando a valorização fôr não arquimediana verificamos que o conjunto dos elementos onde ela é menor ou igual que 1 é fechado relativamente à soma e multiplicação, e portanto esse conjunto forma uma sub-anel de F, chamado anel dos inteiros de F.

VALORIZAÇÃO NÃO ARQUIMEDIANA

Proposição 1.1 - $|\ |$ é não arquimediana se e somente se é limitada sobre os naturais de F.

Demonstração: Admitamos inicialmente que $|\ |$ é não arquimediana. Desde que todo natural de F é uma soma finita da forma $1 + 1 + 1 + \ldots 1$, então por iv) $|1+\ldots+1| \leq 1$ e isto mostra que $|\ |$ é limitada sobre os naturais de F.

Reciprocamente se para todo inteiro natural m em F, existe $M > 0$ tal que $|m| \leq M$, então

$$|\alpha + \beta|^n = |(\alpha + \beta)^n|$$

$$= |\alpha^n + \binom{n}{1}\alpha^{n-1}\beta + \ldots + \beta^n|$$

$$\leq |1||\alpha|^n + |\binom{n}{1}||\alpha|^{n-1}|\beta| + \ldots + |1||\beta|^n$$

$$\leq M\{|\alpha|^n + |\alpha|^{n-1}|\beta| + \ldots + |\beta|^n\}.$$

$$\leq M(n+1)\{\max(|\alpha|, |\beta|)\}^n$$

Portanto,

$$|\alpha+\beta| \leq M^{1/n}(n+1)^{1/n} \max(|\alpha|, |\beta|$$

e, quando $n \to \infty$ teremos o resultado desejado

c.q.d.

Observação 1.2 - Este resultado tem duas consequências imediatas.

1) Um corpo de característica $p > 0$ não pode ter valorização arquimediana.

2) Uma valorização de uma extensão E de F é não arquimediana se e somente se a valorização induzida sobre F é não arquimediana.

Principio da Dominação: Em um corpo não arquimediano temos $|\alpha_1 + \ldots + \alpha_n| \neq |\alpha_1|$ se $|\alpha_i| < |\alpha_1|$ para $i > 1$.

Demonstração: Aplicando o principio da indução, basta provar que $|\alpha+\beta| = |\alpha|$ quando $|\alpha| > |\beta|$

Temos

$$|\alpha| = |\alpha + \beta - \beta| \leq \max(|\beta|, |\alpha + \beta|)$$

e assim

$$|\alpha| \leq |\alpha + \beta| \quad \text{pois por hipotese } |\alpha| > |\beta| .$$

Mas

$$|\alpha + \beta| \leq \max(|\alpha|, |\beta|) = |\alpha|$$

logo

$$|\alpha + \beta| = |\alpha| . \qquad \text{c.q.d.}$$

Como consequência desse resultado temos:

Lema 1.3 - Se $\sum_{i=}^{\infty} \alpha_i$ é convergente, e $|\alpha_i| < |\alpha_1|$ para $i > 1$, então

$$\left|\sum_{i=1}^{\infty} \alpha_i\right| = |\alpha_1| .$$

VALORIZAÇÕES COMPLETAS

Seja $|\ |$ uma valorização em F. Então podemos definir uma distância em F da seguinte maneira

$$d(\alpha,\beta) = |\alpha-\beta| \ , \text{ para } \alpha,\beta \text{ em } F$$

Dessa forma podemos falar em topologia métrica e consequentemente introduzir conceitos de sequência de Cauchy e completamento com respeito à $d(\alpha,\beta)$. Diremos que $|\ |$ é completa se toda sequência de Cauchy em F tem limite em F.

VALORIZAÇÕES DISCRETAS

Seja F um corpo e consideremos o conjunto $|F| = \{|\alpha| \mid \alpha \in \dot{F}\}$ onde $|\ |$ é uma valorização não-trivial. Observamos que $|F|$ tem estrutura de grupo multiplicativo e que ele é infinito. O conjunto $|F|$ será denominado grupo de valorização de $|\ |$.

Definição 1.4 - Uma valorização é dita discreta se:

(i) $|\ |$ é não trivial

(ii) Se $|F|$ é um subgrupo cíclico do grupo multiplicativo P dos números reais positivos.

§2. APROXIMAÇÃO FRACA

VALORIZAÇÕES EQUIVALENTES

Consideremos duas valorizações $|\ |_1$ e $|\ |_2$ em um mesmo corpo F. Elas são equivalentes e escrevemos $|\ |_1 \sim |\ |_2$, se definem a mesma topologia sobre F.

Lema 2.1 - Sejam $|\ |_1$ e $|\ |_2$ valorizações sobre F. Então são equivalentes:

(i) $|\ |_1 \sim |\ |_2$

(ii) $|\alpha|_1 < 1$ se e somente se $|\alpha|_2 < 1$

(iii) Existe um número real positivo r tal que $|\alpha|_1^r = |\alpha|_2$ para todo $\alpha \in F$.

Demonstração: (i) implica (ii)

Basta mostrar que se $|\alpha|_1 < 1$ então $|\alpha|_2 < 1$. A recíproca é análoga.

Seja $N = \{x \in F \mid |x|_2 < 1\}$. Este conjunto é uma vizinhança de 0 na topologia induzida por $|\ |_2$.

Desde que $|\alpha^n|_1 = |\alpha|_1^n$ e $|\alpha|_1 < 1$ é sempre possivel encontrar n tal que $\alpha^n \in N$. Logo $|\alpha|_2^n < 1$ e, consequentemente, $|\alpha|_2 < 1$

(ii) implica (iii)

Usando a contraposição de (ii) temos que $|\alpha|_1 = 1$ se e somente se $|\alpha|_2 = 1$. Logo $|\ |_1$ é trivial se e somente se $|\ |_2$ é trivial.

Vamos supor que $|\ |_1$ e $|\ |_2$ não são triviais. Logo existe $\alpha_o \in F$ tal que $0 < |\alpha_o|_1 < 1$ e, pela hipotese, $0 < |\alpha_o|_2 < 1$. Assim

$$|\alpha_o|_2 = |\alpha_o|_1^r \quad \text{onde } r = \log |\alpha_o|_2 / \log |\alpha_o|_1 > 0.$$

Agora se existe α tal que $|\alpha|_2 \neq |\alpha|_1^r$, assumimos então $|\alpha|_2 < |\alpha|_1^r$. Logo existe um racional m/n, com $n > 0$ tal que $|\alpha|_2 < |\alpha_o|_2^{m/n} = |\alpha_o|_1^{r\,m/n} < |\alpha|_1^r$ e isto significa que $|\alpha^n / \alpha_o^m|_2 < 1$ e $|\alpha^n / \alpha_o^m|_1 > 1$ o que contraria a hipótese.

(iii) implica (i)

Se existe um r tal que $|\alpha|_1^r = |\alpha|_2$ para todo $\alpha \in F$

então é evidente que $|\ |_1$ e $|\ |_2$ definem a mesma topologia em F e, portanto são equivalentes.

c.q.d.

LUGARES PRIMOS

Consideremos um corpo F.

Denominamos lugar primo, ou lugar uma classe de equivalência de valorizações de F.

Lugar Primo $\mathcal{P} = \{|\ |_{\mathcal{P}} \mid |\ |_{\mathcal{P}}$ são equivalentes$\}$

Cada $|\ |_{\mathcal{P}} \in \mathcal{P}$ define uma mesma topologia em F. A essa topologia denominamos topologia $\mathcal{P}$-ádica em F. Se $\mathcal{P}$ contém pelo menos uma valorização trivial, então dizemos que $\mathcal{P}$ é trivial. Analogamente definimos lugares arquimedianos, não arquimedianos, completos e discretos.

Definição 2.2 - Seja $\mathcal{P}$ um lugar em F, dizemos que F é completo em $\mathcal{P}$ se existe pelo menos uma valorização completa em $\mathcal{P}$.

Observação 2.3

1) Como consequência de que $|\ |_1^r = |\ |_2$ são equivalentes, vemos que se F é completo então toda valorização em $\mathcal{P}$ é completa.

2) Se $\mathcal{P}$ é trivial em F então F é completo. Aqui toda sequência de Cauchy tem a forma $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha, \ldots, \alpha, \ldots$ que

converge para α .

Definição 2.4 - Dois lugares $\mathcal{P}$ e $\mathcal{Q}$ são iguais se e somente se as suas topologias são as mesmas.

TEOREMA DA APROXIMAÇÃO FRACA

Antes será necessário provarmos o seguinte resultado:

Lema 2.5 - Seja $\{|\ |_\lambda \ / \ (1 \leq \lambda \leq n)\}$ um conjunto finito de valorizações não equivalentes e não triviais em F. Então existe $\alpha \in F$ tal que $|\alpha|_1 > 1$ e $|\alpha|_\lambda < 1$ para $2 \leq \lambda \leq n$.

Demonstração: (Por indução sobre n)

Para n = 1, isto é verificado pelo fato de que $|\ .\ |_1$ é não trivial. Para n = 2, consideremos $|\ |_1$ e $|\ |_2$ não equivalentes. Logo existem b e c em F tal que

$$|b|_1 < 1 \text{ e } |b|_2 \geq 1 \quad \text{e} \quad |c|_1 \geq 1 \quad \text{e} \quad |c|_2 < 1 .$$

Logo, basta considerarmos $\alpha = \frac{c}{b}$ para obtermos

$$|\alpha|_1 = |\tfrac{c}{b}|_1 = \frac{|c|_1}{|b|_1} > 1 \quad \text{e} \quad |\alpha|_2 = |\tfrac{c}{b}|_2 = \frac{|c|_2}{|b|_2} < 1$$

Finalmente, admitamos que o resultado seja válido para (n-1). Sejam b com $|b|_1 > 1$ e $|b|_\lambda < 1$ onde $2 \leq \lambda \leq n-1$ e c com $|c|_1 < 1$ e $|c|_n < 1$. Se $|b|_n < 1$, está provado.

Se $|b|_n = 1$, colocamos $\alpha = cb^r$ com r suficientemente grande e obtemos $|cb^r|_1 > 1, |cb^r|_\lambda < 1$ $(2 \leq \lambda \leq n)$. Finalmente, se $|b|_n > 1$, constantamos que

$$\left|\frac{cb^r}{1+b^r}\right|_\lambda \quad \text{tende a} \quad \begin{cases} |c|_\lambda & \text{se } \lambda = 1 \text{ ou } \lambda = n. \\ 0 & \text{se } 2 \leq \lambda \leq n-1 \end{cases}$$

Assim $\alpha = \frac{cb^r}{1+b^r}$, com r suficientemente grande, é o elemento desejado.

c.q.d.

TEOREMA DA APROXIMAÇÃO FRACA: Seja $\{|\ |_\lambda \ / \ 1 \leq \lambda \leq n)\}$ um conjunto finito de valorizações não equivalentes e não triviais de F. Consideremos n elementos α_λ $(1 \leq \lambda \leq n)$ em F. Então para cada $\varepsilon > 0$ existe um elemento α em F tal que $|\alpha - \alpha_\lambda|_\lambda < \varepsilon$, para $1 \leq \lambda \leq n$.

Demonstração:

Para cada i $(1 \leq i \leq n)$ podemos encontrar $b_i \in F$ onde $|b_i|_i > 1$ e $|b_i|_\lambda < 1$ para $(\lambda \neq i)$, isto pelo lema 2.5 . Se r tende a infinito vemos que

$$\frac{b_i^r}{1+b_i^r} \quad \text{tende a} \quad \begin{cases} 1 \text{ sobre } |\ |_i \\ 0 \text{ sobre } |\ |_\lambda \text{ se } \lambda \neq i \end{cases}$$

e portanto,

$c_r = \sum_{i=1}^{n} \frac{\alpha_i b_i^r}{1+b_i^r}$ converge para α_i sobre a topologia definida por $|\ |_i$. Então $\alpha = c_r$, com r suficientemente grande.

c.q.d.

§3. APROXIMAÇÃO FORTE

CLASSE RESIDUAL

Sejam F um corpo arbitrário e $\mathfrak{p}$ um lugar primo não arquimediano.

Definimos:

$$o(\mathfrak{p}) = \{\alpha \in F \mid |\alpha|_{\mathfrak{p}} \leq 1\}$$

$$u(\mathfrak{p}) = \{\alpha \in F \mid |\alpha|_{\mathfrak{p}} = 1\}$$

$$m(\mathfrak{p}) = \{\alpha \in F \mid |\alpha|_{\mathfrak{p}} < 1\}$$

Segue-se das considerações feitas na pág. 2 que:

Lema 3.1 - $O(\mathfrak{p})$ é subanel de F tal que $1 \in O(\mathfrak{p})$.

Lema 3.2 - $\mathfrak{p} = \mathfrak{q}$ se e somente se $O(\mathfrak{p}) = O(\mathfrak{q})$. O anel $O(\mathfrak{p})$ é chamado anel dos inteiros de F em .

Notemos que $O(\mathfrak{p}) = F$ se e somente se $\mathfrak{p}$ é um lugar trivial em F e que $m(\mathfrak{p})$ é o único ideal maximal de $O(\mathfrak{p})$, o qual chamamos ideal maximal de F em $\mathfrak{p}$.

Claramente o conjunto $u(\mathfrak{P})$ é um subgrupo multiplicativo de $O(\mathfrak{P})$ e consiste precisamente de todos os elementos inversíveis de $O(\mathfrak{P})$. $u(\mathfrak{P})$ é chamado grupo das unidades de F em $\mathfrak{P}$.

Lema 3.3 - $\mathfrak{P} = \mathfrak{q}$ se e somente se $m(\mathfrak{P}) = m(\mathfrak{q})$.

Lema 3.4 - $m(\mathfrak{P}) = 0$ se e somente se $\mathfrak{P}$ é um lugar trivial.

Definição 3.5: O corpo de classe de residuos de F em $\mathfrak{P}$ é o conjunto $O(\mathfrak{P})/m(\mathfrak{P})$

CONJUNTO DE DEDEKIND

Seja $S \neq \phi$ um conjunto de lugar em um corpo F. S é chamado conjunto de Dedekind se:

1) Todo lugar de S é discreto.

2) Para cada α em F, temos $|\alpha|_{\mathfrak{P}} \leq 1$ para quase todo $\mathfrak{P} \in S$.

3) Quando $\mathfrak{q}$ e $\mathfrak{q}'$ são lugares distintos em S, então para cada $\varepsilon > 0$ e α em F temos

$$|\alpha - 1|_{\mathfrak{q}} < \varepsilon \quad e \quad |\alpha|_{\mathfrak{q}'} < \varepsilon, \quad |\alpha|_{\mathfrak{P}} \leq 1 \quad \text{para todo } \mathfrak{P} \in S - (\mathfrak{q} \cup \mathfrak{q}').$$

O anel de inteiros de F em S é definido como sendo $O(S) = \bigcap_{\mathfrak{P} \in S} O(\mathfrak{P})$ e

o subgrupo multiplicativo $u(S) = \bigcap_{\mathfrak{p} \in S} u(\mathfrak{p})$ de $O(S)$ que consiste exatamente dos elementos inversiveis de $O(S)$ será denominado grupo das unidades de F em S.

Exemplo 3.6 - O conjunto dos lugares não arquimedianos sobre os racionais é Dedekind.

TEOREMA DA APROXIMAÇÃO FORTE

Com o auxilio do terceiro axioma para conjuntos de Dedekind, podemos obter um novo teorema de aproximação que em certas situações importantes é mais forte que o teorema de aproximação apresentado no paragrafo anterior.

Teorema da Aproximação Forte - Seja T um subconjunto finito de um conjunto de Dedekind de lugares S em F. Para cada $\mathfrak{p} \in S$, consideremos um elemento $\alpha_{\mathfrak{p}}$ em F. Então, para cada $\varepsilon > 0$, existe $A \in F$ tal que

$$|A - \alpha_{\mathfrak{p}}|_{\mathfrak{p}} < \varepsilon \quad \text{para todo } \mathfrak{p} \in T$$

e

$$|A|_{\mathfrak{p}} \leq 1 \quad \text{para todo } \mathfrak{p} \in S-T .$$

Demonstração: Esta prova será dividida em três partes.

1) Pelo teorema da Aproximação Fraca podemos assumir que S é um conjunto infinito de lugares e que $|\alpha_{\mathfrak{p}}|_{\mathfrak{q}} \leq 1$ para todo $\mathfrak{p} \in T$ e todo $\mathfrak{q} \in S-T$.

Para isso podemos adicionar a T, se necessário, todos aqueles $\mathfrak{q} \in S-T$ em que $|\alpha_{\mathfrak{p}}|_{\mathfrak{q}} > 1$, para no mínimo um $\alpha_{\mathfrak{p}}$ e tomar $\alpha_{\mathfrak{q}} = 0$ para todo novo $\mathfrak{q}$. De acordo com o axioma 2 de Dedekind este novo conjunto T obtido ainda é finito. Então provando o resultado para esse novo T teremos provado para o T original. Do mesmo modo podemos assumir, acrescentando um lugar a T se necessário, que T consiste de pelo menos dois lugares.

2) Seja $\mathfrak{p}$ um lugar fixo em T. Para cada $\mathfrak{q}$ em $T-\mathfrak{p}$ podemos encontrar um elemento de $O(S)$ que está arbitrariamente perto de 1 em $\mathfrak{p}$ e de 0 em $\mathfrak{q}$. Procedendo analogamente para cada $\mathfrak{q}$ em $T-\mathfrak{p}$ e multiplicando os elementos obtidos, encontraremos do mesmo modo um elemento de $O(S)$ que está arbitrariamente perto de 1 em $\mathfrak{p}$ e de 0 em todo $\mathfrak{q}$ em $T-\mathfrak{p}$, isto pelo fato da multiplicação ser contínua na topologia p-ádica. O resultado obtido indicaremos por $A_{\mathfrak{p}}$ para cada $\mathfrak{p} \in T$.

3) Consideremos, então o elemento da forma $\sum_{\mathfrak{p} \in T} \alpha_{\mathfrak{p}} A_{\mathfrak{p}}$. Este elemento satisfaz

$$\left| \sum_{\mathfrak{p} \in T} \alpha_{\mathfrak{p}} \; A_{\mathfrak{p}} \right|_{\mathfrak{q}} \leq 1 \text{ para todo } \mathfrak{q} \in S-T$$

pela escolha de T e de $A_{\mathfrak{p}}$.

Pela continuidade da adição e multiplicação isto

pode ser feito arbitrariamente perto de α, simultaneamente em todo $\mathfrak{p}$ em T, pelas construções das aproximações $A_{\mathfrak{p}}$ da parte 2), o que é suficiente.

c.q.d.

Corolário 3.7 - Seja T um subconjunto finito de um conjunto de Dedekind S de lugares em F. Sejam $\varepsilon_{\mathfrak{p}} \in |F|_{\mathfrak{p}}$, para cada $\mathfrak{p} \in S$, tais que $\varepsilon_{\mathfrak{p}} = 1$, para quase todo $\mathfrak{p} \in S$. Então existe um $A \in F$ tal que $|A|_{\mathfrak{p}} = \varepsilon_{\mathfrak{p}}$, para todo $\mathfrak{p} \in T$ e $|A|_{\mathfrak{p}} \leq \varepsilon_{\mathfrak{p}}$ para todo $\mathfrak{p} \in S$.

Demonstração: Podemos assumir, aplicando T se necessário, que $\varepsilon_{\mathfrak{p}} = 1$ para todo $\mathfrak{p} \in S-T$.

Consideremos $\alpha_{\mathfrak{p}} \in F$, para cada $\mathfrak{p} \in T$, de tal maneira que $|\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = \varepsilon_{\mathfrak{p}}$.

Escolhendo A em F tal que

$$\begin{cases} |A - \alpha_{\mathfrak{p}}|_{\mathfrak{p}} < |\alpha_{\mathfrak{p}}|_{\mathfrak{p}} & \text{para todo } \mathfrak{p} \in T . \\ |A|_{\mathfrak{p}} \leq 1 & \text{para todo } \mathfrak{p} \in S-T . \end{cases}$$

obtemos o elemento desejado.

c.q.d.

§4. CORPOS LOCAIS E GLOBAIS

CORPOS RACIONAIS

Definição 4.1 - Seja F um corpo. O corpo primo K de F é o menor subcorpo de F.

Observação 4.2 - Sejam F um corpo e K seu corpo primo.

1) Se a característica de F é zero então K é o corpo dos racionais.

2) Se a característica de F é p primo então K é o corpo finito F_p, que consiste das classes de inteiros modulo p.

Definição 4.3 - Um corpo F é dito corpo de números algébricos se F fôr uma extensão finita dos racionais.

Definição 4.4 - Um corpo F é dito corpo de funções algébricos se F fôr uma extensão finita do corpo $F_p(x)$, onde x é transcendente sobre F_p.

A qualquer desses corpos F denominamos corpo global. E chamamos de corpo racional global a Q e a $F_p(x)$.

LUGAR P-ÁDICO EM Q

Cada primo p de Q determina um lugar chamado lugar p-ádico em Q.

É definido da sequinte maneira:

Todo $\alpha \in \dot{Q}$ pode ser escrito de maneira única na forma $\alpha = p^i \frac{u}{v}$ com $u, v \in z$ e tais que p não divide u e v. O expoente i será chamada ordem de α e será denotado por $ord_p\alpha$. Definiremos $ord_p 0 = \infty$

Definimos $|\alpha|_p = \lambda^i$ onde $\lambda \in \mathbb{R}$ e $0 \leq \lambda < 1$.

Proposição 4.5 - A valorização $|\ |_p$ assim definida é não arquimediana e independe da escolha de λ.

Demonstração: Pela definição de $|\alpha|_p = \lambda^i$ vemos claramente que ela é não arquimediana. Mostraremos que $|\ |_p$ independe da escolha de λ.

Seja $\alpha = p^i \frac{u}{v}$ um elemento qualquer de Q e consideremos $|\alpha|_p^1 = \lambda_1^i$ e $|\alpha|_p^2 = \lambda_2^i$.

Seja $r = \frac{\log \lambda_2}{\log \lambda_1}$. Desde que $(|\alpha|_p^1)^r = \lambda_1^{i \frac{\log \lambda_1}{\log \lambda_2}} = (\lambda_1 \frac{\log \lambda_2}{\log \lambda_1})^i = (\lambda_2)^i = |\alpha|_p^2$, concluimos que $|\ |_p^1$ e $|\ |_p^2$ são equivalentes.

c.q.d.

O CORPO DOS RACIONAIS P.ÁDICOS - Qp

Consideremos o corpo dos números racionais Q e um primo p em Q. O primo p determina um lugar p.ádico $\mathfrak{p}$ em Q.

Definimos o completado de Q em $\mathfrak{p}$ como o conjunto $Q_\mathfrak{p}$. O anel dos inteiros de $Q_\mathfrak{p}$ é chamado o anel dos inteiros p.ádicos e é escrito como $\mathbb{Z}_p$.

Proposição 4.6 - Q é denso em Qp .

Demonstração: É evidente usando a definição de Qp.

c.q.d.

Proposição 4.7 - Qp é completo.

Demonstração: Como Qp é o completado de Q, então segue, por um resultado elementar para espaços métricos completados, que o completado é completo.

c.q.d.

Proposição 4.8 - Toda série da forma $\sum_{\ell=-m}^{\infty} a_\ell \, p^\ell$ converge onde a_ℓ pertence ao conjunto $\{0,1,\ldots,p-1\}$.

Demonstração:

Consideremos as somas parceais $B_i = \sum_{\ell=-m}^{i} a_\ell \, p^\ell$

Se $m \geq n$

$$|Bm - Bn|_p \quad \Big|\sum_{\ell=n+1}^{m} a_\ell \, p^\ell\Big|_p \leq \max(|a_{n+1}p^{n+1}|+\ldots+|a_m p^m|)$$

e, consequentemente, $|Bm - Bn|_p \leq (\frac{1}{p})^m$.

Portanto $\{B_m\}$ é uma sequência de Cauchy em Qp e, pela proposição anterior, $\sum_{\ell=-m}^{\infty} a_\ell \, p^\ell$, com a_ℓ pertencente ao conjunto $\{0,\ldots,p-1\}$, converge.

c.q.d.

Proposição 4.9 - Todo elemento em Qp é da forma

$$\alpha = \sum_{i=n}^{\infty} a_i\, p^i \quad \text{onde } a_i \in \{0,1,\ldots,p-1\} \text{ e } \operatorname{ord}_p \alpha = n.$$

Demonstração:

1) Podemos colocar $\alpha = \varepsilon p^n$ para algum ε em $u[p]$ onde $\operatorname{ord}_p \alpha = n$.

Sejam $C = \{0,\ldots,p-1\}$ e $a_n \in C$ tal que $\varepsilon \equiv a_n \bmod m[p]$. Então $\alpha = a_n p^n + \alpha'$ com $\operatorname{ord}_p \alpha' > n$. Analogamente aplicamos o mesmo processo para α' para obtermos α'' e assim por diante. Depois de (m+1) transformações, obtemos

$$\alpha = a_n p^n + \ldots + a_{n+m} p^{n+m} + \alpha^{(m+1)} \text{ com } \operatorname{ord}_p \alpha^{m+1} > n+m$$

e considerando a_n , a_{n+1} , ... , a_{n+m} em C. As somas parciais $\sum_{\ell=n}^{m+n} a_\ell\, p^\ell$ convergem para α, e portanto $\alpha = \sum_{\ell=n}^{\infty} a_\ell\, p^\ell$.

2) Para mostrar a unicidade vamos supor que existam duas expressões tais que $\alpha = \sum_{i=n}^{\infty} c_i\, p^i = \sum_{i=n}^{\infty} d_i\, p^i$ com $c_i, d_i \in \{0,1,\ldots p-1\}$.

Seja k o primeiro inteiro tal que $c_k \neq d_k$, ou seja $c_i = d_i$ para $n \leq i < k$. Multiplicando a equação $\sum_{i=k}^{\infty} c_i\, p^i = \sum_{i=k}^{\infty} d_i\, p^i$ por p^{-k} obtemos $ck + \sum_{i=k+1}^{\infty} c_i\, p^i = d_k + \sum_{i=k+1}^{\infty} d_i\, p^i$. Portanto dessa forma $c_k \equiv d_k \bmod p$. E desde que c_k e d_k estão na mesma classe

residual então $c_k = d_k$ o que é absurdo.

c.q.d.

O ANEL DOS INTEIROS P.ÁDICOS Z_p

Observemos primeiro que o anel dos inteiros Z_p coincide com o conjunto das séries $\sum_{i=n}^{\infty} a_i p^i$ onde $n \geq 0$.

Proposição 4.10 - Z_p é aberto e compacto.

Demonstração: Na topologia dado por $|p^i \frac{u}{v}|_p = \lambda^i$ com $0<\lambda<1$, Z_p é claramente um aberto. Mostraremos que Z_p é um compacto.

Consideremos a aplicação ϕ: $Z_p \to \prod_{n=0}^{\infty} X_n$, onde $X_n = Z/_{pZ}$, dada por $\Phi(\sum_{i=n}^{\infty} a_i p^i) = (a_1 , a_2,\ldots,a_n ,\ldots)$.

Claramente Φ é contínua e bijetora. Portanto $Z_p \cong \prod_{n=0}^{\infty} X_n$ e, como cada X_n é compacto, então Z_p é compacto.

c.q.d.

Proposição 4.11 - Z_p é completo.

Demonstração: Segue-se do fato de que Z_p é compacto.

CORPOS LOCAIS

Um corpo local é um conjunto consistindo de um lugar $\mathfrak{p}$ e um corpo F tais que

1) $\mathfrak{p}$ é completo e discreto.
2) A classe residual em $\mathfrak{p}$ é finita.

Exemplo 4.12 - Qp é corpo local

CAPÍTULO II

O GRUPO ORTOGONAL E SUA GERAÇÃO

O propósito neste capítulo é de introduzir uma forma quadrática e uma geometria ortogonal em um espaço de dimensão finita e estudar certos grupos de transformações lineares ; mais especificamente o grupo Ortogonal, seus principais subgrupos e também sua geração. Em todo este capítulo F denotará um corpo de característica diferente de 2.

§1. ESPAÇOS QUADRÁTICOS E FORMAS QUADRÁTICAS

Seja V um espaço vetorial sobre F. Uma forma bilinear simétrica $B: V \times V \to F$ é uma aplicação que verifica as seguintes propriedades:

(i) $B(x,y+z) = B(x,y) + B(x,z)$

(ii) $B(\alpha x,y) = \alpha B(x,y)$

(iii) $B(x,y) = B(y,x)$ para todo x, y e z $\in$ V e $\alpha \in$ F.

A aplicação $g: V \to F$ definida por $q(x) = B(x,x)$ é chamada uma forma quadrática.

Para q são válidas

(i) $q(\alpha x) = \alpha^2 q(x)$

(ii) $q(x+y) = q(x) + q(y) + 2\,B(x,y)$

(iii) $q(\sum_{i=1}^{m} \alpha_i x_i) = \sum_{i=1}^{m} q(x_i) + 2\alpha \sum_{i<j} \alpha_i \alpha_j\, B(x_i,x_j)$

Se $q(V) = F$ então V será chamado universal.

ESPAÇO QUADRÁTICO

Definição 1.1 - Um espaço quadrático é um espaço vetorial V sobre F, de dimensão finita, munido de uma forma bilinear simétrica B e uma forma quadrática q.

MATRIZ DE UM ESPAÇO QUADRÁTICO

Seja $\{x_1,\ldots x_n\}$ uma base do espaço quadrático V. Então $N = (B(x_i,x_j))$ é chamada a matriz do espaço quadrático V, em relação a base dada.

Se $\{x_1',\ldots,x_n'\}$ é uma outra base de V e $N' = (B(x_i',x_j'))$ então $N' = T^tNT$, onde T é matriz transformação de base.

DISCRIMINANTE

Definição 1.2 - O discriminante dos vetores $\{z_1,\ldots z_m\}$ é o determinante da matriz $(B(z_i,z_j))$, que denotamos por $d_B(z_1,\ldots z_m)$.

Em particular se N é a matriz de V em relação à base $\{x_1,\ldots,x_n\}$ então $d_B(x_1,\ldots x_n) = \det N$.

Em relação a uma outra base $\{x_1',\ldots x_n'\}$, desde que

$N' = T^t N T$, temos $d_B(x_1', \ldots x_n') = \alpha^2 d_B(x_1, \ldots x_n)$ onde $\alpha = \det T = \det T^t$. Logo a imagem canonica dV de $d_B(x_1, \ldots x_n)$ em $\{0\} \cup (\dot{F}/\dot{F}^2)$ independe da base e será chamada discriminante do espaço V.

DECOMPOSIÇÃO ORTOGONAL

Definição 1.3 - Sejam V um espaço quadrático e B e q as formas bilinear e quadrática associada. Dois subespaços U e W de V são ortogonais se $B(V,W) = 0$.

Dizemos que V tem decomposição ortogoanl em subespaços $V_1, \ldots, V_r$ e indicamos $V = V_1 \perp \ldots \perp V_r$, se

(i) $V = V_1 \oplus \ldots \oplus V_r$,

(ii) $B(V_i, V_j) = 0 \quad 1 \leq i < j \leq r$

Um subespaço U de V é componente ortogonal de V se existe um subespaço W de V tal que $V = U \perp W$.

Lema 1.3 - Todo espaço quadrático não-nulo tem uma base ortogonal.

Demonstração: Se $q(V) = 0$, então qualquer base de V é ortogonal. Caso contrário, seja $x \in V$ com $q(x) \neq 0$. Consideremos uma base $\{x, x_2, \ldots, x_n\}$ para V. Então $\{x, x_2 - \frac{B(x,x_2)}{q(x)} x, \ldots x_n - \frac{B(x,x_n)}{q(x)} x\}$ é ainda uma base para V e as últimos (n-1) vetores geram um subespaço W onde $B(x,W) = 0$. Assim, aplicando indução sobre a dimen

são de V, obtemos o resultado desejado.

COMPLEMENTO ORTOGONAL E RADICAL

Seja U subespaço do espaço quadrático V. O conjunto $U^* = \{x \in V \mid B(x,y) = 0 \text{ para todo } y \in U\}$ é um subespaço de V chamado complemento ortogonal de U em V.

O conjunto rad U = $\{x \in U \mid B(x,y) = 0$, para todo $y \in U\}$ é um subespaço de U chamado radical de U. Observemos que rad $V = V^*$.

Definição 1.5 - Um subespaço U de um espaço quadrático V é regular se rad U = 0.

Proposição 1.6 - Seja V um espaço quadrático e $V = V_1 + \ldots + V_r$, com $B(V_i, V_j) = 0$ para $1 \leq i < j \leq r$.

1) rad $V = \text{rad } V_1 + \ldots + \text{rad } V_r$.

2) V é regular se e somente se cada V_i é regular.

3) Se V é regular então $V = V_1 \perp \ldots \perp V_r$.

Demonstração: Em (1) consideremos $x \in \text{rad } V$ e escrevemos $x = \sum x_\lambda$ com cada $x_\lambda \in V_\lambda$. Para cada i ($1 \leq i \leq r$) temos $B(x_i, V_i) = B(\sum x_\lambda, V_i) \subseteq B(x, V) = 0$, o que mostra que, $x_i \in \text{rad } V_i$ e, consequentemente, $x \in \sum \text{rad } V_i$.

Reciprocamente, considereando $x = \sum x_\lambda$, com cada

$x_\lambda \in \text{rad } V_\lambda$, temos $B(x,V) \subseteq B(x_1,V_1)+\ldots+B(x_r , V_r) = 0$ o que significa que $x \in \text{rad } V$.

A parte (2) é uma consequência imediata da definição de espaço quadrático regular e da parte (1).

Para a demonstração de (3) é somente necessário mostrar que a soma $V_1 +\ldots+ V_r$ é direta. Assim, seja $0 = x_1+\ldots+x_r$, com $x_i \in V_i$, $1 \leq i \leq r$. Então $0 = B(x_1 +\ldots+ x_r , V_i) = B(x_i, V_i)$ e, portanto, $x_i \in \text{rad } V_i = 0$.

c.q.d.

Proposição 1.7 - Um espaço quadrático V é regular se e somente se $d_B V \neq 0$.

Demonstração: Consideremos uma base ortogonal $\{x_1,\ldots x_n\}$ de V.

Então, $V = Fx_1 \perp\ldots\perp Fx_n$. Pela proposição anterior, V é regular se e somente se cada Fx_i é regular. Porem Fx_i é regular se e somente se $q(x_i) \neq 0$. Logo V é regular se e somente se $q(x_1)\ldots q(x_n) \neq 0$; isto é, se e somente se $d_B(x_1\ldots x_n) \neq 0$.

c.q.d.

Proposição 1.8 - Seja U um subespaço regular do espaço quadrático V. Então U é componente ortogonal de V e se $V = U \perp W$ então $W = U^*$.

Demonstração: Seja $\{x_1,\ldots,x_p\}$ uma base ortogonal para U, $U = Fx_1 \perp \ldots \perp Fx_p$.

Um elemento z em V pode ser escrito como $z = y+w$ com $y = \frac{B(z,x_1)}{q(x_1)}\, x_1 + \ldots + \frac{B(z,x_p)}{q(x_p)}\, x_p$ onde cada $q(x_i) \neq 0$ pois U é regular.

Claramente, y ∈ U e desde que $B(w,x_i) = 0$ para $1 \leq i \leq p$, $w \in U^*$. Isto mostra que $V = U + U^*$.

Agora $U \cap U^* = \text{rad } U = 0$. Assim, $V = U \oplus U^*$ e portanto $V = U \perp U^*$. Se $V = U \perp W$, então $W \subseteq U^*$. Mas, como provamos que $V = U \perp U^*$, então dim W = dim U^* . Dessa maneira $W = U^*$.

c.q.d.

DECOMPOSIÇÃO RADICAL

Consideremos o rad V de um espaço quadrático V e U um subespaço de V para qual $V = U \oplus \text{rad } V$. Então segue-se que $V = U \perp \text{rad } V$ e chamamos isto de decomposição radical de V.

ISOTROPIA

Seja $x \neq 0$ em um espaço quadrático V. Dizemos que x é isotrópico se $q(x) \neq 0$ e anisotrópico caso contrário. V é isotrópico se contém um vetor isotrópico e anisotrópico se todo vetor não nulo é anisotrópico. V é totalmente isotrópico se $V \neq 0$

e $q(V) = 0$.

PLANO HIPERBÓLICO

Um espaço quadrático V é chamado plano hiperbólico, se a matriz de V, em relação a alguma base de V, é $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Assim todos os planos hiperbólicos são regulares com discriminante -1 .

Observação 1.9 - Seja V um plano hiperbólico escrito como $V = Fx + Fy$ com $q(x) = q(y) = 0$. Então as retas Fx e Fy são as únicas retas isotrópicas de V_i ; isto claramente é verificado pela equação $q(\alpha x + \beta y) = 2\alpha\beta\ B(x.y)$. Esta equação também mostra que $q(V) = F$, ou seja que todo plano hiperbólico é universal.

Proposição 1.10 - Seja V um espaço quadrático 2-dimensional. As seguintes afirmações são equivalentes.

1) V é plano hiperbólico

2) V é isotrópico e regular

3) $dV = -1$.

Demonstração: (1) implica (2)

Se V é um plano hiperbólico então a matriz de V em relação a alguma base $\{x_1 , x_2\}$ é $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Logo $q(x_i) = 0$ e, portanto, V é isotrópico.

V é regular, pois se $x = \alpha x_1 + \beta x_2$ é rad V, então $B(x,x_1+x_2) = 0$ e $B(x,x_1-x_2) = 0$, de onde segue-se que $\alpha + \beta = 0$ e $\alpha - \beta = 0$, ou seja $\alpha = 0 = \beta$ e, consequentemente, $x = 0$.

( ) (2) implica (3) - Seja x vetor isotrópico em V, e $\{x,y\}$ uma base para V; então a matriz de V tem a forma $\begin{pmatrix} 0 & \beta \\ B & \gamma \end{pmatrix}$ onde $B(x,y) = \beta$ e $B(y,y) = \gamma$. Assim, $dV = -\beta^2$. Porém, V é regular, $\beta \in \dot{F}$ e, desde que $-\beta^2$ e -1 são iguais em $\dot{F}/\dot{F}^2$, temos $dV = -1$.

(3) implica (1). Se V é regular então temos que $q(V) \neq 0$. Sejam $\alpha \neq 0$ e $x \in V$ tal que $q(x) = \alpha$. Desde que V é regular Fx é componente ortogonal de V. Logo $V = Fx \perp Fy$ para algum $y \in V$. Como por hipótese $dV = -1$, temos que $q(x).\ q(y) \neq 0$. Assim, podemos assumir que $q(y) = -\alpha$ e $V = F\left(\frac{x+y}{2}\right) + F\left(\frac{x-y}{\alpha}\right)$

A matriz de V nessa base é facilmente escrita como $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Portanto, V é plano hiperbólico.

c.q.d.

Proposição 1.11 - Sejam V espaço quadrático regular, U subespaço de V com $q(U) = 0$ e $\{x_1,\ldots,x_r\}$ uma base para U. Então existe um subespaço $H_1 \perp \ldots \perp H_r$ de V, onde cada H_i é um plano hiperbólico com $x_i \in H_i$.

Demonstração: (Por indução sobre r)

Se $r = 1$, seja $y_1 \in V$ com $B(x_1,y_1) \neq 0$ e colocamos $H_1 = Fx_1 + Fy_1$. Então H_1 é um plano hiperbólico com a propriedade de pedida.

Para $r > 1$, colocamos $U_{r-1} = Fx_1 + \ldots + Fx_{r-1}$ e $U_r = U$. Então $U_{r-1} \subset U_r$ e, assim, $U_r^* \subset U_{r-1}^*$. Consideremos $y_r \in U_{r-1}^* - U_r^*$ e coloquemos $H_r = Fx_r + Fy_r$. Então $B(x_i,y_r) = 0$ para $1 \leq i \leq r-1$ e $B(x_r,y_r) \neq 0$. Assim, H_r é um plano hiperbólico contendo x_r. Como $x_r \in U_{r-1}^*$ e $y_r \in U_{r-1}^*$ então $H_r \subseteq U_r^*$ e, por conseguinte, $U_{r-1} \subseteq H_r^*$. Desde que V é regular e $V = H_r \perp H_r^*$, então H_r^* é regular e, aplicando a hipótese de indução a U_{r-1} tomado como um subespaço de H_r^*, obtemos $H_1 \perp \ldots\ldots \perp H_{r-1} \subseteq H_r^*$ com $x_i \in H_i$ para $1 \leq i \leq r-1$. Portanto, $H_1 \perp \ldots \perp H_{r-1} \perp H_r$ satisfaz as condições exigidas.

c.q.d.

§2. GRUPO ORTOGONAL

REPRESENTAÇÕES E SIMETRIAS

Definição 2.1 - Sejam V e W espaços quadráticos e q e q' as respectivas formas quadráticas. Uma transformação linear $\sigma: V \to W$ é uma representação de V em W, se $q'(\sigma x) = q(x)$, para todo $x \in V$.

Definição 2.2 - Uma isometria de V em W é uma representação de V em W injetiva. Os espaços V e W serão chamados isométricos se existir uma isometria de V em W.

O conjunto de todas as isometrias de V em W será denotado por $O_n(V,V)$.

Se V = W então σ é inversível e isso mostra que $O_n(V,V)$ é um subgrupo do grupo $GL_n(V)$ das transformações lineares inversiveis de V em V. O grupo $O_n(V,V)$ é chamado grupo ortogonal de V, em relação a q e será indicado simplesmente por $O_n(V)$.

INVOLUÇÕES E SIMETRIAS

Definição 2.3 - Seja V um espaço quadrático. Uma aplicação σ: V→V é uma involução se $\sigma^2 = 1_V$, onde 1_V denota a aplicação identidade em V.

As mais importantes das involuções são as simetrias ; isto é, são as aplicações τ_y: V→ V dadas por

$$\tau_y(x) = x - \frac{2B(x,y)}{q(y)}\, y \text{ , onde } y \in V \text{ é tal que } q(y) \neq 0.$$

Como consequência imediata da definição de τ_y temos as seguintes afirmações:

— τ_y é linear

— τ_y é involução

— τ_y é uma representação injetiva e, portanto $\tau_y \in O_n(V)$.

— $\tau_y(x) = x$ para todo $x \in (Fy)^*$ e $\tau_y(x) = -x$ para todo $x \in Fy$.

Proposição 2.4 - Sejam U e W subespaços isométricos regulares de um espaço quadrático V. Então U^* e W^* são isométricos.

Demonstração: 1) Vamos supor inicialmente que U e W são retas, ou seja $U = Fx$ e $W = Fy$, com $q(x) = q(y) \neq 0$. Então $q(x+y) + q(x-y) = 2q(x) + =q(y) = 4q(x)$ e, por conseguinte $q(x+y)$ ou $q(x-y)$ é não nulo. Trocando y por -y se necessário, podemos assumir que $q(x-y) \neq 0$ e consideremos a simetria τ_{x-y}. Assim temos, $\tau_{y-x}\, x = x - \frac{2B(x,x-y)}{q(x-y)}(x-y)$ e, desde que

$$\begin{aligned} q(x-y) &= q(x) + q(y) - 2B(x,y) \\ &= q(x) - 2B(x,y) \\ &= 2B(x,x-y) , \end{aligned}$$

então $\tau_{y-x}\, x = y$. Portanto $\tau_{x-y}\, U^* = W^*$ o que significa que U^* e W^* são isométricos.

2) No caso geral, usaremos indução sobre a dim U. Desde que U e W são isométricos, podemos considerar as decomposições não triviais $U = U_1 \perp U_2$ e $W = W_1 \perp W_2$, com $U_1 \cong W_1$ e

$U_2 \cong W_2$. Então pela hipótese de indução, temos que $U_2 \perp U^*$ é isométrico a $W_2 \perp W^*$ e, portanto, existe uma decomposição $U_2 \perp U^* = X \perp Y$ com $X \cong W_2$ e $Y \cong W^*$. Mas então $X \cong W_2 \cong U_2$ e a hipótese de indução garante que $Y \cong U^*$. Logo $W^* \cong U^*$.

c.q.d.

TEOREMA DE WITT

Sejam V e V' espaços quadráticos regulares isométricos, U um subespaço de V, e σ uma isometria de U em V'. Então existe um prolongamento de σ a uma isometria de V sobre V'.

Demonstração: Escrevemos $U = W \perp \text{rad } U$ e seja $\{x_1,\ldots,x_r\}$ uma base para rad U. Pela proposição 1.11 deste capítulo existe um subespaço $H = H_1 \perp \ldots \perp H_r$ do espaço W^* na qual cada H_i é plano hiperbólico, tal que $x_i \in H_i$. Desde que H é regular, H decompõe W^* e portanto existe um subespaço S de W^* tal que $V = H \perp S \perp W$.

Sejam $U' = \sigma U$, $W' = \sigma W$ e $x_i' = \sigma x_i$,para $1 \leq i \leq r$. Assim, $\text{rad } U' = \sigma(\text{rad } U) = Fx_1' + \ldots + Fx_r'$ e $U' = W \perp \text{rad } U'$. Repetindo o processo de construção obtemos $V' = H' \perp S' \perp W'$ com $H' = H_1' \perp \ldots \perp H_r'$ onde cada H_i' é um plano hiperbólico contendo x_i' .

Agora, existe claramente uma isometria de H sobre H' que coincide com σ em cada x_i e, consequentemente em rad U. Verificamos também que σ leva W em W'. Logo, existe um prolongamento de σ a uma isometria σ' de $H \perp W$ sobre $H' \perp W'$. Aplicando a proposição anterior, vemos que S é isométrico a S'. Portanto, existe um prolongamento de σ para uma isometria de V sobre V'.

c.q.d.

§3. GERAÇÃO DO GRUPO ORTOGONAL

Se V é um espaço quadrático regular, mostraremos que as simetrias geram $O_n(V)$ e faremos um estudo sobre certos subgrupos de $O_n(V)$ tais como O_n^+, Ω_n e Z_n.

Proposição 3.1 - Se $\sigma \in O_n(V)$ então $\det\sigma = \pm 1$.

Demonstração: Sejam $\{x_1,\ldots,x_n\}$ uma base para V e M a matriz de V em relação a base dada.

Seja σ uma isometria de V e $T = (t_{ij})$ a matriz de na base dada, isto é, $\sigma x_j = \sum t_{ij}\, x_i$. Logo $\{\sigma x_1,\ldots\sigma x_n\}$ é uma base de V é a matriz associada a V nesta base também é M, desde que σ é uma isometria. Assim, $M = T^t MT$ e $\det M = \det T^t$, $\det M$, $\det T$, de onde segue-se que $(\det T)^2 = 1$, ou $\det\sigma = \pm 1$.

c.q.d.

Definição 3.2 - σ é uma rotação se $\det\sigma = +1$.

Definição 3.3 - σ é uma reflexão se $\det\sigma = -1$

Sejam $O_n^+ = \{\sigma / \sigma \text{ é rotação, } \det\sigma = +1\}$ e

$O_n^- = \{\sigma / \sigma \text{ é reflexão, } \det\sigma = -1\}$

Proposição 3.4 - O_n^+ é subgrupo normal de $O_n(V)$.

Demonstração: Dados σ_1 e σ_2 e $O_n^+(V)$ então σ_1 e σ_2^{-1} e $O_n^+(V)$ pois $\det\sigma.\sigma_2^{-1} = \det\sigma_1.\det\sigma_2^{-1} = 1$. Assim $O_n^+(V)$ é subgrupo de $O_n(V)$. Se σ e $O_n^+(V)$ e $\bar{\sigma}$ e $O_n(V)$ então $\bar{\sigma}^{-1}\sigma\bar{\sigma}$ e $O_n^+(V)$ pois $\det\bar{\sigma} = \det\bar{\sigma}^{-1} = \pm 1$. Portanto, O_n^+ é subgrupo normal de $O_n(V)$.

c.q.d.

Observação 3.4a - O_n^- não é subgrupo de O_n . Isto é devido ao fato de que dados σ_1, σ_2 e O_n^- , $\sigma_1.\sigma_2 \notin O_n^-$, pois $\det\sigma_1\sigma_2 = 1$.

Proposição 3.5 - Se V é um plano hiperbólico e σ uma isome-tria de V em V a qual é identidade em um subespaço totalmente isotrópico maximal de V, então σ é uma rotação.

Demonstração: Seja M o subespaço totalmente isotrópico maximal de V, tal que dim M = r . Então 2r é a dimensão de V. Pela proposição 1.11 deste capítulo, existe um outro subespaço N de V totalmente isotrópico maximal tal que $V = M \oplus N$. Para $x \in M$ e $y \in N$ temos: $\sigma x = x$ e $B(x,\sigma y - y) = 0$. Assim, $\sigma y - y \in M^*$. Mas como $M \subseteq M^*$

comparando as dimensões, vemos que $M=M^*$. Logo $\sigma y - y \in M$ para todo $y \in N$.

Agora, se $\{x_1,\ldots,x_r\}$ é uma base de M e $\{y_1,\ldots,y_r\}$ é uma base para N então $\{x_1,\ldots,x_r, y_1,\ldots,y_r\}$ é uma base para V e, usando o fato de que $\sigma(x_i) = x_i$ para todo $x_i \in M$ para todo $y_i \in N$, teremos $\det \sigma = 1$. Portanto, σ é uma rotação.

c.q.d.

Proposição 3.6 - Seja U um hiperplano de um espaço quadrático regular V e seja σ uma isometria de U em V. Se U é regular, existem dois prolongamentos de σ a V que diferem por uma simetria. Se U é não regular, existe um único prolongamento de σ a V.

Demonstração: 1) Primeiramente vamos supor o caso onde U é um hiperplano regular. Pelo teorema de Witt existe um prolongamento σ_1 de σ a V. Seja σ_2 um elemento de O_n. Então σ_2 é um prolongamento de σ se e somente se $\sigma_2^{-1}\sigma_1$ é identidade em U. Isto significa que σ_1 e $\sigma_1 \zeta_y$ são os únicos prolongamentos de σ, onde Fy é uma reta ortogonal ao hiperplano U.

2) Agora vamos supor que U não seja regular. Sabemos que existe pelo menos um prolongamento de σ a V. Se existisse um outro, teríamos um ρ em O_n, o qual é identidade em U, mas

não em V. Vamos mostrar que isso é impossível. Desde que U é um hiperplano, U^* é uma reta. Logo rad U = $U \cap V^*$ é uma reta F_x. Por isso, uma decomposição radical de U conduz a uma decomposição $V = W \perp (F_x + F_y)$, com $q(x) = Q(y)$, e $W \subseteq U$.

Agora, ρ deixa W fixo e, portanto, deixa também $F_x + F_y$ fixo. Desde que $\rho x = x$ então $\rho y = \alpha y$ para algum escalar α. Mas $B(x\ y) = B(\rho x, \rho y) = B(x, \alpha y) = \alpha\ B(x,y)$ e isso mostra que ρ é a identidade em U é tambem a identidade em V. Assim σ tem exatamente um prolongamento.

c.q.d.

GERAÇÃO DE O_n POR SIMETRIAS

Para a demonstração do teorema da geração de O_n por simetrias será necessário antes o seguinte resultado:

Lema 3.7 - Seja V um espaço quadrático regular. Se $\sigma \neq 1_V$ é uma isometria em V satisfazendo a condição (*). "Se x é anisotrópico em V então $\sigma x - x \neq 0$ e $q(\sigma x - x) = 0$", então $n \geq 4$, n é par e σ é uma rotação.

Demonstração: É evidente que não podemos ter n = 1. Se n = 2 e x é anisotrópico, usando a condição (*), concluiremos que x e σx são linearmente independentes e $d(x, \sigma x) = 0$. Essas condições

contrariam o fato de V ser regular. Assim devemos ter $n \geq 3$. Finalmente será mostrado que n é par e que σ é uma rotação. Para esta demonstração ainda necessitaremos mostrar que a condição (*) também é satisfeita para elementos isotrópicos de V, ou seja $q(\sigma x - x) = 0$ para todo $x \in V$. Para isso, consideremos y um elemento isotrópico em V. Então existe um plano hiperbólico H que contem y e decompõe V, isto é, $V = H \perp H_1$. Logo existe z em V, tal que $q(z) \neq 0$ e $B(y,z) = 0$. Portanto, $q(y+\varepsilon z) \neq 0$ para todo $\varepsilon \in \dot{F}$ e, consequentemente, $q(\sigma y - y) + 2\varepsilon B(\sigma y - y, \sigma z - z) = q(\sigma(y+\varepsilon z) - (y+\varepsilon z)) - \varepsilon^2 q(\sigma z - z) = 0$. Em particular tomando $\varepsilon = \pm 1$, encontraremos o resultado desejado, ou seja $q(\sigma y - y) = 0$, como y é isotrópico. Logo, o espaço $W = (\sigma - 1)V$ satisfaz $q(W) = 0$ e, se considerarmos x em V e y em W^*, teremos $B(x, \sigma y - y) = 0$. Portanto, $\sigma y - y \in \text{rad } V = 0$ de onde segue-se que $\sigma y = y$, para todo $y \in W^*$. Aplicando a condição (*) obtemos $q(W^*) = 0$. Assim, $W \subseteq W^* \subseteq (W^*)^* = W$. Portanto n é par e $\dim W = \frac{n}{2}$; em outras palavras, V é um espaço hiperbólico e W é um subespaço totalmente isotrópico maximal. Mas, como σ é uma identidade em $W = W^*$, concluimos pela proposição 3.5 que σ é uma rotação.

c.q.d.

Teorema 3.8 - Toda isometria σ de um espaço quadrático regular n-dimensional em si mesmo é um produto de no máximo n simetrias.

Demonstração: 1) (Por indução sobre n)

Para n = 1 é trivial.

Para n > 1. Vamos supor que existe um vetor anisotrópico x com $\sigma x = x$. Então a restrição $\sigma|_U$ de σ a um hiperplano U ortogonal a Fx é um elemento de $O_{n-1}(U)$. Usando a hipótese de indução, σ é um produto de no máximo (n-1) simetrias em relação à retas em U. Cada uma dessas simetrias tem um prolongamento natural a V por meio de uma simetria considerada em relação à reta original em U. O produto desses prolongamentos colocados na ordem original coincidem com σ em U e também em Fx , onde $\hat{0}$ e o produto são identidades. Logo eles coincidem em V. Portanto, σ é um produto de no máximo (n-1) simetrias quando σ deixa um vetor anisotrópico fixo.

A próxima suposição é que existe x anisotrópico com $q(\sigma x - x) \neq 0$. Consideremos a simetria $\tau_{\sigma x - x}$ definida em V. Vemos que $\tau_{\sigma x - x}\sigma$ deixa x fixo. Logo, pelo caso anterior, $\tau_{\sigma x - x}\sigma$ é o produto de no máximo (n-1) simetrias, portanto σ é o produto de no máximo n simetrias. Então provamos, nesses dois, que qualquer

simetria que não satisfaz a condição (x) "Se x é anisotrópico em $\dot{V}$, então $\sigma x - x$ é isotrópico em $\dot{V}$" , satisfaz o teorema.

Finalmente, consideremos σ em V qua satisfaz a condição (*), Então, pelo lema 3.7 σ é rotação e n é par. Seja τ simetria de V. Desde que $\tau\sigma$ é uma reflexão, então $\tau\sigma$ não satisfaz a condição (*) e, por conseguinte, $\tau\sigma$ é um produto de no máximo n simetrias. Logo, σ é um produto de no máximo n+1 simetrias. No entanto, σ é uma rotação e n+1 é ímpar, de onde concluimos que σ só pode ser um produto de no máximo n simetrias.

Definição 3.9 - Seja σ uma isometria de V. O conjunto $\{x \in V \mid \sigma x = x\}$ é um subespaço de V chamado espaço fixo de σ.

Corolário 3.10 - Se σ é um produto de n simetrias, então a dimensão de seu espaço fixo é no mínimo n-r.

Demonstração: Pelo teorema 3.8, $\sigma = \tau_1 \ldots \tau_r$ onde cada τ_i é uma simetria. Sejam U_i o espaço fixo de τ_i , para $1 \leq i \leq r$ e U o espaço fixo de σ. Então $U_1 \cap \ldots \cap U_r \subset U$ pois se $x \in U_1 \cap \ldots \cap U_r$ então $\tau_1(x) = \ldots = \tau_r(x)$ e, consequentemente, $\sigma(x) = \tau(x) \ldots \ldots \tau_r(x) = x$. Isto é suficiente para mostrar que cada U_i é um hiperplano de V e então $\dim (U_1 \cap \ldots \cap U_r) \geq n-r$. Esta última afirmação é demonstrada por indução sobre r.

Para $r = 1$, desde que U_1 é um hiperplano, temos dim $U_1 = n-1$.

Para $r > 1$,

$$\dim (U_1 \cap \ldots \cap U_r) = \dim(U_1 \cap \ldots \cap U_{r-1}) + \dim U_r - \dim((U_1 \cap \ldots \cap U_{r-1}) + U_r)$$

$$\geq (n-r+1) + (n-1) - (n) = n-r.$$

c.q.d

Corolário 3.11 - Suponhamos que σ seja um produto de n simetrias. Então ela ppde ser expressa como um produto de n simetrias, com a primeira ou a última escolhida arbitrariamente.

Demonstração: Escrevemos σ como um produto de n simetrias , ou seja $\sigma = \tau_1 \ldots \tau_n$. Se τ é uma simetria qualquer então pode-mos expressar $\tau\sigma$ como um produto de no máximo n simetrias. Logo $\sigma = \tau \cdot \tau_2' \ldots \tau_r'$ com $r \leq n+1$. Então $\det \sigma = (-1)^r$. Mas, por hipotese, $\det \sigma = (-1)^n$. Concluimos, então, que r e n tem a mesma paridade. Em particular $r \leq n$. Se $r < n$, colocamos um número par de simetrias iguais a τ no final e obtemos $\sigma = \tau\tau_2' \ldots \tau_r'$. Isto permite-nos escolher a primeira simetria de uma maneira arbitrária e, analogamente, a última.

c.q.d.

§4. ALGUNS SUBGRUPOS DE $O_n(V)$

Alem de O_n^+ , podemos considerar os subgrupos Ω_n e Z_n de $O_n(V)$.

O SUBGRUPO COMUTADOR Ω_n DE O_n

Denotaremos por Ω_n o subgrupo comutador de O_n . Claramente $\Omega_n \subset O_n^+$. Os subgrupos O_n^+ , Ω_n são definidos somente para espaços regulares não nulos.

Proposição 4.1 - Ω_n contem os quadrados de todos os elementos de O_n e é gerado pelos comutadores da forma $\tau_x\tau_y\tau_x\tau_y = \tau_x\tau_y\tau_x^{-1}\tau_y^{-1}$ onde τ_x e τ_y são simetrias. Em particular Ω_n é gerado pelos quadrados dos elementos de O_n^+ .

Demonstração: Seja G subgrupo de O_n gerado pelos comutadores do tipo $\tau_x\tau_y\tau_x\tau_y$. Para qualquer $\sigma \in O_n$, temos $\sigma\,\tau_x\,\sigma^{-1} = \tau_{\sigma x}$ e, então

$$\sigma(\tau_x\tau_y\tau_x\tau_y)\sigma^{-1} = \tau_{\sigma x}\tau_{\sigma y}\tau_{\sigma x}\tau_{\sigma y}$$ o que mostra que G é um subgrupo normal de O_n .

Consideremos $O_n/G = \{\overline{\tau}_x = \tau_x + G\}$. Para quaisquer simetrias τ_x , τ_y temos $\overline{\tau}_x.\overline{\tau}_y.\overline{\tau}_x.\overline{\tau}_y = \overline{1}$ ou $\overline{\tau}_x.\overline{\tau}_y = \overline{\tau}_y.\overline{\tau}_x$, o que significa que O_n/G é comutativo. Então $\Omega_n \subseteq G$. Mas $G \subset \Omega_n$ por definição e, portanto, $G = \Omega_n$.

Finalmente, de

$$\bar{\sigma}^2 = \bar{\tau}_1 \ldots \bar{\tau}_m \cdot \bar{\tau}_1 \ldots \bar{\tau}_m = \bar{\tau}_1 \bar{\tau}_1 \ldots \bar{\tau}_m \cdot \bar{\tau}_m = \bar{1}$$

segue-se que $\sigma^2 \in G = \Omega_n$. Desde que $\Omega_n = G$ é gerado pelos quadrados do tipo $(\tau_x \tau_y)^2$ concluimos que Ω_n é gerado pelos quadrados de todos elementos de O_n^+ .

c.q.d.

Proposição 4.2 - Ω_n é também o subgrupo comutador de O_n^+ quando $n \geq 3$.

Demonstração - (Vide [O] , pag 107)

Observação 4.3

Quando n = 1 o grupo O_1 é um grupo de dois elementos e sua estrutura é trivial. Se n=2, sabemos que O_2^+ é comutativo e, por isso, seu grupo comutador é 1_V . Veremos mais adiante que $\Omega_2 = 1$ se e somente se V é um plano hiperbólico sobre um corpo com três elementos.

Sabemos que o subgrupo comutador Ω_2 de O_2 é gerado pelo conjunto dos quadrados de todas rotações. Mas esse conjunto é um grupo, desde que O_2^+ é comutativo. Logo Ω_2 é o conjunto dos quadrados de todas rotações e, simbolicamente, denotamos $\Omega_2 = (O_2^+)^2$.

O CENTRO Z_n DE O_n

$Z_n(V)$ denota o centro de $O_n(V)$ de um espaço quadrático V.

Observação 4.5

i) Pode-se provar que $Z_n = \{\pm 1_V\}$ exceto quando V é um plano hiperbólico sobre um corpo com três elementos. Neste caso excepcional $Z_2 = O_2$. (Vide [O], 43:12)

ii) Se $n \geq 3$ então o centro de O_n^+ é $O_n^+ \cap Z_n$ e o centro de Ω_n é $\Omega_n \cap Z_n$. (Vide [O], 43:13a) .

CAPÍTULO III

APROXIMAÇÃO FRACA PARA ROTAÇÕES

§1. GRUPO ORTOGONAL SOBRE CORPOS COM VALORIZAÇÕES

Neste parágrafo F denota um corpo com valorização qualquer, não necessariamente um corpo global, $|\ |$ ou $|\ |_{\mathfrak{p}}$ a valorização dada em F e $\mathfrak{p}$ o lugar determinado pela valorização. V é um espaço vetorial n-dimensional sobre F, $L_F(V)$ denota a álgebra das transformações lineares em V, e $M_n(F)$ denota a álgebra das matrizes nxn sobre F. Seja $\{x_1,..,x_n\}$ uma base para V. Todas as normas $\|\ \|$ serão consideradas em relação a essa base.

NORMA EM V

Dado $x \in V$, $x = \sum_{i=1}^{n} \alpha_i x_i$ ($\alpha_i \in F$), a norma de x é definida por $\|x\| = \max_i |\alpha_i|_{\mathfrak{p}}$.

Assim, $\|\ \|_{\mathfrak{p}}$ ou $\|\ \|$ é uma função real com as seguintes propriedades.

1) $\|x\| > 0$ se $x \in \dot{V}$ e $\|0\| = 0$

2) $\|\alpha x\| = |\alpha|\ \|x\|$, para todo $\alpha \in F$ e $x \in V$.

3) $\|x+y\| \leq \|x\| + \|y\|$ para todo $x,y \in V$.

No caso não arquimediano temos

$\|x+y\| \leq \max(\|x\|, \|y\|)$ para todo $x,y \in V$,

com $\|x+y\| = \max(\|x\|,\|y\|)$ se $\|x\| \neq \|y\|$

O espaço vetorial V pode ser considerado um espaço métrico, com a métrica dada por $d(x,y) = \|x-y\|$ para todo $x,y \in V$.

As aplicações $(x,y) \longrightarrow (x+y)$ de VxV em V

$x \longrightarrow -x$ de V em V

$(\alpha,x) \longrightarrow \alpha x$ de FxV em V

são continuas em relação a topologia de V e isto significa que V é um espaço vetorial topológico sobre um corpo topológico F.

NORMA EM $L_F(V)$

Seja $\sigma \in L_F(V)$. Escrevemos $\sigma(x_j) = \sum_i \alpha_{ij} x_i$ $(\alpha_{ij} \in F)$ para $1 \leq j \leq n$, e definimos a norma de σ pela equação

$$\|\sigma\|_p = \max_{i,j} |\alpha_{ij}|_p = \max_j \|\sigma x_j\|$$

denotamos a norma em $L_F(V)$ por $\| \ \|_p$ ou simplesmente $\| \ \|$.

Então, $\| \ \|$ torna $L_F(V)$ um espaço vetorial normado; isto é, as seguintes propriedades são verificadas.

1) $\|\sigma\| > 0$, $\sigma \in L_F(V)$ com $\sigma \neq 0$ e $\|0\| = 0$

2) $\|\alpha\sigma\| = |\alpha| \ \|\sigma\|$ para todo $\alpha \in F$, $\sigma \in L_F(V)$.

3) $\|\sigma + \tau\| \leq \|\sigma\| + \|\tau\|$ para todo $\sigma, \tau \in L_F(V)$.

O espaço vetorial $L_F(V)$ está provido com uma topologica métrica na qual a distância entre σ e τ é definido por

$$d(\sigma,\tau) = \|\sigma - \tau\| .$$

No caso não arquimediano, temos

$$\|\sigma + \tau\| \leq \max(\|\sigma\|, \|\tau\|) \quad \text{para todo } \sigma , \tau \in L_F(V)$$

com $$\|\tau + \sigma\| = \max(\|\sigma\|, \|\tau\|) \quad \text{se} \quad \|\sigma\| \neq \|\tau\|$$

Da mesma maneira, como em V, pode-se verificar que $L_F(V)$ é também um espaço vetorial topológico sobre um corpo topológico. Temos também leis multiplicativas em V e em $L_F(V)$ a considerar. Em V

$$\|\overline{\sigma x}\| \leq \begin{cases} n\|\sigma\| \, \|x\| \text{ em geral} \\ \|\sigma\| \, \|x\| \text{ se não arquimediana} \end{cases}$$

e em $L_F(V)$ $$\|\sigma \, \tau\| \leq \begin{cases} n\|\sigma\| \, \|\tau\| \text{ em geral} \\ \|\sigma\| \, \|\tau\| \text{ se não arquimediana} \end{cases}$$

Logo a função $(\sigma,\tau) \to \sigma \, \tau$ de $L_F(V) \times L_F(V) \to L_F(V)$ é contínua. Isto faz com que $L_F(V)$ seja um anel topológico.

As aplicações $(\sigma_1,\ldots,\sigma_r) \to \sigma_1+\ldots+\sigma_r$

$(\sigma_1,\ldots,\sigma_r) \to \sigma_1 \ldots \sigma_r$ são continuas.

Assim as aplicações $(\sigma,x) \to \sigma x$ de $L_F(V) \times V$ em V e

$\sigma \to \det\sigma$ de $L_F(V)$ em F são contínuas. A continuidade do determinante mostra que $G\ell_n(V)$ é um subconjunto aberto de $L_F(V)$. Se nos restringirmos a $G\ell_n(V)$ verificaremos que $\sigma \to \sigma^{-1}$ de $G\ell_n(V)$ em $G\ell_n(V)$ é contínua.

NORMA EM $M_n(F)$

Podemos também introduzir a norma $\| \ \|$ em $M_n(F)$ pela equação

$$\|(a_{ij})\|_{\mathfrak{p}} = \max_{i,j} |a_{ij}|_{\mathfrak{p}} \text{ para uma matriz } (a_{ij}) \text{ sobre F.}$$

Denotamos a norma por $\|a_{ij}\|_{\mathfrak{p}}$ ou $\|a_{ij}\|$. Observemos que a norma $\|\sigma\|$ de uma transformação linear σ é igual a norma de sua matriz na base $\{x_1,\ldots x_n\}$.

NORMA ESPINORIAL

Proposição 1.1 - Se V é um espaço quadrático regular e $\tau_{u_1},\ldots\tau_{u_r}$ são simetrias tais que $\tau_{u_1}\ldots\tau_{u_r} = 1_V$, então $q(u_1)\ldots q(u_r) \in \dot{F}^2$.

Demonstração: Devido o fato de envolver Álgebras de Clifford, o qual não é de nosso objetivo estudar, vamos omitir tal demonstração. (Vide [O], pag 136).

Seja V um espaço não nulo quadrático regular e n dimensional, com suas respectivas forma bilinear simétrica B e

forma quadrática associada q. Consideremos σ em $O_n(V)$. Pelo teorema da geração em $O_n(V)$, σ pode ser expressa como um produto de simetrias, ou seja $\sigma = \tau_{u_1} \ldots \tau_{u_r}$. Suponhamos que isto seja feito de outra forma, ou seja $\sigma = \tau_{v_1} \ldots \tau_{v_s}$. Então como $\sigma.\sigma^{-1} = 1_V$, temos

$$\tau_{u_1} \ldots \tau_{u_r} . \tau_{v_s} \ldots \tau_{v_1} = 1_V$$

e, pelo resultado anterior assumido,

$$q(u_1)\ldots q(u_r) = q(v_1)\ldots q(v_s) \pmod{\dot{F}^2}$$

A imagem canonica de $q(u_1)\ldots q(u_r)$ em $F/\dot{F}^2$ é chamada norma espinorial de σ e é indicada por $\theta(\sigma)$. De acordo com o que vimos acima, θ está bem definida, pois independe da representação de σ. Claramente $\theta(\sigma.\tau) = \theta(\sigma).\theta(\tau)$.

Assim temos um homomorfismo de grupos

$$\theta : O_n \to \dot{F}/\dot{F}^2$$

O nosso maior interesse é sobre a norma espinorial de reflexões e passaremos então a considerar a restrição

$$\theta : O_n^+ \to \dot{F}/\dot{F}^2 \quad .$$

O núcleo desta restrição é indicado por $O_n'(V)$.

Assim $O_n'(V) = \{\sigma \in O_n^+(V) \mid \theta(\sigma) = 1\}$

O comutador claramente tem norma espinorial 1, assim

$$\Omega_n \subseteq O_n' \subseteq O_n^+ \subseteq O_n$$

Notemos ainda que cada um desses subgrupos é normal em O_n .

Observação 1.2 - A equação $\theta\sigma = \alpha$, com α em $\dot{F}$, frequentemente vai aparecer; isto realmente significa que $\theta\sigma$ é a imagem canônica de α em $\dot{F}/\dot{F}^2$. Ocasionalmente olharemos $\theta\sigma$ como toda a classe $\alpha\dot{F}^2$, colocado como um subconjunto de $\dot{F}$. Mais geralmente, se X é um subconjunto qualquer de O_n , o símbolo θX é a imagem de X em $\dot{F}/\dot{F}^2$ através de θ ; mas também a olharemos como sendo o conjunto

$$\theta(X) = \bigcup_{\sigma \in X} \theta(\sigma)\,\dot{F}^2 \text{ de X em } \dot{F}$$

Se X é um subgrupo de O_n então $\theta(X)$ é um subgrupo de $\dot{F}$.

Proposição 1.3 - Seja V um espaço quadrático regular n-dimensional com $n \geq 2$. Então $\theta(O_n^+)$ é um subgrupo de $\dot{F}$, consistindo de todos so escalares não nulos da forma $\alpha_1, \ldots, \alpha_{2r}$ com $2r \leq n$ e $\alpha_1, \ldots \alpha_{2r}$ em $q(V)$.

Demonstração: O resultado segue, usando o fato de que

$$\theta(O_n^+) = \bigcup_{\sigma \in O_n^+} \theta(\sigma)\,\dot{F}^2$$

c.q.d.

Proposição 1.4 - Sejam $u_1,\ldots,u_r$ e $v_1,\ldots,v_r$ vetores anisotrópicos em um espaço quadrático regular V e suponhamos que $(q(u_1),\ldots q(u_r))$ seja uma permutação de $(q(v_1),\ldots,q(v_r))$ então

$$\tau_{u_1} \ldots \tau_{u_r} = \tau_{v_1} \ldots \tau_{v_r} \pmod{\Omega_n}$$

Demonstração: Seja $\{w_1,\ldots,w_r\}$ uma reordenação de $\{v_1,\ldots,v_r\}$ tal que $q(w_i) = q(u_i)$ para $1 \leq i \leq r$.

Seja $-: O_n \to O_n/\Omega_n$ o homomorfismo natural de O_n em O_n/Ω_n . Desde que O_n/Ω_n é comunativo, então

$$\bar{\tau}_{v_r} \ldots \bar{\tau}_{v_1}\ \bar{\tau}_{u_1} \ldots \bar{\tau}_{u_r} = (\bar{\tau}_{w_1}\ \bar{\tau}_{u_1}) \ldots (\bar{\tau}_{w_r}\ \bar{\tau}_{u_r})$$

e, consequentemente,

$$\tau_{v_r} \ldots \tau_{v_1}\ \tau_{u_1} \ldots \tau_{u_r} = (\tau_{w_1}\ \tau_{u_1}) \ldots (\tau_{w_r}\ \tau_{u_r}) \pmod{\Omega_n}$$

Assim, é suficiente provar que $\tau_w \tau_u \in \Omega_n$ sempre que $q(w) = q(u) \neq 0$.

Pelo teorema de Witt existe um $\sigma \in O_n$ tal que $\sigma w = u$.

Então $\sigma \tau_w \sigma^{-1} = \tau_{\sigma w} = \tau_u$ e, portanto, $\tau_w \tau_u = \tau_w \sigma \tau_w^{-1} \sigma^{-1} \in \Omega_n$.

c.q.d.

Proposição 1.5 - Seja U subespaço regular de um espaço quadrático V. Se $q(U) = q(V)$ e $\Omega(U) = O'(U)$ então $\Omega(V) = O'(V)$.

Demonstração: Seja $\sigma \in O'(V)$. Pelo teorema da geração podemos expressar σ como um produto de simetrias

$$\sigma = \tau_{v_1} \cdots \tau_{v_r}$$

Tomemos $u_1, \ldots u_r \in U$ com $q(u_i) = q(v_i)$ para $1 \leq i \leq r$ e seja $\rho = \tau_{u_1} \cdots \tau_{u_r} \in O'(V)$. Então $\sigma \in \rho\,\Omega(V)$ pela proposição 1.4 e, portanto, é suficiente provar que $\rho \in \Omega(V)$. Se considerarmos a decomposição $V = U \perp W$, então $\rho = \bar{\rho} \perp 1_W$ com $\bar{\rho} \in O(U)$ desde cada u_i esteja em U. Mas $\theta(\bar{\rho}) = \theta(\rho) = 1$ de onde segue-se que $\bar{\rho} \in O'(U)$ ou $\bar{\rho} \in \Omega(U)$ e, portanto, $\rho \in \Omega(V)$.

c.q.d.

Proposição 1.6 - Se V é isotrópico então $\Omega(V) = O'(V)$.

Demonstração: Seja $H \subseteq V$ um plano hiperbólico. Então $q(h) = F = q(V)$, pois todo plano hiperbólico é universal e $\Omega(H) = O'(H)$ pela observação 4.3 do capítulo II. Logo $\Omega(V) = O'(V)$ usando a proposição anterior.

c.q.d.

§2. O GRUPO ORTOGONAL SOBRE CORPOS GLOBAIS

LOCALIZAÇÃO

E é uma extensão de F.

Definição 2.1 - Consideremos dois espaços vetoriais V e W de dimensão finita sobre corpos E, F respectivamente. Dizemos que W é F-edificação de V se:

i) $V \subset W$

ii) Toda base de V sobre E é também uma base de W sobre F.

Observação 2.2 - Se V é um espaço quadrático regular n-dimensional sobre um corpo global F e $F_\mathfrak{p}$ é o completamento de F, usaremos $V_\mathfrak{p}$ para indicar a $F_\mathfrak{p}$-edificação de V (como um espaço vetorial ou como um espaço quadrático) e diremos que $V_\mathfrak{p}$ é uma $\mathfrak{p}$-edificação ou localização de V em $\mathfrak{p}$. Aqui $\mathfrak{p}$ é um lugar não arquimediano ou discreto.

Desde que $V_\mathfrak{p}$ é um espaço vetorial sobre um corpo com valorização $F_\mathfrak{p}$, podemos introduzir uma norma $\| \ \|_\mathfrak{p}$ em $V_\mathfrak{p}$ e $L_{F_\mathfrak{p}}(V_\mathfrak{p})$ com respeito a uma base qualquer de $V_\mathfrak{p}$; em particular com respeito a uma base qualquer de V sobre F. Observemos que $\| \ \|_\mathfrak{p}$ independe da base escolhida.

Definição 2.3 - Se $\sigma \in L_F(V)$, então existe uma única transformação linear $\sigma_{\mathfrak{p}}$ em $V_{\mathfrak{p}}$ induzida por σ em V. Diremos que $\sigma_{\mathfrak{p}}$ é a localização de σ em $\mathfrak{p}$.

Claramente são verificadas as seguintes propriedades, em relação a uma certa base de V.

1) $(\sigma + \tau)_{\mathfrak{p}} = \sigma_{\mathfrak{p}} + \tau_{\mathfrak{p}}$

2) $(\sigma\tau)_{\mathfrak{p}} = \sigma_{\mathfrak{p}} \cdot \tau_{\mathfrak{p}}$

3) $(\alpha\sigma)_{\mathfrak{p}} = \alpha\sigma_{\mathfrak{p}}$, $\det\sigma_{\mathfrak{p}} = \det\sigma$, para todo σ, τ em $L_F(V)$ e todo α em F.

Em particular a aplicação $\sigma \to \sigma_{\mathfrak{p}}$ é um homomorfismo injetor de $L_F(V)$ em $L_{F_{\mathfrak{p}}}(V_{\mathfrak{p}})$. Claramente, usando as definições e propriedades relacionadas, as seguintes afirmações são verificadas:

- Se σ é uma isometria então $\sigma_{\mathfrak{p}}$ é uma isometria.
- Se σ é uma rotação então $\sigma_{\mathfrak{p}}$ é uma rotação.
- Se τ_u é uma simetria de V com respeito a reta F_u então $(\tau_u)_{\mathfrak{p}}$ é uma simetria de $V_{\mathfrak{p}}$ com respeito a reta $F_{\mathfrak{p}} u$.

Denotaremos por $A_{\mathfrak{p}}$ a imagem de um subconjunto A de $L_F(V)$ em $L_F(V_{\mathfrak{p}})$ através de uma localização em $\mathfrak{p}$. Temos, en-

tão, $O_n(V)_{\mathfrak{p}} \subseteq O_n(V_{\mathfrak{p}})$

$\Omega_n(V)_{\mathfrak{p}} \subseteq \Omega_n(V_{\mathfrak{p}})$

$O_n^+(V)_{\mathfrak{p}} \subseteq O_n^+(V_{\mathfrak{p}})$

e $O_n'(V)_{\mathfrak{p}} \subseteq O_n'(V_{\mathfrak{p}})$.

TEOREMA DA APROXIMAÇÃO FRACA PARA ROTAÇÕES

Sejam V um espaço quadrático regular sobre um corpo global F e T um conjunto finito de lugares em F. Para cada $\mathfrak{p}$ em T, seja $\vartheta_{\mathfrak{p}}$ é um elemento de $O^+(V_{\mathfrak{p}})$. Então para cada $\varepsilon > 0$, existe σ em $O^+(V)$ tal que $\|\sigma - \vartheta_{\mathfrak{p}}\|_{\mathfrak{p}} < \varepsilon$, para todo $\mathfrak{p}$ em T.

Demonstração: Cada $\vartheta_{\mathfrak{p}}$ em $O^+(V_{\mathfrak{p}})$ pode ser expresso como um produto de simetrias $\vartheta_{\mathfrak{p}} = \tau_{u_1\mathfrak{p}} \ldots \tau_{u_r\mathfrak{p}}$, onde $u_i\mathfrak{p}$ são vetores anisotrópicos em $V_{\mathfrak{p}}$. O número r é ímpar e sempre podemos considerar o mesmo número para todo $\mathfrak{p}$ (adicionando quadrados de simetrias, se necessário). Pelo teorema da Aproximação Fraca aplicada às coordenadas do vetor $u_1\mathfrak{p}$ em uma base $\{x_1 \ldots x_n\}$ de V, obtemos um vetor u_1 em V tal que $\|u_1 - u_1\mathfrak{p}\|_{\mathfrak{p}}$ é arbitrariamente pequeno para todo $\mathfrak{p}$ em T. Pelo fato da aplicação $u \to \tau_u$ ser contínua, então τ_{u_1} está arbitrariamente perto de $\tau_{u_1\mathfrak{p}}$. Se repetirmos o processo para i = 1,...,r obteremos vetores anisotrópicos $u_1,\ldots,u_r$ de V com $\|\tau_{u_i} - \tau_{u_i\mathfrak{p}}\|_{\mathfrak{p}}$ arbitrariamente pequeno para todo $1 \leq i \leq r$ e

todo $\mathfrak{p}$ em T. Logo, pela continuidade da multiplicação em $L_{F_\mathfrak{p}}(V_\mathfrak{p})$, segue-se que $\|\tau_{u_1} \ldots \tau_{u_r} - \tau_{u_1\mathfrak{p}} \ldots \tau_{u_r\mathfrak{p}}\| < \varepsilon$, para todo $\mathfrak{p}$ em T. Se considerarmos $\sigma = \tau_{u_1} \ldots \tau_{u_r} \in O^+(V)$, então teremos o resultado desejado, ou seja $\|\sigma - \varphi_\mathfrak{p}\|_\mathfrak{p} < \varepsilon$ para todo $\mathfrak{p}$ em T.

c.q.d.

Observação 2.4 - Pode-se provar que se V é um espaço quadrático regular n-dimensional sobre um corpo global F e σ é um elemento de $O_n^+(V)$, então σ está em $\Omega_n(V)$ se e somente se $\sigma_\mathfrak{p}$ está em $\Omega_n(V_\mathfrak{p})$, para cada lugar $\mathfrak{p}$ em F.

CAPÍTULO IV

APROXIMAÇÃO FORTE PARA ROTAÇÕES

O principal objetivo desse capítulo é a prova do teorema da aproximação forte para rotações, como também apresentar diversas aplicações do tal teorema.

As principais notações continuam sendo as mesmas usadas nos capítulos anteriores, ou seja F é um corpo de característica diferente de 2, $0 = 0(S)$ é o anel dos inteiros de F no conjunto de Dedekind de lugares S, $u = u(S)$ é o grupo das unidades de F em S e V é um espaço vetorial n dimensional sobre F.

§1. LATICES

Definimos um ideal fracionário $\mathfrak{a}$ de F em S como um 0-modulo não nulo $\mathfrak{a} \subseteq F$ com a seguinte propriedade: existe um $\lambda \neq 0$ em 0 tal que $\lambda\mathfrak{a} \subseteq 0$. Denotaremos por $I = I(S)$ com o conjunto de todos ideais fracionários de F em S.

Consideremos o conjunto $FM = \{\alpha x \mid \alpha \in F,\ x \in M\}$ onde $M \subseteq V$ é um 0-Módulo. Desde que M é um 0-módulo e F é o corpo quociente de 0, então temos

$$FM = \{\alpha^{-1} x \mid \alpha \in 0\ ,\ \alpha \neq 0,\ x \in M\}\ .$$

Claramente observamos que FM é um subespaço vetorial de V. Dados $\alpha \in F$ e $\mathfrak{a} \in I$, definimos os seguintes conjuntos

$$\alpha M = \{\alpha x \mid x \in M\} \quad \text{e} \quad \mathfrak{a}M = \{ \sum_{\text{finita}} \beta x \mid \beta \in \mathfrak{a}, x \in M\}$$

Os conjuntos αM e $\mathfrak{a}M$ são O-módulos e as seguintes propriedades são facilmente verificadas

i) $\alpha(M \cap N) = \alpha M \cap \alpha N$, $\alpha \in F$

ii) $(\alpha O)M = \alpha M$, $\alpha \in F$

iii) $(\alpha\mathfrak{a})M = \alpha(\mathfrak{a}M)$, $\alpha \in F$ e $\mathfrak{a} \in I$

iv) $(\mathfrak{a}+\mathfrak{b})M = \mathfrak{a}M + \mathfrak{b}M$ e $(\mathfrak{a}\mathfrak{b})M = \mathfrak{a}(\mathfrak{b}M)$, $\mathfrak{a},\mathfrak{b} \in I$

v) $\mathfrak{a}(M+N) = \mathfrak{a}M + \mathfrak{a}N$

vi) $F(M+N) = FM + FN$.

Definição 1.1 - Um O-módulo $M \subseteq V$ é um latice em V se existe uma base $\{x_1,\ldots x_n\}$ em V tal que $M \subseteq Ox_1 + \ldots + Ox_n$. Se M satisfizer a propriedade acima e FM = V, diremos que M é um latice sobre V.

Observação 1.2 - Em particular $Ox_1 + \ldots + Ox_n$ é um latice sobre V.

Proposição 1.3 - Seja L um látice em um espaço vetorial V sobre F. Então um O-módulo M em V é um látice em V se e somente se

existe $\alpha \neq 0$ em O tal que $\alpha M \subseteq L$.

Demonstração: Admitamos que M seja um latice em V. Então existe uma base $\{x_1,\ldots,x_n\}$ de V tal que $M \subseteq Ox_1 +\ldots+ Ox_n$. Desde que L é um latice sobre V, podemos encontrar n elementos linearmente independentes $\{y_1,\ldots,y_n\}$ em L tal que $x_j = \sum_{i=1} a_{ij}\, y_i (a_{ij} \in F)$. No entanto esses a_{ij} geram um certo ideal fracionário e, portanto, existe um $\alpha \neq 0$ em C tal que $\alpha a_{ij} \in O$ para todo i,j . Assim, $\alpha x_j \in Oy_1 +\ldots+ Oy_n \subseteq L$. Logo $\alpha M \subseteq L$.

Reciprocamente vamos supor que existe $\alpha \neq 0$ em O tal que $\alpha M \subseteq L$. Desde que L é um latice, existe uma base $\{z_1,\ldots,z_n\}$ de V tal que $L \subseteq Oz_1 +\ldots+ Oz_n$, portanto $M \subseteq \alpha^{-1} L \subseteq O(\frac{z_1}{\alpha})+\ldots+O(\frac{z_n}{\alpha})$. Logo M é um latice em V.

Corolário 1.4 - Seja U um subespaço de V com $M \subseteq U \subseteq V$. Então M é um latice em V se e somente se M é um latice em U.

Demonstração: Sejam $\{x_1,\ldots,x_r\}$ uma base para U e $\{x_1,\ldots,x_r, x_{r+1},\ldots,x_n\}$ uma extensão dessa base para V. Consideremos $L' = Ox_1 +\ldots+ Ox_r$ e $L = Ox_1 +\ldots+ Ox_n$. Se M é um latice em U então $\alpha M \subseteq L' \subseteq L$, para algum α não nulo em O. Portanto M é um latice em V.

Reciprocamente, se M é um latice em V então exis

te um α não nulo em O tal que $\alpha M \subseteq L$. Portanto, $\alpha M \subseteq L \cap U = L'$ e, assim, M é um latice em U.

Sejam V um espaço vetorial n-dimensional sobre F e $V_{\mathfrak{p}}$ a $\mathfrak{p}$-edificação ou localização de V em $\mathfrak{p}$. Seja L um latice em V. Uma $\mathfrak{p}$-edificação ou localização $L_{\mathfrak{p}}$ de L em $\mathfrak{p}$ é o $O_{\mathfrak{p}}$-módulo gerado por L em $V_{\mathfrak{p}}$. Claramente $L_{\mathfrak{p}}$ é um latice em $V_{\mathfrak{p}}$.

Proposição 1.5 - Sejam S um conjunto de Dedekind de lugares em F, L um latice em um espaço vetorial V sobre F e seja σ um elemento do espaço das transformações lineares de V em V sobre F. Então $\sigma_{\mathfrak{p}} L_{\mathfrak{p}} = (\sigma L)_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em S.

Demonstração: Vamos expressar $L = \mathfrak{a}_1 y_1 + \ldots + \mathfrak{a}_r y_r$ onde $\mathfrak{a}_i$ são ideais fracionários e y_i elementos de V. Portanto,

$$\begin{aligned}
\sigma_{\mathfrak{p}} L_{\mathfrak{p}} &= \sigma_{\mathfrak{p}} (\mathfrak{a}_{1\mathfrak{p}} y_1 + \ldots + \mathfrak{a}_{r\mathfrak{p}} y_r) \\
&= \mathfrak{a}_{1\mathfrak{p}}(\sigma y_1) + \ldots + \mathfrak{a}_{r\mathfrak{p}}(\sigma y_r) \\
&= (\mathfrak{a}_1(\sigma y_1) + \ldots + \mathfrak{a}_r(\sigma y_r))_{\mathfrak{p}} \\
&= (\sigma L)_{\mathfrak{p}}
\end{aligned}$$

c.q.d.

Como consequência imediata temos:

$O_n(L)_{\mathfrak{p}} \subseteq O_n(L_{\mathfrak{p}})$ e $O_r^+(L)_{\mathfrak{p}} \subseteq O_n^+(L_{\mathfrak{p}})$ para todo $\mathfrak{p}$ em S.

Observação 1.6 - Segue imediatamente da definição de latice, que todo submodulo de um latice é um latice. Em particular se L e K são latices em V então $L \cap K$ é um latice em V e a Proposição 1.3 também mostra que αL , ∂L e L+K são latices em V para algum $\alpha \in F$ e $\partial \in I$. Claramente Ox, com $x \in V$ e ∂x com $\partial \in I$, são latices. Em particular, todo O-Modulo finitamente gerado em V é um latice.

BASES

Consideremos L um latice em V. Um conjunto de vetores em L é linearmente independente sobre O se e somente se esse conjunto é linearmente independente sobre F.

Definição 1.7 - O conjunto $\{x_1, \ldots, x_n\}$ é uma base para L, se tal conjunto é uma base no sentido de O-modulos; ou seja, se $\{x_1, \ldots x_n\}$ é linearmente independente e gera L sobre O. Assim $\{x_1, \ldots, x_n\}$ é uma base para L se e somente se é uma base para FL com $L = Ox_1 + \ldots + Ox_n$.

Definição 1.8 - Um latice que tem uma base é chamado um lâtice livre.

Observação 1.9 - Qualquer duas bases de um latice livre tem o mesmo número de elementos e esse número é chamado dimensão

de L e é denotado por dim L.

Todo iátice L é quase livre no sentido de que ele pode ser expresso na forma $L = \mathfrak{a}x_1 + Ox_r + \ldots + Ox_r$ com $\mathfrak{a}$ um ideal fracionário e $\{x_1,\ldots,x_n\}$ uma base para FL. Claramente, se todo ideal fracionário é principal, todo latice é livre.

MATRIZ DE UM LATICE

Uma matriz quadrada (a_{ij}) com coeficientes em F é integral (com respeito a O) se cada um de seus coeficientes está em O. Se (a_{ij}) é integral e $\det(a_{ij}) = 1$, diremos que (a_{ij}) é unimodular.

Seja V um espaço quadrático e B a forma bilinear associada. Se L é um latice livre sobre V, então existe uma base $\{x_1,\ldots x_n\}$ de V tal que $L = Ox_1 + \ldots + Ox_n$. Definimos como matriz de L na base $\{x_1,\ldots x_n\}$ a matriz $N = (B(x_i,x_j))$, isto é, a matriz de V na base $\{x_1,\ldots x_n\}$. Se N é unimodular diremos que L é unimodular.

Sejam U e V espaços quadráticos e L e K latices em U e V, respectivamente. O latice K é representado por L e denotamos por $K \rightarrow L$, se existe uma representação σ: $FK \rightarrow FL$ tal que $\sigma K \subseteq L$. Dizemos que existe uma isometria de K em L e denotamos

$K \rightarrowtail L$ se existe uma isometria σ: $FK \to FL$ tal que $\sigma K \subseteq L$.

Dois latices K e L são isométricos se existe uma isometria σ: $FK \to FL$ tal que $\sigma K = L$ e denotamos $K \rightarrowtail L$ ou $K \tilde{=} L$.

Uma matriz M é integralmente representada por uma matriz N, se existe uma matriz T com coeficientes em O tal que $M = {}^{t}T\,N\,T$ e denotamos $M \to N$ (sobre O). Se T é unimodular, dizemos que M e N são integralmente equivalentes e escrevemos $M \tilde{=} N$ (sobre O).

Sejam U e V espaços quadráticos.

Proposição 1.10 - Sejam K e L latices em U e V, com matrizes M e N respectivamente. Então,

1) $K \to L$ se e somente se $M \to N$ (sobre O)

2) $K \tilde{=} L$ se e somente se $M \tilde{=} N$ (sobre O)

Demonstração: (Vide [O] , pg 222)

CLASSE DE UM LATICE

Consideremos um espaço quadrático regular V sobre F e K e L latices sobre V. Dizemos que K e L estão na mesma classe de isometria se $K = \sigma L$ para algum σ em $O_n(V)$ e denotaremos classe de L por $c\ell s\ L$. Denotaremos por $c\ell s^{+}L$ o conjunto dos latices em V tal que $K = \sigma L$ onde σ está em $O^{+}(V)$.

Seja L um lâtice em V. O conjunto $O(L)=\{\sigma \in O(V) | \sigma L = L\}$ é claramente um subgrupo de O(V), chamado grupo das unidades de L em V. Indicaremos $O^+(L) = O(L) \cap O^+(V)$.

A aplicação determinante $\det : O(L) \to \{+1,-1\}$ tem como núcleo $O^+(L)$. Portanto $O^+(L)$ é um subgrupo normal de O(L). Definimos $O^-(L) = O(L) \cap O^-(V)$. Logo $O(L) = O^+(L) \cap O^-(L)$ e $O^+(L) \cap O^-(L) = \emptyset$.

Observação 1.11 - 1) Seja F um corpo local. Logo se $\sigma \in O(V)$, $\det \sigma = \pm 1$ e isto significa que $\det \sigma$ é uma unidade. Assim, $\|\sigma\| \geq 1$. Agora consideremos a latice $M = Ox_1 + \ldots + Ox_n$ onde $\{x_1, \ldots x_n\}$ é uma base em V usada na definição de $\| \ \|$. Então a asserção $\|\sigma\| = 1$ se e somente se $\|\sigma\| \leq 1$ é equivalente a $\sigma M \subseteq M$ e assim $\sigma M = M$. Dessa maneira os elementos de O(M) são precisamente as isometrias de V com $\|\sigma\| = 1$.

2) Consideremos um latice L em V. Podemos verificar que $\sigma L = L$, para todo σ em $O_n(V)$ que esta suficientemente perto de 1_V . Para isto consideremos uma base $\{x_1', \ldots x_n'\}$ de L e seja $\| \ \|'$ a norma em relação a esta nova base, Então todo σ que esta suficientemente perto de 1_V satisfaz $\|\sigma - 1_V\|' < 1$. Assim cada σ satisfaz $\|\sigma\|' = 1$. Logo $\sigma L = L$.

3) Sejam L e K latices em V e suponhamos que $K = \lambda L$ para algum λ em $O_n(V)$. Podemos verificar que $\sigma L = K$ para todo σ em $O_n(V)$ que está suficientemente perto de λ. Pela escolha de σ suficientemente perto de λ podemos assumir que $\|\lambda^{-1}\sigma - 1_V\|$ é suficientemente pequeno, pois $\|\lambda^{-1}\sigma - 1_V\| \leq \|\lambda^{-1}\|\sigma - \lambda\|$. Porem pela parte (2) todo $\lambda^{-1}\sigma$ que esta suficientemente perto de 1_V faz com que $(\lambda^{-1}\sigma)L = L$. Logo todo σ que está suficientemente perto de λ faz $\sigma L = \lambda L = K$.

§2. GENUS E GENUS ESPINORIAL

Sejam V um espaço quadrático regular sobre um corpo global F, S um conjunto de Dedekind consistindo de quase todos os lugares sobre F e Ω o conjunto de lugares não triviais sobre F.

O GRUPO DAS ROTAÇÕES DECOMPOSTAS EM J_V

Consideremos o grupo multiplicativo $\pi_{\mathfrak{p}\in\Omega} O^+(V_{\mathfrak{p}})$, consistindo do produto direto de todos os grupos $O^+(V_{\mathfrak{p}})$. Um elemento desse grupo é definido por suas coordenadas ou seja $\sum = (\sum_{\mathfrak{p}})_{\mathfrak{p}\in\Omega}$ $(\sum_{\mathfrak{p}} \in O^+(V))$. Definimos $J_V = \{\sum = (\sum_{\mathfrak{p}}) \mid \|\sum_{\mathfrak{p}}\|_{\mathfrak{p}} = 1$ para todo $\mathfrak{p}$ em $\Omega\}$ como sendo o grupo das rotações decompostas do espaço quadrático V e seja $J'_V = \{\sum \in J_V \mid \sum_{\mathfrak{p}} \in O'(V_{\mathfrak{p}})$ para todo $\mathfrak{p}$

em Ω} . Observemos ainda que J_V' é subgrupo normal de J_V e que J_V/J_V', é comutativo.

Observação 2.1 - 1) Se σ é um elemento de $O^+(V)$, então σ tem uma localização $\sigma_\mathfrak{p}$ para cada $\mathfrak{p}$ em e $\|\sigma_\mathfrak{p}\|_\mathfrak{p} = 1$ para quase todo $\mathfrak{p}$. Logo σ determina uma rotação decomposta $(\sigma)=(\sigma_\mathfrak{p})_\mathfrak{p} \in \Omega$. A aplicação $\sigma \to (\sigma)$ determina um isomorfismo natural de $O^+(V)$ em J_V .

2) Definimos o subgrupo J_L de J_V , onde L é um latice em V em relação ao conjunto de lugares em S, pela equação $J_L = \{\sum \in J_V \mid \sum_\mathfrak{p} \in O^+(L_\mathfrak{p})$ para todo $\mathfrak{p}$ em S$\}$. Se σ é um elemento de $O^+(L)$, então $\sigma_\mathfrak{p}$ esta em $O^+(L_\mathfrak{p})$ para todo $\mathfrak{p}$ em S.

GENUS

Definição 2.2 - O genus (gen L) de um latice L em V é o conjunto de todos os latices K em V com a seguinte propriedade: para cada $\mathfrak{p}$ em S existe uma isometria $\sum_\mathfrak{p}$ em $O(V_\mathfrak{p})$ tal que $K_\mathfrak{p} = \sum_\mathfrak{p} L_\mathfrak{p}$. Segue imediatamente da definição que gen K = gen L se e somente se cls $K_\mathfrak{p}$ = cls $L_\mathfrak{p}$ para todo $\mathfrak{p}$ em S.

Definição 2.3 - O genus próprio (gen^+L) de um latice L em V é o conjunto de todos os latices K em V com a seguinte propriedade: Para cada $\mathfrak{p}$ em S existe uma rotação $\sum_\mathfrak{p}$ em $O^+(V_\mathfrak{p})$ tal que $K_\mathfrak{p} = \sum_\mathfrak{p} L_\mathfrak{p}$.

Da mesma forma, $gen^{+}K = gen^{+}L$ se e somente se $cls^{+}K_{\mathfrak{p}} = cls^{+}L_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em S.

Observação 2.4 - Pelo fato de que clsL e $cls^{+}L$ coincidem sobre corpos locais então, nesse caso, gen L coincide com $gen^{+}L$.

Observação 2.5 - Podemos tambem mostrar que o genus de um lattice L em V pode ser descrito em termos de rotações decompostas, ou seja $K \in$ gen L se e somente $K = \sigma L$ para algum σ em J_V .

Definição 2.6 - Um latice K em V está no mesmo genus espinorial de L se existe uma isometria σ em $O_n(V)$ e uma rotação $\sigma_{\mathfrak{p}}$ em $O'(V_{\mathfrak{p}})$, em cada $\mathfrak{p}$ em S, tal que $K_{\mathfrak{p}} = \sigma_{\mathfrak{p}} \cdot \sigma_{\mathfrak{p}} L_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em S. Podemos expressar tal definição em termos de rotações decompostas, ou seja, existe σ em $O_n(V)$ e σ em J'_V tal que $K = \sigma \sigma L$. Usaremos spnL para denotar o conjunto de latices no-mesmo genus espinorial de L. Claramente podemos verificar, pelo uso das definições, que latices que estão na mesma classe de isometria estão no mesmo genus espinorial, e latices no mesmo genus espinorial estão no mesmo genus. Temos então que $clsL \subseteq spnL \subseteq genL$.

Denotaremos por h(L) o número de classes de isometria em gen L e g(L) o número de genera espinoriais em gen L . Pode ser verificado que g(L) e h(L) são sempre finitos.

Definição 2.7 - Um latice K está no mesmo genus próprio espinorial de um látice L se existe uma rotação σ em $O^+(V)$ e uma rotação $\sum_{\mathfrak{p}}$ em $O'(V_{\mathfrak{p}})$, em cada $\mathfrak{p}$ em S, tal que $K_{\mathfrak{p}} = \sigma_{\mathfrak{p}} \sum_{\mathfrak{p}} L_{\mathfrak{p}}$, para todo $\mathfrak{p}$ em S. Esta definição pode ser expressa em termos de rotações decompostas, ou seja que existe σ em $O^+(V)$ e $\sum$ em J'_V, para cada $\mathfrak{p}$ em S, tal que $K = \sigma \sum L$. Usaremos spn^+L para denotar o conjunto de latices no mesmo genus próprio espinorial de L. Da mesma forma temos que: $cls^+ \subseteq spn^+L \subseteq gen^+L$ e que $h^+(L)$ é o número de classes próprias em genL e $g^+(L)$ o número de genera próprios espinoriais em genL. Os números $h^+(L)$ e $g^+(L)$ são ambos finitos.

APLICAÇÃO DA APROXIMAÇÃO FRACA PARA ROTAÇÕES

Sejam K um látice em genL e T um subconjunto finito de lugares S. Queremos provar que existe um latice K' em cls^+K tal que $K'_{\mathfrak{p}} = L_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em T.

Pela definição de genus existe uma rotação $\varphi_{\mathfrak{p}}$ em $O^+(V_{\mathfrak{p}})$, para cada $\mathfrak{p}$ em T, tal que $\varphi_{\mathfrak{p}} K_{\mathfrak{p}} = L_{\mathfrak{p}}$. Usando o teorema da aproximação fraca para rotações existe uma rotação σ em $O^+(V)$ tal que $\|\sigma - \varphi_{\mathfrak{p}}\|_{\mathfrak{p}}$ é arbitrariamente pequeno para cada $\mathfrak{p}$ em T. Se as aproximações são suficientemente boas, então teremos,

devido a proposição 1.5 e a observação 1.11 que $(\sigma K)_{\mathfrak{p}} = \sigma_{\mathfrak{p}} K_{\mathfrak{p}} = \varphi_{\mathfrak{p}} K_{\mathfrak{p}} = L_{\mathfrak{p}}$, para todo $\mathfrak{p}$ em T. Portanto σK esta em $c\ell s^{+} K$. Logo este é o latice K' procurado.

§3. APROXIMAÇÃO FORTE PARA ROTAÇÕES

A diferença entre aproximação Fraca e Forte é que no teorema da aproximação forte é requerido ainda que o elemento σ que aproxima cada $\varphi_{\mathfrak{p}}$ tenha matriz a coeficientes inteiros, para todo lugar $\mathfrak{p}$ que não esta em T, onde T é um subconjunto finito de um conjunto de lugares S.

O teorema da aproximação forte não é válido para todo espaço quadrático e nem para $O^{+}(V)$. Contudo ele é válido numa situação bastante geral, no caso onde trabalhamos com o grupo $O'(V)$ e requeremos que o conjunto de lugares seja indefinido.

Sejam S um conjunto de Dedekind consistindo de quase todos os lugares em um corpo global F, V um espaço quadrático regular sobre F e Ω o conjunto de lugares não triviais sobre F.

Definição 3.1 - O conjunto S é indefinido para V se existe pelo menos um lugar $\mathfrak{p}$ (arquimediano ou discreto) em Ω-S tal que $V_{\mathfrak{p}}$ é isotrópico. Se $V_{\mathfrak{p}}$ é anisotrópico para cada $\mathfrak{p}$ em Ω-S, dize

mos que S é um conjunto definido de lugares para V.

O teorema seguinte será admitido sem demonstração.

Teorema 3.2 - Sejam V um espaço quadrático regular com forma quadrática q, sobre um corpo global F, com dim V $\geq$ 5, S um conjunto indefinido de lugares para V e T um subconjunto finito de S. Seja a um elemento não nulo de q(V) tal que, para cada $\mathfrak{p}$ em S, existe um $Z_{\mathfrak{p}}$ em V com $q(Z_{\mathfrak{p}}) = a$ e $\|Z_{\mathfrak{p}}\|_{\mathfrak{p}} \leq 1$ para todo $\mathfrak{p}$ em S-T. Então para cada $\varepsilon > 0$, existe um Z em V com $q(Z) = a$ tal que

$\|Z\|_{\mathfrak{p}} \leq 1$ para todo $\mathfrak{p}$ em S-T

e $\|Z - Z_{\mathfrak{p}}\|_{\mathfrak{p}} < \varepsilon$ para todo $\mathfrak{p}$ em T.

Demonstração: (Vide [O], pag 311)

Vamos provar o teorema da aproximação forte para rotações, onde dimV $\geq$ 5.

TEOREMA DA APROXIMAÇÃO FORTE: Sejam V um espaço quadrático regular sobre um corpo global F, com dimV $\geq$ 5, S um conjunto indefinido de lugares para V e T um subconjunto finito de S. Seja $\varphi_{\mathfrak{p}}$ uma rotação em $O'(V_{\mathfrak{p}})$ para cada $\mathfrak{p}$ em T. Então para cada $\varepsilon > 0$ existe uma rotação σ em O'(V) tal que $\|\sigma - \varphi_{\mathfrak{p}}\|_{\mathfrak{p}} < \varepsilon$ para todo $\mathfrak{p} \in T$ e $\|\sigma\|_{\mathfrak{p}} = 1$ para todo $\mathfrak{p}$ em S-T.

Demonstração: Seja $\{x_1,\ldots,x_n\}$ uma base para V, a qual determina todas as normas $\| \ \|_p$. Podemos assumir que $0 < \varepsilon < 1$. Vamos dividir a prova em duas partes:

1) Primeiramente vamos supor que cada φ_p é um "pequeno comutador", isto é, $\varphi_p = \sigma_{u_p} \cdot \sigma_{v_p} \cdot \sigma_{u_p} \cdot \sigma_{v_p}$, onde σ_{u_p} e σ_{v_p} são simetrias de V_p com respeito aos vetores anisotrópicos u_p e v_p de V_p. Pelo teorema da Aproximação Fraca usado nas coordenadas de u_p em relação à base dada para V, podemos encontrar um vetor u em V, o qual está arbitrariamente perto para u_p, cada p em T. Assim pela continuidade da aplicação $x \to \sigma_x$, podemos assumir que σ_u esta arbitrariamente perto de σ_{u_p}, para cada p em T. Aplicamos o mesmo procedimento ao vetor v_p para obter um vetor v em V tal que a simetria σ_v está arbitrariamente perto de σ_{v_p}, para cada p em T. Pela continuidade da multiplicação em $L_{F_p}(V_p)$, podemos assumir que existe vetores u e v em V tal que

$$\|\sigma_u \sigma_v \sigma_u \sigma_v - \sigma_{u_p} \sigma_{v_p} \sigma_{u_p} \sigma_{v_p}\|_p < \varepsilon \text{ para todo } p \text{ e T.}$$

Seja $w = \sigma_v u$. Então $\sigma_w = \sigma_v \sigma_u \sigma_v$ e, portanto, temos um par de vetores u e w em V com $q(u) = q(w) \neq 0$, tal que

$$\|\sigma_u \sigma_w - \varphi_p\|_p < \varepsilon \text{ para todo } p \in T.$$ Logo, é suficiente

encontrar $\sigma \in O'(V)$ com $\|\sigma\|_{\mathfrak{p}} = -1$ para todo $\mathfrak{p} \in S-T$, e $\|\sigma - \zeta_u\zeta_w\|_{\mathfrak{p}} < \varepsilon$ para todo $\mathfrak{p} \in T$. Para isso consideremos o latice $L = Ox_1 + \ldots + Ox_n$ em V. Podemos assumir que u e w estão em L (se necessário podemos troca-los por λu e λv com um λ em O). Seja T_1 um subconjunto finito de S-T tal que $L_{\mathfrak{p}}$ é unimodular com $q(u) = q(w)$ uma unidade em cada $\mathfrak{p}$ em $S - (T_1 \cup T)$. Aplicando o teorema 3.2, podemos encontrar um vetor z em L, com $q(z) = q(u) = q(w)$, tal que z esta arbitrariamente perto de u para todo $\mathfrak{p}$ em T_1 e arbitrariamente perto de w, para todo $\mathfrak{p}$ em T. Assim pela continuidade da aplicação $x \to \zeta_x$ podemos então assumir que a simetria ζ_z esta arbitrariamente perto de ζ_w, para todo $\mathfrak{p} \in T$. Seja $\sigma = \zeta_u\zeta_z$. Então σ esta em $O'(V)$. Pela continuidade da multiplicação, podemos supor que σ que está arbitrariamente perto de $1_{V_{\mathfrak{p}}}$, para todo $\mathfrak{p}$ em T_1 e arbitrariamente perto de $\zeta_u\zeta_w$, para todo $\mathfrak{p}$ em T, ou seja,

$$\|\sigma\|_{\mathfrak{p}} = 1 \qquad \text{para todo } \mathfrak{p} \in T_1$$

$$\|\sigma - \zeta_u\zeta_w\| < \varepsilon \text{ para todo } \mathfrak{p} \in T$$

Resta somente provar que $\|\sigma\|_{\mathfrak{p}} = 1$ para todo $\mathfrak{p}$ em $S-(T_1 \cup T)$. Mas como u e v são elementos de $L_{\mathfrak{p}}$, para cada $\mathfrak{p}$, com $q(u) = q(z)$ uma unidade em $\mathfrak{p}$, concluimos que ζ_u e ζ_z são unidades de $L_{\mathfrak{p}}$, pela definição de simetria. Portanto $\sigma_{\mathfrak{p}}$ é uma unida

de de $L_{\mathfrak{p}}$. Logo $\|\sigma\|_{\mathfrak{p}} = 1$ para todo $\mathfrak{p} \in S-(T_1 \cup T)$.

2) Agora vamos supor que cada $\varphi_{\mathfrak{p}}$ seja um elemento arbitrário de $\Omega_n(V_{\mathfrak{p}})$, para $\mathfrak{p}$ em T. Podemos expressar na forma $\varphi_{\mathfrak{p}} = \psi_{\mathfrak{p}}^1 \ldots \psi_{\mathfrak{p}}^r$ onde ψ^i é um pequeno comutador em $O_n(V_{\mathfrak{p}})$. Podemos assumir que temos o mesmo número r, para todo $\mathfrak{p}$ em T, adicionando um "pequeno comutador" trivial quando necessário. Pela primeira parte podemos encontrar ψ^i em $O'(V)$ com ψ^i arbitrariamente perto de ψ^i , para cada $\mathfrak{p}$ em T e $\|\psi^i\|_{\mathfrak{p}} = 1$, para cada $\mathfrak{p}$ em S-T. Fazemos isso para cada i = 1,...,r. Portanto, $\sigma = \psi^1 \ldots \psi^r$ é o elemento desejado.

APLICAÇÕES

Encerraremos o capítulo aplicando Teorema da Aplicação Forte para as classes de isometria.

Teorema 3.3 - Seja V um espaço quadrático regular sobre o corpo global F com dim V $\geq$ 5 , S um conjunto indefinido de lugares para V e L um latice em V com respeito a S. Então $c\ell s^+L = spn^+L$ e $c\ell sL = spnL$.

Demonstração: Vamos provar que $c\ell sL = spnL$. A demonstração de $c\ell s^+L = spn^+L$ é análoga. Consideremos um latice L em spnL, então devemos provar que L está em $c\ell sL$. Pela definição de genus

espinorial, existem σ em $O(V)$ e $\sum_{\mathfrak{p}}$ em $O'(V_{\mathfrak{p}})$ tais que $K_{\mathfrak{p}} = \sigma_{\mathfrak{p}} \sum_{\mathfrak{p}} L_{\mathfrak{p}}$, para todo $\mathfrak{p} \in S$. Então $(\sigma^{-1}K)_{\mathfrak{p}} = \sum_{\mathfrak{p}} L_{\mathfrak{p}}$, para todo $\mathfrak{p}$ em S. Mas $\sigma^{-1}K \in cls K$. Portanto, podemos assumir que $\sigma = 1_V$. Assim $K_{\mathfrak{p}} = \sum_{\mathfrak{p}} L_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em S.

Fixemos uma base $x_1, \ldots x_n$ para V e sejam $\| \ \|_{\mathfrak{p}}$ a norma definida com respeito a esta base em $V_{\mathfrak{p}}$, para cada $\mathfrak{p}$ em S e M o latice $M = Ox_1 + \ldots + Ox_n$. Consideremos um subconjunto finito T de S tal que $K_{\mathfrak{p}} = L_{\mathfrak{p}} = M_{\mathfrak{p}}$, para todo $\mathfrak{p}$ em S-T. Portanto pelo teorema da aproximação forte para rotações, existe uma rotação ρ em $O'(V)$ tal que $\|\rho\|_{\mathfrak{p}} = 1$, para todo $\mathfrak{p} \in S-T$, com $\|\rho - \sum_{\mathfrak{p}}\|_{\mathfrak{p}}$ arbitrariamente pequeno, para todo $\mathfrak{p}$ em T. A primeira condição tem como resultado $(\rho L)_{\mathfrak{p}} = \rho_{\mathfrak{p}} M_{\mathfrak{p}} = K_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em S-T e da segunda condição resulta que podemos obter $\rho_{\mathfrak{p}} L_{\mathfrak{p}} = K_{\mathfrak{p}}$, para todo $\mathfrak{p}$ em T, pela escolha de uma boa aproximação na seleção de ρ. Então $(\rho L)_{\mathfrak{p}} = K_{\mathfrak{p}}$ para todo $\mathfrak{p}$ em S. Logo, $\rho L = K$ e $K \in cls L$.

c.q.d.

O teorema acima tem como consequência o seguinte resultado.

Teorema 3.4 - Sejam V um espaço quadrático regular, com $\dim V \geq 5$, sobre o corpo dos números racionais Q e S um conjunto indefinido de lugares para V. Se L e K são latices unimodulares,

então $c\ell s^{+}L = c\ell s^{+}K$.

Este é o famoso teorema de Meyer cuja prova data do inicio deste século. Uma prova simples de tal teorema é encontrada em $[S_r]$.

BIBLIOGRAFIA

B	BOREVICH	Number Theory Academic Press 1973.
L	S. LANG	Algebra, New York 1965.
O	O.T.O' MEARA	Introduction to quadratic forms, Springer Verlog, 1973.
Sr	J.P. SERRE	Cour's d' Aritmétique. Paris 1968.
Sr	J.P. SERRE	Corps Locaux. Paris 1969.
S	P. SAMUEL	Introdução a teoria dos números algébricos.