Teoria Algébrica dos números

Aula 10: Reticulados

Ramon M. Nunes

UFC

27 de março de 2020

Resumo da Aula

- Inteiros de Gauss

1. Reticulados
   - Definição e equivalências
   - Espaços euclidianos
   - Volume e covolume
   - Teorema de Minkowski
   - Exercícios propostos

Inteiros de Gauss

Lembre-se que ao estudar o anel $\mathbb{Z}[i]$, nós utilizamos, em nosso favor, a representação geométrica dos elementos de $\mathbb{Z}[i]$ como pontos de coordenadas inteiras em $\mathbb{R}^2$ (veja a figura no próximo slide).

Como veremos a seguir, isso nos dá um exemplo de reticulado em $\mathbb{R}^2$. Na aula de hoje, estudaremos as propriedades de reticulados em espaços vetoriais de dimensão finita. Essas propriedades serão utilizadas mais adiante para deduzir informações sobre corpos de números.

Inteiros de Gauss (cont.)

$$\mathbb{Z}[i] \simeq \mathbb{Z}^2 \subseteq \mathbb{R}^2 \simeq \mathbb{C}$$

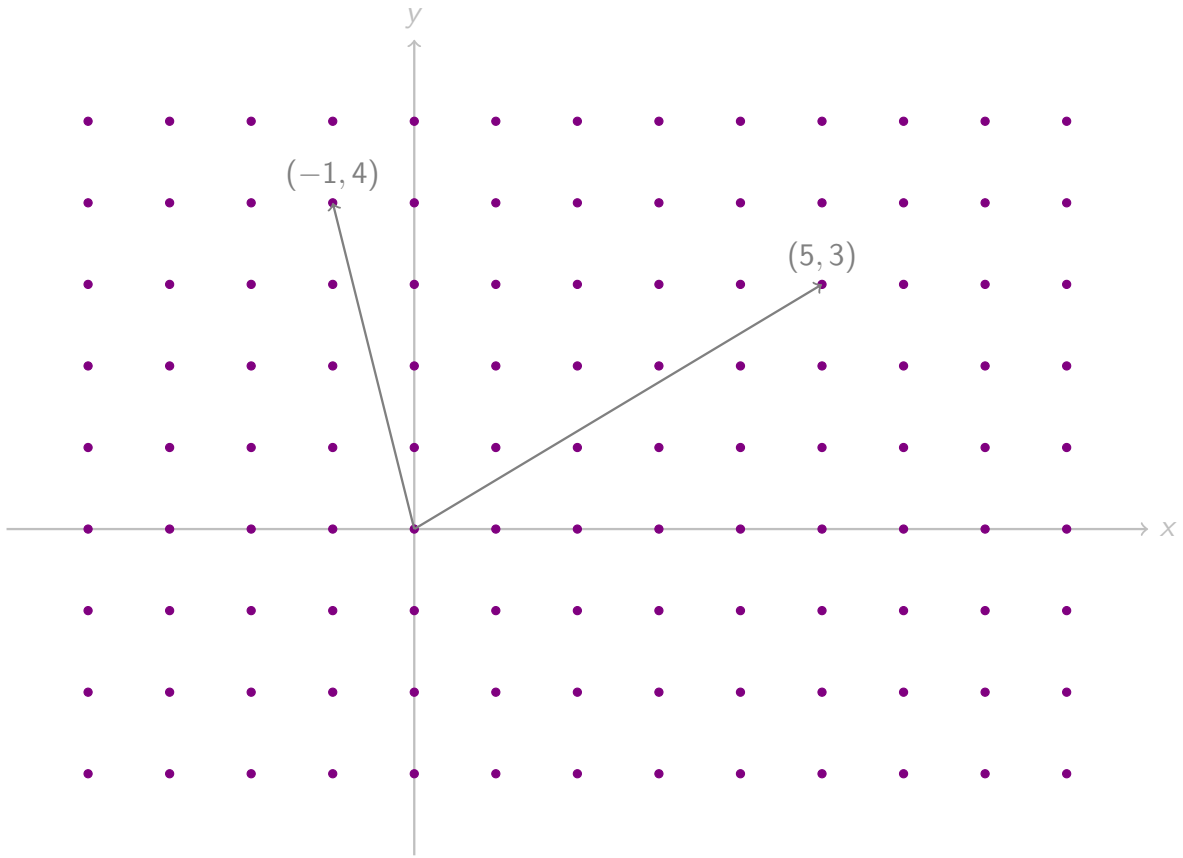

Figura: $Z[i]$ visto como um reticulado em $\mathbb{R}^2$

Definição de reticulado

Definição

Seja V um $\mathbb{R}$-espaço vetorial de dimensão n. Um *reticulado* em V é um subgrupo da forma

$$\Gamma = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \ldots \mathbb{Z}v_m,$$

onde $v_1, v_2, \ldots v_m$ são linearmente independentes. A m-upla $v_1, v_2, \ldots v_m$ é dita uma *base* de Γ e o conjunto

$$\Phi := \{x_1 v_1 + \ldots + v_m;\ x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

é chamado de *domínio fundamental* do reticulado Γ. Por fim, o reticulado é dito *completo* quando sua dimensão for igual à de V. *i.e.* $m = n$.

OBS: A completude de um reticulado é equivalente ao fato de que $V = \Gamma + \Phi$, onde, é claro, $\Gamma + \Phi := \{\gamma + \phi;\ \gamma \in \Gamma, \phi \in \Phi\}$.

Reticulado, definição alternativa

A definição acima de reticulado depende da escolha de uma base, o que é muito concreto. Porém, assim como para espaços vetoriais, será importante obter uma definição mais intrínseca, que independa da base.

É fácil ver que todo reticulado é um subgrupo finitamente gerado de $\mathbb{R}$[1]. Porém, nem todo subgrupo finitamente gerado de $\mathbb{R}$ é um reticulado.

e.g. $\Gamma = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ é um $\mathbb{Z}$-submódulo de $\mathbb{R}$ mas não é reticulado pois não existe $v \in \mathbb{R}$ tal que $v\mathbb{R} = \Gamma$ (exercício!).

Analisando o exemplo de $Z[i] \subset \mathbb{C}$, vemos que além de ser um subgrupo, este reticulado possui outra propriedade. A saber: $Z[i]$ é um subgrupo *discreto* de $\mathbb{C}$. A definição de subgrupo discreto setrá dada no próximo slide.

[1] todos os grupos são considerados aqui com respeito à adição

Definição alternativa (cont.)

Definição

Um subgrupo Γ de $\mathbb{R}^n$ (ou mais geralmente de um grupo topológico) é *discreto* se para todo $\gamma \in \Gamma$, existir um aberto U_γ cujo único elemento de Γ em U seja γ.

OBS: Dado qualquer espaço vetorial V e um isomorfimo linear $T : V \to \mathbb{R}^n$, podemos transferir a topologia euclidiana de $\mathbb{R}^n$ para V. Além disso, a topologia independe do isomorfismo T. Seja Γ um

reticulado e $\{v_1, v_2, \ldots v_m\}$ uma base de Γ que completaremos para uma base $\{v_1, v_2, \ldots v_n\}$ de V. Seja $\gamma = a_1 v_1 + \ldots + a_m v_m$, $a_i \in \mathbb{Z}$ um elemento de Γ e tome

$$U_\gamma := \{x_1 v_1 + \ldots + x_n v_n;\ |x_i - a_i| < 1\}.$$

Esse conjunto é aberto para a topologia de V descrita acima. Logo, podemos concluir que Γ é discreto.

Definição alternativa (cont.)

Pelo que vimos, todo reticulado de um $\mathbb{R}$-espaço vetorial de dimensão finita V é um subgrupo discreto de V. Veremos a seguir que a recíproca também é verdadeira.

Proposição

Um subgrupo Γ de um $\mathbb{R}$-espaço vetorial de dimensão finita V é um reticulado se, e somente se, ele é discreto.

Prova: Basta provar que todo subgrupo discreto é um reticulado. Seja $\Gamma \subseteq V$ um subgrupo discreto.

Vale então que Γ é um conjunto fechado. De fato, suponha que exista $y \notin \Gamma$ e uma sequência $(x_n)_n$, $x_n \in \Gamma$ tal que $x_n \to y$. Segue então que a sequência $(\tilde{x_n})_n$, $\tilde{x_n} = x_n - x_{n+1}$ é uma sequência de elementos de Γ convergindo para $0 \in \Gamma$, o que é uma contradição.

Definição alternativa (cont.)

Seja agora $V_0 \subseteq V$ o subespaço gerado pelos elementos de Γ e seja $\{u_1, \ldots, u_m\}$ uma base de V_0 tal que $u_i \in \Gamma$ para $i = 1, \ldots, m$. Considere o reticulado

$$\Gamma_0 := \mathbb{Z}u_1 + \mathbb{Z}u_2 + \ldots \mathbb{Z}u_m \subseteq \Gamma.$$

Afirmamos que o índice $(\Gamma : \Gamma_0)$ é finito. Para ver isto, seja $\{\gamma_i\}_{i \in I}$ um sistema completo de representates para Γ/Γ_0. Como Γ_0 é completo em V_0, podemos tomar os γ_i de modo que

$$\gamma_i \in \Phi_0, \text{ para todo } i \in I,$$

Onde Φ_0 é o domínio fundamental de Γ_0 com respeito à base $\{u_1, \ldots, u_m\}$. Veja que como $\overline{\Phi_0}$ é compacto e Γ é discreto, segue que I é finito.

Definição alternativa (cont.)

Seja agora $q = (\Gamma : \Gamma_0)$. Segue do teorema de Lagrange que $q\Gamma \subseteq \Gamma_0$. Em outras palavras

$$\Gamma \subseteq \frac{1}{q}\Gamma = \mathbb{Z}\frac{u_1}{q} + \mathbb{Z}\frac{u_2}{q} + \ldots \mathbb{Z}\frac{u_m}{q} \subseteq .$$

Pela caracterização dos grupos abelianos finitamente gerados, segue que Γ é um grupo abeliano livre de posto $r \leq m$. Porém, como $\Gamma_0 \subset \Gamma$, temos que $r = m$. Seja $\{v_1, \ldots, v_m\}$ uma $\mathbb{Z}$-base de Γ. Como V_0 é gerado por Γ e tem dimensão m. Segue que $\{v_1, \ldots, v_m\}$ é linearmente independente. Logo, Γ é um reticulado.

A seguir, provaremos um critério para a completude de um reticulado que se provará bastante útil.

Critério para completude

Lema

Um reticulado Γ de um $\mathbb{R}$-espaço vetorial de dimensão finita V é completo se, e somente se, existe um conjunto limitado $M \subseteq V$ tal que $V = \Gamma + M$.

Prova: Se Γ é um reticulado completo, então podemos tomar M como sendo o domínio fundamental com respeito a uma base de Γ.

Reciprocamente, suponha que M é um conjunto limitado e $\Gamma + M = V$. Seja V_0 o subespaço vetorial de V gerado por Γ. Seja $v \in V$. Como $\Gamma + M = V$, então para todo $n \in \mathbb{Z}_{>0}$, temos

$$nv = \gamma_n + \mu_n,\ \gamma_n \in \Gamma,\ \mu_n \in M.$$

Como M é limitado, segue que $\lim_n \frac{\mu_n}{n} = 0$. Donde concluímos que $v = \lim_n \frac{\gamma_n}{n} \in V_0$, pois V_0 é fechado. Logo, $V = V_0$.

Espaços euclidianos

Nesse e nos próximos quadros, prepararemos os terreno para a prova do teorema de Minkowski, que é o teorema principal sobre reticulados que nos será crucial na prova dos teoremas de finitude sobre o grupo de classes e o grupo das unidades do anel de inteiros de um corpo de números.

Definição

Um *espaço euclidiano* é um $\mathbb{R}$-espaço vetorial de dimensão finita V, munido de uma forma bilinear simétrica e positiva-definida

$$\langle\ ,\ \rangle : V \times V \to \mathbb{R}.$$

Mais pragmáticamente, um espaço euclidiano é, a menos de uma transformação linear, o mesmo que o espaço $\mathbb{R}^n$ com o produto interno usual

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle := x_1 y_1 + \ldots + x_n y_n.$$

Noção de volume

Em um espaço euclidiano V, temos uma noção de volume e mais precisamente de uma medida de Lebesgue, equivalente à medida $dx_1 dx_2 \dots dx_n$ em $\mathbb{R}^n$. A noção de volume assim obtida é tal que se $\mathcal{B} = \{v_1, \dots, v_n\}$ é uma base V e seΦ é o paralelepípedo gerado pelos vetores de $\mathcal{B}$, dado por

$$\Phi = \{x_1 v_1 + \dots x_n v_n;\ x_i \in \mathbb{R},\ 0 \leq x_i < 1\},$$

então Φ tem volume 1 se $\mathcal{B}$ é ortonormal[2] e, mais geralmente,

$$\text{vol}(\Phi) = |\,\text{vol}\, A|,$$

onde A é a matriz de mudança de base entre $\mathcal{B}$ e uma base ortonormal. Sem muito esforço, podemos mostrar que vale a relação mais intrínsseca

$$\text{vol}(\Phi) = |\det(\langle v_i, v_j\rangle)_{ij}|^{1/2}.$$

[2] $\{v_1, \dots, v_n\}$ é ortonormal se $\langle v_i, v_j\rangle = \delta_{ij}$

Covolume

Seja agora Γ um reticulado completo no espaço euclidiano V, definimos então seu covolume como sendo o volume de um domínio fundamental para Γ:

$$\text{covol}(\Gamma) = \text{vol}(\Phi).$$

Para ver que este volume é independe da base escolhida, basta ver que a matriz de mudança de base entre duas bases de Γ é uma matriz inteira de inversa inteira e portanto possui determinante ± 1.

Finalmente, antes de enunciar o teorema de Minkowski, precisamos introduzir mais alguns conceitos.

Dado $X \subseteq V$, dizemos que X é *centralmente simétrico* se para todo x em X, temos que $-x$ também está em X. Dizemos que X é *onvexo* se para todos x e y em X, temos $tx + (1-t)y \in X$ para todo $t \in [0,1]$.

Teorema de Minkowski

No resto desta, concentramos nossos esforços em provar o seguinte resultado:

Teorema

Seja Γ um reticulado completo de um espaço euclidiano V e seja $X \subseteq V$ um conjunto centralmente simétrico e convexo. Suponha que

$$\mathrm{vol}(X) > 2^n \,\mathrm{covol}(\Gamma).$$

Então X contém pelo menos um elemento não-nulo do reticulado Γ.

Prova: Primeiro mostraremos que o teorema segue se encontrarmos γ_1 e γ_2 em Γ, distintos e tais que

$$\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_1 + \frac{1}{2}X\right) \neq \emptyset.$$

Teorema de Minkowski (cont.)

De fato, se tivermos um ponto na interseção acima, isto significa que existem x_1 e x_2 em X tais que

$$\gamma_1 + \frac{x_1}{2} = \gamma_2 + \frac{x_2}{2} \Leftrightarrow \gamma_1 - \gamma_2 = \frac{1}{2}(-x_1) + \frac{1}{2}x_2.$$

Como X é centralmente simétrico e convex, o ponto $\frac{1}{2}(-x_1) + \frac{1}{2}x_2$ está em X. Como Γ é um reticulado e $\gamma_1 \neq \gamma_2$, temos a conclusão do teorema.

Suponha agora que os conjuntos $\gamma + \frac{1}{2}X$ são todos distintos e seja

$$Y_\gamma := \left(\gamma + \frac{1}{2}X\right) \cap \Phi.$$

Segue que

$$\mathrm{vol}\,(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}(Y_\gamma).$$

Teorema de Minkowski (cont.)

Note agora que como translações deixam volumes invariantes, temos que

$$\mathrm{vol}(Y_\gamma) = \mathrm{vol}\left((-\gamma + \Phi) \cap \frac{1}{2}X\right).$$

Lembre agora que ao variar $\gamma \in \Gamma$, os conjuntos $\gamma + \Phi$ recobrem (sem se sobrepor) o espaço V. Temos, portanto, que

$$\mathrm{vol}\,(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}(Y_\gamma) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\,\mathrm{vol}(X),$$

o que gera uma contradição e conclui a prova do teorema.

Exercícios Propostos

Para treinar, sugiro os seguintes exercícios do livro do Neukirch:

Seção 4: exercćicios 1, 3 e o exercício proposto nas notas.

Fim!