Miscelánea Matemática **79** (2024) 5-10 SMM

**DOI:** https://doi.org/10.47234/mm.7902

# Sobre los subgrupos de $(\mathbb{R}, +)$

Santos Hernández Hernández
Unidad Académica de Matemáticas
Universidad Autónoma de Zacatecas
shh@uaz.edu.mx

## 1.

Consideremos el sistema de los números reales. En particular, consideremos el grupo $(\mathbb{R}, +)$, es decir, $\mathbb{R}$ con la estructura de grupo aditivo. Sea $(G, +) \leqslant (\mathbb{R}, +)$ un subgrupo, es decir, $G \subseteq \mathbb{R}$ tal que si $a, b \in G$ entonces $a - b \in G$. Como es costumbre, abusaremos de la notación y, para decir que $(G, +)$ es un subgrupo de $(\mathbb{R}, +)$ solo escribiremos $G$ es subgrupo de $\mathbb{R}$ o $G \leqslant \mathbb{R}$. Por ejemplo, $(\mathbb{Z}, +)$ y $(\mathbb{Q}, +)$ son subgrupos de $\mathbb{R}$. También lo es el siguiente subconjunto: sea $d > 0$ un entero que no es un cuadrado perfecto y consideremos el subconjunto

$$\mathbb{Z}[\sqrt{d}] := \{m + n\sqrt{d} \,:\, m, n \in \mathbb{Z}\},$$

donde $\sqrt{d}$ denota la única raíz positiva[1] de $d$ en $\mathbb{R}$. Como

$$(m + n\sqrt{d}) - (p + q\sqrt{d}) = (m - p) + (n - q)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

si $m, n, p, q \in \mathbb{Z}$, se tiene que $\mathbb{Z}[\sqrt{d}]$ es un subgrupo de $\mathbb{R}$. Notamos por ejemplo que $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}]$ y $\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$: en el primer caso escribimos cada elemento de $m \in \mathbb{Z}$ como $m + 0 \cdot \sqrt{d}$; en el segundo, $0 + 1 \cdot \sqrt{d}$.

Por otro lado, el subgrupo $\mathbb{Z}$ tiene la característica de que dado $n \in \mathbb{Z}$, existe un intervalo de $\mathbb{R}$ que solo contiene a tal elemento, por ejemplo, $(n-(1/2), n+(1/2))$. Contrario a $\mathbb{Q}$, que dado $r \in \mathbb{Q}$ cada subintervalo de $\mathbb{R}$ que contiene a $r$ tiene la propiedad de intersectar a $\mathbb{Q}$ en un punto $s$ distinto de $r$. Esto se conoce como '$\mathbb{Q}$ es denso en $\mathbb{R}$'. En este sentido, ¿cómo se comporta $\mathbb{Z}[\sqrt{d}]$?. Parte de la finalidad de este escrito es exponer un poco de este tipo de comportamiento de subgrupos de $\mathbb{R}$.

Recordemos y formalicemos los conceptos del párrafo anterior. Un subconjunto $T \subseteq \mathbb{R}$ se dice que es *abierto* si para cada $a \in T$ existe

*Palabras clave*: Subgrupos de $\mathbb{R}$, subconjuntos densos, discretos, puntos aislados.

[1] Mediante $\sqrt{x}$, donde $x$ es un número real $> 0$, denotamos al único número real positivo cuyo cuadrado es $x$. Este número real existe y es el supremo del conjunto $\{t \in \mathbb{R} : t > 0 \text{ y } t^2 < x\}$.

un intervalo abierto $(b, c)$ de $\mathbb{R}$ tal que $a \in (b, c) \subseteq T$. A la familia de todos estos subconjuntos de $\mathbb{R}$ se le conoce como la *topología usual* de $\mathbb{R}$. Para establecer los conceptos que aquí se usan, es suficiente considerar intervalos abiertos; el lector puede verificar que de hecho estos son equivalentes a los mismos conceptos establecidos con la topología usual de $\mathbb{R}$. Dado $a \in \mathbb{R}$ denotamos mediante $\mathcal{I}_a$ a toda la familia de intervalos abiertos de $\mathbb{R}$ que contienen a $a$. Dado $A \subseteq \mathbb{R}$ se define la *cerradura* de $A$ mediante

$$\overline{A} := \{a \in \mathbb{R} : \text{para todo } I \in \mathcal{I}_a,\ I \cap A \neq \emptyset\}.$$

Decimos que $A$ es *denso* si $\overline{A} = \mathbb{R}$. Ahora, un elemento $a \in A$ se dice que es *aislado* si existe $I \in \mathcal{I}_a$ tal que $I \cap A = \{a\}$. Se dice que $A$ es *discreto* si cada uno de sus elementos es aislado. Con este lenguaje notamos que $\mathbb{Z}$ es discreto y que $\mathbb{Q}$ es denso. Como dijimos anteriormente, estos subconjuntos son subgrupos de $(\mathbb{R}, +)$; sin embargo, hay subconjuntos que son densos sin ser subgrupos de $\mathbb{R}$ por ejemplo $\mathbb{R} \setminus \mathbb{Q}$, pues $1 - \sqrt{2}, \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ pero su suma $1 \notin \mathbb{R} \setminus \mathbb{Q}$. En este escrito se presenta el siguiente resultado:

**Teorema 1.1.** *Si $G$ es un subgrupo de $\mathbb{R}$ entonces $G$ es denso o es discreto. Además, en el caso de que $G$ es discreto y $G \neq \{0\}$ entonces existe $\alpha \in G$, $\alpha > 0$ tal que $G = \mathbb{Z}\alpha$.*

Como pretexto, se presenta la demostración de la irracionalidad de raíces cuadradas de números naturales que no son cuadrados perfectos dada por T. Estermann [3]; luego, con este hecho, se aplica el teorema 1.1 para concluir que subgrupos como $\mathbb{Z}[\sqrt{d}]$ son densos en $\mathbb{R}$.

Nada de lo que aquí se escribe es en modo alguno original. Los cálculos que aquí se presentan para la demostración del teorema 1.1 están basados en [4] (véase también [1]). El teorema 1.1 se puede encontrar también en [2]. El lenguaje analítico de los números reales como un campo ordenado con la propiedad de la mínima cota superior, así como las propiedades de los números naturales que se usan en este escrito, se puede encontrar en [5].

## 2.

En esta sección se demuestra el teorema 1.1. Se prueba primero la primera parte. La idea principal se basa en que el cero, que está en $G$, es un punto aislado de $G$ o no. Sea pues $G$ un subgrupo de $(\mathbb{R}, +)$. Si $G$ es un subgrupo trivial es decir $G = \{0\}$ o $G = \mathbb{R}$ no hay nada que probar porque en particular, el primero es discreto y el segundo es denso. Supongamos entonces que $G$ es no trivial, en particular $G \neq \{0\}$.

Consideremos el elemento $0 \in G$. Este tiene dos posibilidades: o es un punto aislado o no lo es.

Analicemos el primer caso, esto es, que 0 es un punto aislado de $G$. Se demostrará entonces que $G$ es discreto. Por definición pues, existe un intervalo abierto $(a, b)$ que contiene a 0 tal que $(a, b) \cap G = \{0\}$. Sea $g \in G$ cualquier otro elemento de $G$, lo fijamos y consideramos el intervalo $(a + g, b + g)$. Notamos que, como $a < 0 < b$ se tiene que $a+g < g < b+g$. Es decir, $g$ pertenece al intervalo abierto $(a+g, b+g)$. Ahora, sea $h \in G \cap (a + g, b + g)$. En particular, $a + g < h < b + g$ que implica $a < h - g < b$. Esto es, $h - g \in (a, b)$. Como $G$ es un subgrupo y $h, g \in G$ se tiene que $h - g \in G$. Así, $h - g \in G \cap (a, b)$. Como esta intersección solo consta del elemento 0, se tiene que $g - h = 0$ o bien $g = h$. Por lo tanto concluimos que $G \cap (a + g, b + g) = \{g\}$ y así, $g$ es aislado en $G$. Como $g \in G$ fue arbitrario, se tiene que todo elemento de $G$ es aislado y por lo tanto $G$ es discreto.

Estudiemos ahora el segundo caso, es decir, que 0 no es aislado en $G$. Por lo tanto, para todo intervalo abierto $(a, b)$ que contiene a 0 se tiene que existe $g \in G \cap (a, b)$ con $g \neq 0$. En este caso se va a probar que $G$ es denso, es decir, se va a probar que para todo intervalo abierto $(c, d)$ se tiene que $(c, d) \cap G \neq \emptyset$.

Observemos lo siguiente: dado $\varepsilon > 0$ existe $g \in G \cap (-\varepsilon, \varepsilon)$ con $g > 0$. En efecto, como $(-\varepsilon, \varepsilon)$ es un intervalo abierto que contiene a 0, se sigue que existe $g \in G \cap (-\varepsilon, \varepsilon)$ con $g \neq 0$. Ahora, si $g < 0$ entonces $-g > 0$ y $-g \in G$ pues $G$ es subgrupo. Además, como $-\varepsilon < g$ se tiene que $-g < \varepsilon$. Esto prueba la observación.

Sea ahora $(c, d)$ cualquier intervalo abierto donde $c < d$ y sea $0 < \varepsilon \leqslant d - c$. Por la observación precedente, existe $g \in G \cap (-\varepsilon, \varepsilon)$ con $g > 0$. La afirmación es que existe $n \in \mathbb{N}$ tal que $ng \in (c, d)$. Supongamos que no es el caso. Por la propiedad arquimediana[2] y el principio del buen orden[3] de $\mathbb{R}$ y $\mathbb{N}$, respectivamente, existe $N \in \mathbb{N}$ mínimo tal que $d < Ng$. Esto implica que $(N - 1)g \leqslant d$. Como hemos supuesto que no hay ningún múltiplo de $g$ en $(c, d)$ se tiene que o bien $(N - 1)g \leqslant c$ o bien $(N - 2)g \leqslant c$, dependiendo de si $(N - 1)g < d$ o $(N - 1)g = d$, respectivamente. Así, se tiene $(N - 2)g \leqslant c < d = (N - 1)g$ o bien $(N - 1)g \leqslant c < d < Ng$. En ambos casos, tomando distancia o resolviendo las respectivas desigualdades se infiere que

$$\varepsilon \leqslant d - c \leqslant g < \varepsilon,$$

que es una contradicción. Por lo tanto, existe $n \in \mathbb{N}$ tal que $ng \in (c, d)$. Como $G$ es grupo $ng \in G$. Así $G \cap (c, d) \neq \emptyset$, como se quería demostrar.

[2]Dados $a, b \in \mathbb{R}$ con $a > 0$, existe $n \in \mathbb{N}$ tal que $b < na$.

[3]Todo subconjunto no vacío de números naturales tiene elemento mínimo.

Estudiamos ahora la segunda parte del enunciado del teorema 1.1. Sea $G \neq \{0\}$ un subgrupo discreto y consideremos

$$\alpha = \text{ínf}\{g \in G \,:\, g > 0\}.$$

Como $G \neq \{0\}$, existe $g \in G$ con $g \neq 0$. Si $g < 0$ entonces $-g > 0$ y $-g \in G$ pues $G$ es subgrupo. Por lo tanto el subconjunto de $G$, $G_+ := \{g \in G \,:\, g > 0\} \neq \emptyset$ y por lo tanto $\alpha$ existe. Claramente $\alpha \geqslant 0$, pues 0 es una cota inferior de tal conjunto. Si $\alpha = 0$, consideramos cualquier intervalo que lo contenga, digamos $(a, b)$. En particular, $a < 0 < b$. Por ser 0 la máxima cota inferior de $G_+$ y $b > 0$, se tiene que existe $g \in G_+$ tal que $0 < g < b$. Esto implica que $g \in G \cap (a, b)$ con $g > 0$. Por lo tanto, todo intervalo abierto $(a, b)$ que contiene a 0, contiene también puntos de $G$ que son distintos de cero. Como $0 \in G$, esto significa que 0 no es punto aislado de $G$, lo que contradice que $G$ es discreto. Por lo tanto $\alpha > 0$.

Vamos a demostrar ahora que $\alpha \in G$. Se probará que existe $a \in G$ tal que $\alpha = a$. En efecto, sabemos que $\alpha > 0$ y sabemos que como $0 \in G$ es aislado, existe un intervalo $(b, c)$ que contiene a 0 tal que $G \cap (b, c) = \{0\}$. Sean $\tau_0 := \text{máx}\{-\alpha, b\}$ y $\tau_1 := \text{mín}\{\alpha, c\}$. Notemos que $b \leqslant \tau_0 < 0 < \tau_1 \leqslant c$ y que por lo tanto $G \cap (\tau_0, \tau_1) = \{0\}$. Como $\tau_1 > 0$ entonces $\alpha < \alpha + \tau_1$ y, como $\alpha$ es máxima cota inferior de $G_+$, existe $a \in G_+$ tal que $\alpha \leqslant a < \alpha + \tau_1$. Afirmamos que $\alpha = a$. En efecto, si no, es decir, si $\alpha < a$, existe $g \in G_+$ tal que $\alpha \leqslant g < a$. Como $a < \alpha + \tau_1$ se concluye que $0 < a - g < \alpha + \tau_1 - \alpha = \tau_1$. Pero como $a - g \in G$, la conclusión anterior contradice que $G \cap (\tau_0, \tau_1) = \{0\}$. Por lo tanto $\alpha = a \in G$.

Finalmente, sea $g \in G$ y consideremos primero el caso $g > 0$. Por la propiedad arquimediana de $\mathbb{R}$ y el principio del buen orden de $\mathbb{N}$, existe $m \in \mathbb{N}$ mínimo tal que $g < m\alpha$. Entonces $(m-1)\alpha \leqslant g$. Si $q := m - 1$ se tiene entonces que $0 \leqslant g - q\alpha < \alpha$. Como $G$ es subgrupo y $\alpha \in G$ se tiene que $g - q\alpha \in G$. Recordemos que $\alpha$ es el ínfimo de los elementos positivos de $G$; por lo tanto, si $g - q\alpha > 0$ entonces se tendría $g - q\alpha < \alpha \leqslant g - q\alpha$, que es absurdo. Por lo tanto $g - q\alpha = 0$ o $g = q\alpha$. Si $g < 0$ consideramos $-g > 0$ y, como hemos probado que existe $q \in \mathbb{N}$ tal que $-g = q\alpha$ se tiene que $g = r\alpha$ con $r = -q \in \mathbb{Z}$. Por lo tanto, $G \subseteq \mathbb{Z}\alpha$. Como $\alpha \in G$, $-\alpha \in G$ y por lo tanto $n\alpha \in G$ para todo entero $n \in \mathbb{Z}$. Así, $\mathbb{Z}\alpha \subset G$. Combinando ambas contenciones se concluye que $G = \mathbb{Z}\alpha$.

## 3.

Se presenta ahora la demostración de T. Estermann [3] sobre la irracionalidad de las raíces cuadradas de los números enteros que no son un cuadrado perfecto. Supongamos pues que $d \in \mathbb{N}$ y que no es un cuadrado perfecto, es decir, no es de la forma $q^2$ con $q \in \mathbb{N}$. Lo primero que observamos es que $\sqrt{d} \notin \mathbb{N}$ (recordemos que $\sqrt{d}$ denota el único número real positivo cuyo cuadrado es $d$). En efecto, sea $n \in \mathbb{N}$ el mínimo tal que $d < n^2$. Por lo tanto $(n-1)^2 \leqslant d$. Sin embargo, la igualdad no se puede dar porque $d$ no es un cuadrado perfecto. Por lo tanto $(n-1)^2 < d < n^2$, de donde $n - 1 < \sqrt{d} < n$. Ahora, como no existen números enteros entre dos números naturales consecutivos se tiene que $\sqrt{d} \notin \mathbb{N}$.

Consideramos pues $d$ como antes y supongamos que $\sqrt{d} \in \mathbb{Q}$ es decir existen $a, b \in \mathbb{Z}$, $b \neq 0$ tal que

$$\sqrt{d} = \frac{a}{b}.$$

Como $\sqrt{d} > 0$, sin pérdida de generalidad suponemos que $a, b$ son positivos, es decir, $a, b \in \mathbb{N}$. Se obtiene entonces que $b\sqrt{d} = a \in \mathbb{N}$. Por lo tanto existe $m \in \mathbb{N}$ mínimo tal que $m\sqrt{d} \in \mathbb{N}$. Sea ahora $p$ la parte entera de $\sqrt{d}$. Sabemos que $p$ es el único número entero (y en este caso, positivo) que satisface las desigualdades

$$p \leqslant \sqrt{d} < p + 1.$$

Notamos que la primera desigualdad no puede ser una igualdad porque demostramos hace un momento que $\sqrt{d}$ no es un entero. Por lo tanto se tiene

$$p < \sqrt{d} < p + 1.$$

Ahora, multiplicando por $m$ se obtiene que

$$mp < m\sqrt{d} < mp + m.$$

Como $m\sqrt{d} \in \mathbb{N}$, la primera desigualdad implica que $m\sqrt{d} - mp \in \mathbb{N}$. La segunda desigualdad implica que $m\sqrt{d} - mp < m$. Ahora,

$$0 < (m\sqrt{d} - mp)\sqrt{d} = md - p(m\sqrt{d}).$$

Por lo tanto, la última expresión es un número entero positivo, es decir, pertenece a $\mathbb{N}$. Como $m\sqrt{d} - mp$ es un número natural $< m$, lo anterior contradice la minimalidad de $m$. Por lo tanto $\sqrt{d} \notin \mathbb{Q}$.

## 4.

Para concluir, veamos cómo es $\mathbb{Z}[\sqrt{d}]$ donde $d \in \mathbb{N}$ no es un cuadrado perfecto. Si este no fuera denso, como es no trivial sería discreto por el teorema 1.1 y por lo tanto de la forma $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}\alpha$ con $\alpha \in \mathbb{Z}[\sqrt{d}]$, $\alpha > 0$. Escribamos $\alpha = m + n\sqrt{d}$ para algunos $m, n \in \mathbb{Z}$ y observamos que $m$ y $n$ no pueden ser cero simultáneamente. Además, como $1 \in \mathbb{Z}[\sqrt{d}]$ entonces $1 = \ell(m + n\sqrt{d})$ de donde se obtiene que $m \neq 0$, pues de otro modo, se deduce que $\sqrt{d}$ es racional, contrario a la sección precedente. Tampoco $n$ puede ser cero pues como $\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $\sqrt{d} = p(m + n\sqrt{d})$, con $p \in \mathbb{Z}$. De ser $n = 0$ se infiere que $\sqrt{d}$ es un entero, contrario nuevamente a la sección anterior. Así, elevando al cuadrado la igualdad para $\sqrt{d}$ y realizando los cálculos aritméticos se llega a que

$$\sqrt{d} = \frac{d - p^2(m^2 + dn^2)}{2p^2mn},$$

que implica que $\sqrt{d}$ es racional, y nuevamente obtenemos una contradicción. Por lo tanto, $\mathbb{Z}[\sqrt{d}]$ es denso en $\mathbb{R}$.

## Agradecimientos

El autor agradece a los revisores por la lectura cuidadosa y por sus valiosas observaciones y sugerencias que ayudaron a mejorar la presentación de este escrito. También agradece a L. Jiménez Sandoval por la amable invitación a redactar este trabajo.

## Bibliografía

[1] H. Abels y A. Manoussos, «Topological generators of abelian lie groups and hypercyclic finitely generated abelian semigroups of matrices», *Adv. in Math.*, vol. 229, núm. 3, 2012, 1862–1872, https://doi.org/10.1016/j.aim.2011.11.015.

[2] J. O. Araujo y L. B. Fernández, «Problemas con subgrupos discretos y subgrupos densos», *Bol. Asoc. Mat. Venezolana*, vol. 13, núm. 2, 2006, 187–215.

[3] T. Estermann, «The irrationality of $\sqrt{2}$», *The Mathematical Gazette*, vol. 59, núm. 408, 1975, 110, https://doi.org/10.2307/3616647.

[4] J. Singh, «Subgroups of the additive group of real line», *arXiv:1312.7067v3 [math.NT]*, 2014, 1–5, https://doi.org/10.48550/arXiv.1312.7067.

[5] K. L. Stromberg, *Introduction to classical real analysis*, Wadsworth, 1981.