Körper, in denen -1 nicht Quadratelement ist

Autor(en): **Steiner, H.-C.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **22 (1967)**

Heft 5

PDF erstellt am: **22.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-25361

ELEMENTE DER MATHEMATIK
Revue de mathématiques élémentaires – Rivista di matematica elementare
Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts
Publiziert mit Unterstützung des Schweizerischen Nationalfonds
zur Förderung der wissenschaftlichen Forschung

El. Math. Band XXII Heft 5 Seiten 97–120 10. September 1967

Körper, in denen -1 nicht Quadratelement ist

1. In angeordneten Körpern $A = (M, +, \cdot, <)$ führt man den *Quadratwurzelterm* $\sqrt{x}$ und damit die Quadratwurzelfunktion $x \to \sqrt{x}$ bekanntlich gemäss

$$\sqrt{x} =_{Df} \text{dasjenige } y, \text{ für das } y^2 = x \text{ und } y > 0 \tag{1}$$

ein. Dieser Term ist auf der Menge Q aller Quadratelemente von A definiert, und es gilt die Formel

$$\sqrt{a}\sqrt{b} = \sqrt{ab} \text{ für alle } a, b \in Q\,. \tag{2}$$

Bei der Definition (1) wie bei der Ableitung von (2) wird von den *Anordnungseigenschaften* von $<$ Gebrauch gemacht, die wir kurz in Erinnerung bringen:
Für alle $a, b, c \in M$:

(A_1) Entweder $a < b$ oder $a = b$ oder $b < a$,
(A_2) Wenn $a < b$ und $b < c$, so $a < c$,
(A_3) Wenn $a < b$, so $a + c < b + c$,
(A_4) Wenn $a < b$ und $0 < c$, so $ac < bc$.

Die Rolle, die die Anordnung in (1) spielt, besteht offensichtlich darin, dass durch die Bedingung $y \geqslant 0$ von den beiden für $x \in Q$ und $x \neq 0$ existierenden Lösungen von $y^2 = x$ genau eine ausgesondert wird. Mit y ist ja stets auch $-y$ eine Lösung. Ist $x \neq 0$, so ist auch $y \neq 0$, also nach (A_1) entweder $y > 0$ oder $y < 0$. Nach (A_3) ist im ersten Falle $-y < 0$, im zweiten $-y > 0$.

Bei der Ableitung von (2) greifen wir zunächst auf (1) zurück. Es sei

$$\sqrt{a} = c, \text{ also } c^2 = a \text{ und } c \geqslant 0, \qquad \sqrt{b} = d, \text{ also } d^2 = b \text{ und } d \geqslant 0\,.$$

Dann ist $ab = c^2d^2 = (cd)^2$. Gemäss (A_4) folgt nun aber aus $c \geqslant 0$ und $d \geqslant 0$, dass $cd \geqslant 0$. Wir können deshalb gemäss (1) von der letzten Gleichung zu $\sqrt{a}\sqrt{b} = cd = \sqrt{ab}$ übergehen.

2. Bekanntlich lassen sich nicht alle Körper anordnen. Ein notwendiges Kriterium für die Existenz einer den Axiomen (A_1) bis (A_4) genügenden Relation $<$ in einem (hier stets kommutativ vorausgesetzten) Körper $K = (M, +, \cdot)$ lautet: -1 ist nicht Quadratelement in K. Existiert nämlich eine Anordnung $<$, so sind in bezug auf $<$ alle von 0 verschiedenen Quadratelemente von K positiv, während nicht zugleich a als auch $-a$ positiv sein können. Der Körper der komplexen Zahlen zum Beispiel lässt sich demgemäss nicht anordnen.

Unabhängig davon lassen sich alle Körper mit von 0 verschiedener *Charakteristik*, also insbesondere die endlichen Körper, nicht anordnen. Die Charakteristik $\chi(K)$ eines Körpers $K = (M, +, \cdot)$ ist ja gleichbedeutend mit der Ordnung des Elements 1 in der Gruppe $(M, +)$ von K, d.h. gleich der kleinsten natürlichen Zahl m derart, dass hinsichtlich der Vielfachenbildung $\perp_{(+)}$ in $(M, +)$ gilt

$$m \perp_{(+)} 1 = \underbrace{1 + 1 + \cdots + 1}_{m\text{ - mal}} = 0\,, \tag{3}$$

wobei vorausgesetzt ist, dass (3) überhaupt für natürliche Zahlen erfüllbar ist. m ist dann stets eine Primzahl. Ist (3) für natürliche Zahlen nicht erfüllbar, so hat per definitionem das Element 1 die Ordnung 0 und K die Charakteristik 0. Für eine Anordnung $<$ in einem Körper K mit $\chi(K) = p$ müsste nun wegen $1 > 0$ gemäss (A_3) und (A_2) gelten $p \perp_{(+)} 1 > 0$, also nach (3): $0 > 0$, was (A_1) widerspricht.

Ein notwendiges und hinreichendes Kriterium für die Existenz einer Anordnung in K lautet: -1 ist nicht als Quadratsumme in K darstellbar[1]). Offensichtlich gleichbedeutend dazu ist: 0 ist nicht Summe von Quadratelementen, deren Basen von 0 verschieden sind. Körper mit dieser Eigenschaft nennt man *formal-reell*. Man sieht unmittelbar, wie die beiden vorangehend erörterten Fälle sich hier einordnen.

3. Es liegt nahe, nach den Möglichkeiten zur Einführung eines Quadratwurzelterms in beliebigen, also vor allem in nicht anordnungsfähigen Körpern zu fragen und dabei insbesondere die Gültigkeit der Formel (2) zu diskutieren[2]). Wie wir schon sahen, wird die Anordnung bei der Definition (1) dazu verwendet, mit $y \geqslant 0$ eine die beiden Lösungen von $y^2 = x$ mit $x \in Q$ und $x \neq 0$ *trennende Bedingung* $\beta(y)$ zu gewinnen. Wir wollen $y > 0$ eine stark trennende und $y \geqslant 0$ eine schwach trennende Bedingung nennen. Von einer *stark trennenden Bedingung* $\beta^*(y)$ in einem Körper $K = (M, +, \cdot)$ wollen wir allgemein verlangen, dass für alle $y \in M$ gilt:

$$(T)\quad \text{Entweder } \beta^*(y) \text{ oder } y = 0 \text{ oder } \beta^*(-y)\,.$$

Die gemäss

$$\beta(y) \Longleftrightarrow_{Df} \beta^*(y) \text{ oder } y = 0$$

jeder stark trennenden Bedingung $\beta^*(y)$ zugeordnete Bedingung $\beta(y)$ nennen wir allgemein *schwach trennend*.

Mit jeder schwach trennenden Bedingung β in K lässt sich in K ein (1) entsprechender Quadratwurzelterm $\sqrt[(\beta)]{x}$ folgendermassen einführen:

$$\sqrt[(\beta)]{x} =_{Df} \text{dasjenige } y, \text{ für das } y^2 = x \text{ und } \beta(y)\,. \tag{4}$$

---

[1]) Siehe [4] im Literaturverzeichnis.

[2]) Siehe [3].

In den Primkörpern K_p der Charakteristik $p \neq 2$ mit den Elementen $0, 1, \ldots, p-1$ können wir etwa (unter Verwendung der natürlichen Ordnung dieser Elemente) wählen[2]:

$$\beta(y) \Longleftrightarrow_{Df} y \leqslant \frac{p-1}{2} . \tag{5}$$

Im Körper der komplexen Zahlen C können wir zum Beispiel nehmen[2],

$$\beta(y) \Longleftrightarrow_{Df} 0 \leqslant \arg y < \pi \text{ oder } y = 0 . \tag{6}$$

Eine von $y \geqslant 0$ im (angeordneten) Körper P der rationalen Zahlen verschiedene Bedingung ist[3]:

$$\beta(y) \Longleftrightarrow_{Df} \text{es gibt } n \in Z \text{ und } k, m \in N, \text{ so dass } y = (-2)^n \frac{2m-1}{2k-1} . \tag{7}$$

In (7) wird davon Gebrauch gemacht, dass jede positive rationale Zahl als Produkt aus einer Zweierpotenz mit ganzer Hochzahl ($n \in Z$) und einem gekürzten Bruch mit ungeradem positivem Zähler und Nenner dargestellt werden kann.

Offensichtlich existiert eine trennende Bedingung in K genau dann, wenn $\chi(K) \neq 2$. Genau unter dieser Voraussetzung ist nämlich für alle $y \neq 0$: $(1+1)\,y = y + y \neq 0$, also $y \neq -y$. Zur «Existenz» sei bemerkt, dass wir für unsere Bedingungen keinen bestimmten sprachlichen Aufbau verlangen; insbesondere lassen wir die Mengenlehre als Darstellungsmittel zu. Nach dem Auswahlaxiom[4] existiert zur Menge aller Mengen $\{y, -y\}$ mit $y \in M$ eine Teilmenge T von M, die aus jeder der Mengen $\{y, -y\}$ genau ein Element enthält. Ist $\chi(K) \neq 2$, so erschliessen wir die Existenz, indem wir setzen:

$$\beta(y) \Longleftrightarrow y \in T .$$

Ist $\chi(K) = 2$, so sind die $\{y, -y\}$ Einermengen. In diesem Falle brauchen wir also zur Definition eines Quadratwurzelterms keine zusätzliche Bedingung. Es gibt hier genau eine Quadratwurzelfunktion, für die dann auch (2) erfüllt ist.

4. Wir interessieren uns jetzt allgemein für die Gültigkeit der Formel (2). Die mittels (6) und im allgemeinen auch die mittels (5) eingeführten Quadratwurzeln besitzen die in (2) angegebene Eigenschaft nicht. Bei den entsprechenden β ist in K_7

$$\underset{(\beta)}{\sqrt{4}} \cdot \underset{(\beta)}{\sqrt{2}} = 2 \cdot 3 = 6 \neq \underset{(\beta)}{\sqrt{4 \cdot 2}} = \underset{(\beta)}{\sqrt{1}} = 1 ,$$

im Körper C der komplexen Zahlen ist

$$\underset{(\beta)}{\sqrt{-1}} \cdot \underset{(\beta)}{\sqrt{-1}} = i \cdot i = -1 \neq \underset{(\beta)}{\sqrt{(-1)\,(-1)}} = \underset{(\beta)}{\sqrt{1}} = 1 .$$

Die obige Ableitung von (2) in angeordneten Körpern mit $y \geqslant 0$ als $\beta(y)$ gibt uns unmittelbar eine notwendige und hinreichende Bedingung dafür an, dass die auf eine trennende Bedingung β gegründete Quadratwurzel die Eigenschaft (2) hat: β^* und damit auch β müssen multiplikativ sein, d.h. es muss gelten:

(M) Wenn $\beta^*(y)$ und $\beta^*(z)$, so $\beta^*(y \cdot z)$.

[3]) Siehe [2].
[4]) Siehe [4].

Ist nun in einem Körper K eine schwache $(M)(T)$-Bedingung β gegeben, so fallen offensichtlich alle Quadratelemente von K darunter: Zunächst gilt ja $\beta(0)$. Falls $y \neq 0$, so gilt $\beta(y)$ oder $\beta(-y)$ gemäss (T). Nach (M) ergibt sich daraus in jedem Falle $\beta(y^2)$.

Dies führt in endlichen Körpern K mit $\chi(K) \neq 2$ zu folgender Überlegung: Hat K die Ordnung (Elementezahl) n, so gibt es in K genau $(n+1)/2$ verschiedene Mengen $\{y, -y\}$, also ebenso viele Quadratelemente. Genau $(n+1)/2$ Elemente müssen aber jeweils einer gegebenen trennenden Bedingung genügen. Nun ist $y \in Q$ multiplikativ. Man hat also auf der Suche nach $(M)(T)$-Bedingungen in K nur noch zu prüfen, ob $y \in Q$ auch trennend ist. Das ist zum Beispiel für K_7 der Fall, wo $Q = \{0, 1, 2, 4\}$. Mit $y \in Q$ als $\beta(y)$ wäre jetzt $\sqrt{2} = 4$, so dass der obige Verstoss gegen (2) nicht auf-
(β)
treten kann. In K_5 ist $y \in Q$ mit $Q = \{0, 1, 4\}$ jedoch nicht trennend; denn wegen $4 = -1$ gilt hier $\beta(1)$ und $\beta(-1)$. In K_5 gibt es also keine $(M)(T)$-Bedingung.

Dass -1 wie in K_5 Quadratelement ist, wird für endliche Körper unmittelbar nicht nur als hinreichend, sondern auch als notwendig für die Nichtexistenz einer $(M)(T)$-Bedingung erkannt. Existiert nämlich keine $(M)(T)$-Bedingung, so ist $y \in Q$ nicht trennend, also gibt es $y \neq 0$ mit $y \in Q$ und $-y \in Q$, etwa $y = a^2$ und $-y = b^2$. Dann ist aber

$$-1 = \frac{y}{-y} = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2$$

Quadratelement in K. Zugleich zeigt diese Überlegung, dass in beliebigen Körpern K gleichbedeutend zu «-1 ist Quadratelement in K» gesagt werden kann: «0 ist als Summe zweier Quadrate in K darstellbar».

Für die Primkörper K_p bedeutet das, dass $p-1$ Quadratzahl ist, was bekanntlich genau dann zutrifft, wenn p eine Primzahl der Gestalt $4n+1$ ist. Diese Zahlen sind aber zugleich auch die Primzahlen, die Summe zweier Quadratzahlen sind. Positiv ausgedrückt: In K_p gibt es genau dann eine $(M)(T)$-Bedingung (nämlich $y \in Q$), wenn $p = 4n-1$. Primzahlen beider Arten gibt es bekanntlich unendlich viele[5]). Dasselbe gilt für alle endlichen K mit $\chi(K) = P$.

Interessant ist, dass es im Körper der rationalen Zahlen P auch $(M)(T)$-Bedingungen gibt, die von $y \geqslant 0$ verschieden sind. Man bestätigt leicht, dass (7) multiplikativ und trennend ist. Im Körper der reellen Zahlen R kann es solche von $y \geqslant 0$ verschiedenen Bedingungen nicht geben, da hier genau alle nicht negativen Zahlen Quadratzahlen sind, also $y \in Q$ schon trennend ist. Hier ist also $y \geqslant 0$ die einzige $(M)(T)$-Bedingung.

5. Die Eigenschaft, dass -1 nicht Quadratelement (oder 0 nicht Summe zweier Quadratelemente) in K ist, ist selbstverständlich in beliebigen K notwendig für die Existenz einer $(M)(T)$-Bedingung, so dass demgemäss zum Beispiel auch im Körper C keine solche Bedingung existiert. Wir wollen jetzt zeigen, dass diese Eigenschaft für alle Körper auch hinreichend ist.

Dazu betrachten wir zunächst die multiplikative Gruppe $K^* = (M - \{0\}, \cdot)$ in K und machen uns klar, dass die Elemente, die einer starken $(M)(T)$-Bedingung β^* in K genügen, eine Untergruppe B^* von K^* vom Index 2 bilden. Genauer beweisen wir:

[5]) Siehe [1].

Satz 1: Im Körper $K = (M, +, \cdot)$ gibt es genau dann eine starke $(M)(T)$-Bedingung β^*, wenn es eine Untergruppe B^* von $K^* = (M - \{0\}, \cdot)$ vom Index 2 gibt, die -1 nicht enthält. Gemäss $\beta^*(y) \Leftrightarrow y \in B^*$ besteht zwischen den β^* und den B^* eine eineindeutige Zuordnung.

Beweis: a) Ist β^* eine starke $(M)(T)$-Bedingung in K, so gilt $\beta^*(1)$, also nicht $\beta^*(-1)$. Falls $\beta^*(y)$, so nicht $\beta^*(-1/y)$, weil sonst $\beta^*(-1)$; also gilt wegen (T) $\beta^*(1/y)$. Unter Beachtung von (M) bedeutet das, dass die unter β^* fallenden Elemente eine Untergruppe B^* von K^* bilden, die -1 nicht enthält. Gilt nun $y \in K^*$ und $y \notin B^*$, so folgt $-y \in B^*$, und wir haben $y = (-1)(-y)$. Das besagt aber, dass y zur Nebenklasse von -1 gehört. B^* ist also vom Index 2 in K.

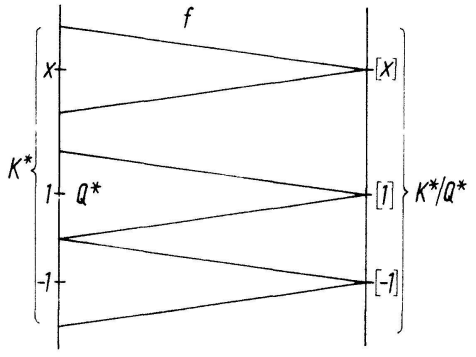
b) Ist B^* eine Untergruppe von K^* vom Index 2, die -1 nicht enthält, so ist $y \in B^*$ multiplikativ. Ferner ist $y \in B^*$ stark trennend; ist $y \neq 0$, so trifft entweder $y \in B^*$ oder $y = (-1)\,b$ mit $b \in B^*$ zu. Letzteres ist gleichbedeutend mit $-y = b \in B^*$.

Wir kommen damit zum Beweis unseres Hauptresultates:

Satz 2: In einem Körper K existiert eine $(M)(T)$-Bedingung genau dann, wenn -1 nicht Quadratelement in K ist.

Beweis: Es bleibt nach dem Vorangehenden noch zu zeigen, dass aus «-1 ist nicht Quadratelement in K» die Existenz einer $(M)(T)$-Bedingung in K oder gleichwertig nach Satz 1 die Existenz einer Untergruppe B^* von K^* vom Index 2 mit $-1 \notin B^*$ folgt. Um eine solche Gruppe B^* anzugeben, gehen wir davon aus, dass die Menge aller von 0 verschiedenen Quadratelemente in K eine Untergruppe Q^* von K^* bildet, die jedenfalls in dem gesuchten B^* enthalten ist. Es kommt offensichtlich darauf an, eine maximale Untergruppe von K^* zu bestimmen, die Q^* umfasst und -1 nicht enthält. Dies gelingt durch Betrachtung der Quotientengruppe $V = K^*/Q^*$. Die Abbildung $f\colon x \to [x]$, die jedem Element $x \in K^*$ die zugehörige Restklasse $[x]$ in V zuordnet, ist ein Homomorphismus mit $f(Q^*) = [1]$ (siehe Figur 1). Demgemäss ist für alle $[x] \in V$:

$$[x] \cdot [x] = [x^2] = [1]\,.$$



Figur 1

Das heisst: Jedes vom neutralen Element [1] verschiedene Element von V ist von der Ordnung 2. Die Gruppe V ist also in natürlicher Weise ein Vektorraum über dem Primkörper K_2. Nach einem allgemeinen Satz besitzt jeder Vektorraum eine Basis[6]). $\mathfrak{B} = \{e_i\}_{i \in I}$ sei eine Basis von V mit $0 \in I$ und $e_0 = [-1]$. Eine maximale Untergruppe

[6]) Siehe [5].

U von V erhalten wir jetzt dadurch, dass wir den von $\mathfrak{B} - \{e_0\}$ aufgespannten Unterraum betrachten. Dieser enthält $[-1]$ nicht und ist vom Index 2 in V. Ist nämlich $y \notin U$, so ist (unter Verwendung der additiven Schreibweise):

$$y = 1\, e_0 + \lambda_1\, e_1 + \ldots = 1\, e_0 + u$$

mit $u \in U$. Die Gruppe $f^{-1}(U)$ ist dann – wie man sofort sieht – eine Untergruppe von K^* vom Index 2, die -1 nicht enthält.

6. Ist K ein nichtkommutativer *Schiefkörper*, so existiert eine $(M)(T)$-Bedingung für K genau dann, wenn -1 nicht zu der von den von 0 verschiedenen Quadraten erzeugten Untergruppe $\hat{Q}^*$ von K gehört. Wegen $a\, x^2\, a^{-1} = (a\, x\, a^{-1})\,(a\, x\, a^{-1}) = (a\, x\, a^{-1})^2$ ist $\hat{Q}^*$ Normalteiler in K. Wir können also genau so schliessen wie oben. In nichtkommutativen Schiefkörpern ist mit der Trennung von y und $-y$ allerdings im allgemeinen noch nicht die Isolierung einer der Lösungen der Gleichung $y^2 = x$ erreichbar, da diese Gleichung dort sogar unendlich viele Lösungen haben kann, wie zum Beispiel $y^2 = -4$ im Schiefkörper der Quaternionen über den reellen Zahlen.

7. Abschliessend weisen wir noch auf die von A. KIRSCH entdeckte eigentümliche Rolle hin, die die Körper, in denen -1 nicht Quadratelement ist, bei der Beurteilung der Unabhängigkeit des obigen Axioms (A_2) von den Axiomen (A_1), (A_3) und (A_4) bei fest vorgegebenen Körpern K spielen[7]). Die Frage nach der Existenz einer den Axiomen (A_1), (A_3) und (A_4) genügenden Relation ϱ in K ist offensichtlich gleichbedeutend mit der Frage nach der Existenz einer $(M)(T)$-Bedingung β in K, wobei wir setzen:

$$a \varrho b \Longleftrightarrow \beta\,(b - a)\,.$$

Eine solche Relation ϱ erfüllt nun auch das Axiom (A_2), d.h. ist eine Ordnungsrelation in K, genau dann, wenn die Menge B der β-Elemente additiv abgeschlossen ist. Das ist für die Bedingung (7) in P nicht der Fall, so dass hier (A_2) unabhängig ist von (A_1), (A_3) und (A_4). In R gibt es jedoch nur eine einzige $(M)(T)$-Bedingung β. Die Menge der β-Elemente ist zudem additiv abgeschlossen. In R ist (A_2) also abhängig von den übrigen Anordnungsaxiomen.

In nicht anordnenbaren Körpern K, also insbesondere in endlichen Körpern, sind nicht alle vier Axiome zugleich erfüllbar. Das Axiom (A_2) ist also für ein endliches K genau dann abhängig, wenn auch (A_1), (A_3) und (A_4) nicht erfüllbar sind, und es ist unabhängig genau dann, wenn die (A_1), (A_3) und (A_4) erfüllbar sind, wenn also -1 nicht Quadratelement in K ist.

H.-G. STEINER, Münster/Westf.

LITERATUR

[1] H. HASSE, *Vorlesungen über Zahlentheorie*, 2. Auflage 1964.
[2] A. KIRSCH, *Die Anordnungseigenschaften der Zahlen als Gegenstand für Axiomatisierungsübungen*, Math.-phys. Sem.-Ber. *XIII*, 83–105 (1966).
[3] H.-G. STEINER, *Quadratische Gleichungen und Quadratwurzelfunktion in Körpern*, Math.-phys. Sem.-Ber. *XII*, 211–229 (1965).
[4] B. L. VAN DER WAERDEN, *Algebra I*, 7. Auflage 1966.
[5] N. BOURBAKI, *Algèbre linéaire*, Paris 1955.

[7]) Siehe [2].