Zusammenfassung Im zweiten Teil (vgl. [25]) unseres Artikels über den Euklidischen Vierzahlensatz gehen wir vom Begriff der Inkommensurabilität aus und leuchten die Irrationalitätsbeweise algebraischer Zahlen aus. Dabei treffen wir auf das Gaußsche Lemma, die ganze Abgeschlossenheit und Dedekinds Prager Satz, um schließlich wieder beim Vierzahlensatz zu landen.

Noname manuscript No.
(will be inserted by the editor)

Zur Zahlentheorie der Griechen

Franz Lemmermeyer

Received: date / Accepted: date

Teil II. Gaußsche Lemmas und Rieszsche Ringe

8 Noch einmal die Alten Griechen: Inkommensurabilität

Bekanntlich wird den Pythagoreern auch die Entdeckung der Inkommensurabilität zugeschrieben, also der Beobachtung, dass z.B. Diagonale d und Seite s eines Quadrats kein rationales Verhältnis zueinander haben, dass sich also nicht $d : s = p : q$ für natürliche Zahlen p, q schreiben lässt. Für diese Behauptung gibt es eine Unzahl von Beweisen, von denen zwei bereits auf die Griechen zurückgehen

- Der eine Beweis folgert aus $\sqrt{2} = \frac{p}{q}$, dass p und q beide gerade sein müssen, was der Kürzbarkeit von Brüchen (bzw. Proportionen) widerspricht. Dieser Beweis geht auf Aristoteles zurück und ist in manchen Ausgaben der Elemente als Proposition X.115 enthalten; er gilt heute aber als später eingefügter Zusatz.
- Der andere Beweis (vgl. Hasse [17] und Apostol [2]) ist geometrischer Natur und basiert auf der "Wechselwegnahme", dem Vater des Euklidischen Algorithmus.

Dass bereits die Pythagoreer die Existenz inkommensurabler Strecken entdeckten gilt als sicher; dass Hippasus diese Entdeckung gemacht (bzw. bekannt gemacht) hat ist dagegen ungewiss, ebenso die Behauptung, er sei durch das Studium des Pentagramms darauf geführt worden (sh. von Fritz [14]). Die hin und wieder anzutreffende Behauptung, dies hätte eine "Grundlagenkrise" der griechischen Mathematik verursacht, ist schließlich durch keinerlei historische Fakten mehr zu belegen (muss deswegen aber nicht falsch sein).

Die Inkommensurabilität von Strecken hat sich im Zuge der Erweiterung des Zahlbegriffs von einem geometrischen zu einem arithmetischen Problem gewandelt: das Verhältnis zweier Strecken ist für uns einfach eine Zahl, und die Inkommensurabilität von Seite und Diagonale eines Quadrats die Irrationalität der Quadratwurzel aus 2.

F. Lemmermeyer
Mörikeweg 1, 73489 Jagstzell
E-mail: hb3@ix.urz.uni-heidelberg.de

Wenn man weiß, dass der Ring $\mathbb{Z}$ faktoriell ist, wird der Beweis der Irrationalität von $\sqrt{2}$ trivial: aus $2q^2 = p^2$ liest man ab, dass 2 die linke Seite in ungerader, die rechte in gerader Potenz teilt: Widerspruch.

Derselbe Beweis zeigt allgemeiner[1]:

Satz 1 *Für $m \in \mathbb{Z}$ ist $\sqrt{m}$ genau dann rational, wenn m das Quadrat einer ganzen Zahl ist.*

Auch dies ist ein Satz, der im Wesentlichen bereits den Griechen bekannt war; allerdings ist er so explizit nicht in Euklids Elementen zu finden.

Anstatt den Beweis der Irrationalität von $\sqrt{2}$ mit Hilfe der eindeutigen Primfaktorzerlegung zu führen, können wir ihn auch durch Ausnutzen der euklidischen Division mit Rest erhalten (was angesichts der Tatsache, dass Euklidische Ringe faktoriell sind, natürlich keinesfalls verwundern sollte): Sei m kein Quadrat in $\mathbb{N}$; dann gibt es ein $n \in \mathbb{N}$ mit $n^2 < m < (n+1)^2$, also mit $0 < \sqrt{m} - n < 1$. Ist $\sqrt{m}$ rational, so können wir $\sqrt{m} = \frac{p}{q}$ mit minimalem $q \in \mathbb{N}$ schreiben. Dann ist $r := q(\sqrt{m} - n)$ ebenfalls ganz, und wegen $0 < \sqrt{m} - n < 1$ ist $0 < r < q$. Nun ist $r\sqrt{m} = q(\sqrt{m} - n)\sqrt{m} = mq - nq\sqrt{m}$ ganz, da mq und $q\sqrt{m}$ ganz sind; dies widerspricht aber der Minimalität von q. Für Verallgemeinerungen dieser Schlussweise[2], sowie andere Irrationalitätsbeweise sh. z.B. die Übungen in [28, Kap. 1].

Hier ist ein Beweis, welcher auf der Tatsache basiert, dass $\mathbb{Z}$ ein Bezout-Ring ist: sei $\sqrt{m} = \frac{p}{q}$ mit teilerfremden ganzen Zahlen p und q. Dann ist wegen $p^n = mq^n$

$$(1) = (p, q)^n \subseteq (p^n, q) = (mq^n, q) \subseteq (q),$$

folglich $(q) = (1)$ und m eine ganze Zahl.

So hübsch solche Beweise auch sind, verschleiern sie in gewisser Weise doch den eigentlichen Kern der Angelegenheit; diesen wollen wir im nächsten Abschnitt offenlegen.

9 Ganze Abgeschlossenheit

Der Begriff der ganzen Abgeschlossenheit begegnet Studierenden in der Regel in einführenden Algebravorlesungen: ist R ein Integritätsring mit Quotientenkörper K, so nennt man $t \in K$ ganz über R, wenn t Nullstelle eines normierten Polynoms $f \in R[X]$ ist. Ist jedes $t \in K$, das ganz über R ist, bereits in R enthalten, so nennt man R ganz abgeschlossen (in seinem Quotientenkörper).

Sind $t_1, t_2 \in K$ ganz über R, so sind auch $t_1 + t_2$ und $t_1 t_2$ ganz über R. Der klassische Beweis über Resultanten wurde im Laufe der Zeit ersetzt durch Beweise via endlich erzeugter Moduln; im Gewande der Tensorsprache kommt der klassische Beweis aber an Eleganz fast an den Modulbeweis heran: t_j ist als Nullstelle eines normierten Polynoms vom Grad m_j mit Koeffizienten aus R auch Eigenwert einer Matrix T_j mit Einträgen aus R. Man zeigt nun leicht, dass $t_1 t_2$ Eigenwert des Kroneckerprodukts

[1] Im Monoid M aller natürlichen Zahlen $\equiv 0, 1, 2 \bmod 4$ ist 9 das Quadrat des Bruchs $\frac{6}{2}$ im Quotientenmonoid, aber kein Quadrat einer Zahl in M. Entsprechend ist $2i$ kein Quadrat in $\mathbb{Z}[2i] = \mathbb{Z} \oplus 2i\mathbb{Z}$, wohl aber eines im Quotientenkörper $\mathbb{Q}(i)$ wegen $2i = (1+i)^2 = (\frac{2+2i}{2})^2$.

[2] Dieser Beweis geht im wesentlichen auf Dedekind [11] zurück; für eine geometrische Einkleidung des Beweises durch Hajos sh. [37]. Varianten dieses Beweises finden sich u.a. in [3, 13, 34, 38, 40].

$T_1 \otimes T_2$ und damit ganz über R ist. Entsprechend folgt, dass $t_1 + t_2$ Eigenwert von $T_1 \otimes I_1 + I_2 \otimes T_2$ ist, wo die I_j Einheitsmatrizen geeigneter Dimension sind (sh. [22]).

Der Satz, dass faktorielle Ringe ganz abgeschlossen sind, gehört zum Grundwissen von Algebrastudenten; der übliche Beweis liefert sogar die stärkere Aussage, dass GGT-Ringe ganz abgeschlossen sind. Aber selbst in Vorlesungen über algebraische Zahlentheorie wird selten klar herausgearbeitet, wie grundlegend der Begriff der ganzen Abgeschlossenheit für die Entwicklung dieser Disziplin gewesen ist, und welche Bedeutung diese unscheinbare Definition für die moderne Algebra gewonnen hat, seitdem Dedekind und Emmy Noether ihn[3] aus dem Aufbau der Dedekindschen Idealtheorie herauskristallisiert haben. In der Tat zeigt ein Blick auf die folgende Abbildung, dass die meisten der in den einführenden Algebravorlesungen auftauchenden Klassen von Ringen[4] ganz abgeschlossen sind:

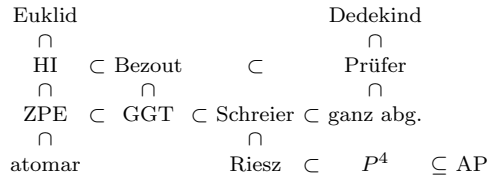

Abbildung 1 Klassen von Ringen

Die ganze Abgeschlossenheit von $\mathbb{Z}$ ist auch der eigentliche Grund für die Gültigkeit von Satz 1. Ist nämlich $n \in \mathbb{Z}$ das Quadrat einer rationalen Zahl, also z.B. $\sqrt{n} = \frac{p}{q}$, so ist $\frac{p}{q}$ Nullstelle des quadratischen Polynoms $X^2 - n \in \mathbb{Z}[X]$. Da $\mathbb{Z}$ ganz abgeschlossen ist, muss $\frac{p}{q} \in \mathbb{Z}$ sein.

Es ist daher keineswegs erstaunlich, dass sich die Irrationalität von $\sqrt{2}$ durch Ausnutzen der Faktorialität von $\mathbb{Z}$ nachweisen lässt. Weiter kann man versuchen, derartige Irrationalitätsbeweise mit all denjenigen Sätzen zu führen, aus denen ebenfalls die ganze Abgeschlossenheit von $\mathbb{Z}$ folgt. Ein Beispiel hierfür ist der folgende Beweis:

---

[3] Kummer hat den Begriff der ganzen algebraischen Zahl nicht gekannt, und die Bedeutung der ganzen Abgeschlossenheit ist ihm nicht klar geworden. Seine Konstruktion der idealen Zahlen in Kreiskörpern hat deswegen funktioniert, weil die Ringe, die Kummer betrachtete, ganz abgeschlossen waren; allerdings hat sein Aufbau seiner Theorie der idealen Zahlen eine Lücke, die erst Dedekind geschlossen hat – unter Ausnutzung der ganzen Abgeschlossenheit (vgl. [26]).
Auch Dirichlet und Eisenstein blieb die ganze Abgeschlossenheit verborgen: Dirichlet bewies seinen Einheitensatz in Ringen der Form $\mathbb{Z}[\alpha]$, wo α eine ganze algebraische Zahl ist, und aus einer Bemerkung Eisensteins folgt, dass die ganzen algebraischen Zahlen einen Ring bilden. Heine [18] definierte ganze algebraische Zahlen als solche, die sich mittels Ringoperationen und wiederholtes Ziehen von n-ten Wurzeln aus den ganzen Zahlen gewinnen lassen.
Dedekind zeigte, dass in den Ringen ganzer Zahlen eines Zahlkörpers $K \subseteq \mathbb{C}$ jedes Ideal eindeutig Produkt von Primidealen ist; schließlich gelang es Emmy Noether 1926 zu zeigen, dass dieser Satz in allen Integritätsringen gilt, in denen gewissen Axiome erfüllt sind – eines davon ist die ganze Abgeschlossenheit.

[4] Bisher noch nicht definierte Begriffe wie Schreier oder P^4 werden in den Abschnitten 12 und 13 erklärt.

$$\begin{aligned}\sqrt{m} \text{ ist rational} &\iff X^2 - m \text{ ist reduzibel in } \mathbb{Q}[X] \\ &\iff X^2 - m \text{ ist reduzibel in } \mathbb{Z}[X] \\ &\iff X^2 - m = (X-n)(X+n) \text{ für ein } n \in \mathbb{Z} \\ &\iff m = n^2 \text{ für ein } n \in \mathbb{Z}.\end{aligned}$$

Der Übergang von $\mathbb{Q}[X]$ zu $\mathbb{Z}[X]$ geschieht dabei mit dem Gaußschen Hebungslemma[5] für normierte Polynome:

Lemma 2 *Sind $g, h \in \mathbb{Q}[X]$ normierte Polynome mit $gh = f \in \mathbb{Z}[X]$, dann sind $g, h \in \mathbb{Z}[X]$.*

In dieser Form taucht das Gaußsche Hebungslemma in den Disquisitiones Arithmeticae auf (nämlich in [15, Art. 42]), und wird dort zum Nachweis der Irreduzibilität der Kreisteilungspolynome $F_p(X) = \frac{X^p-1}{X-1}$ für prime p verwendet. Zur Abgrenzung von anderen Ergebnissen, die ebenfalls unter dem Namen "Gaußsches Lemma" bekannt sind[6], werden wir Lemma 2 das Gaußsche Hebungslemma (für normierte Polynome) nennen.

Mit Lemma 2 lässt sich viel mehr zeigen als nur die Irrationalität gewisser Quadratwurzeln: ist nämlich α Nullstelle eines normierten Polynoms mit ganzen Koeffizienten (also eine ganze algebraische Zahl), so ist α eine ganze Zahl oder irrational. In der Tat: ist α rationale Nullstelle des normierten Polynoms $f \in \mathbb{Z}[X]$, dann ist $f(X) = (X - \alpha)g(X)$, und $g \in \mathbb{Q}[X]$ normiert. Das Gaußsche Hebungslemma für normierte Polynome zeigt dann $X - \alpha \in \mathbb{Z}[X]$, also $\alpha \in \mathbb{Z}$.

Das Gaußsche Hebungslemma für normierte Polynome ist ein Spezialfall von

Satz 3 (Gaußsches Hebungslemma) *Ist $F \in \mathbb{Z}[X]$ ein Polynom und gibt es Polynome $g, h \in \mathbb{Q}[X]$ mit $F = gh$, dann existiert ein $c \in \mathbb{Q}$ mit der Eigenschaft, dass $G = cg, H = \frac{1}{c}h \in \mathbb{Z}[X]$ ist. Jede Faktorisierung von $F = gh$ in $\mathbb{Q}[X]$ lässt sich daher zu einer Faktorisierung $F = GH$ in $\mathbb{Z}[X]$ "hochheben".*

Dieser Satz ist auch in heutigen Algebravorlesungen noch ein wichtiges Hilfsmittel beim Nachweis der Irreduzibilität von Polynomen und wird beispielsweise beim Beweis des Eisensteinschen Kriteriums benutzt: mit dessen Hilfe zeigt man nämlich, dass ein Polynom in $R[X]$ genau dann irreduzibel in $K[X]$ ist, wenn es irreduzibel in $R[X]$ ist.

Ist R ein Integritätsbereich mit Quotientenkörper K, so sagen wir, in $R[X]$ gelte das Gaußsche Hebungslemma, wenn sich jede Faktorisierung eines $F \in R[X]$ von $K[X]$ nach $R[X]$ hochheben lässt. Wir stellen uns nun die Frage, in welchen Ringen die obigen Versionen des Gaußschen Hebungslemmas gelten. Für normierte Polynome ist diese Frage relativ leicht zu beantworten:

[5] Der Name soll andeuten, dass sich Faktorisierungen von Polynomen über $\mathbb{Q}$ hochheben lassen Faktorisierungen über $\mathbb{Z}$.

[6] Es gibt mindestens drei solcher Resultate: das oben angeführte Hebungslemma, und je eines aus der Theorie der quadratischen Reste bzw. der quadratischen Formen. Alle drei finden sich in den Disquisitiones Arithmeticae.
Weiter wird das Gaußsche Hebungslemma in $\mathbb{Z}$ oft anders formuliert, und diese Versionen sind zwar über $\mathbb{Z}$, nicht aber über allgemeinen Integritätsringen zu dem oben formulierten Hebungslemma äquivalent.

Satz 4 *Sei R ein Integritätsring mit Quotientenkörper K. Dann sind folgende Aussagen gleichbedeutend:*

1. *R ist ganz abgeschlossen.*
2. *In $R[X]$ gilt das Gaußsche Hebungslemma für normierte Polynome: Sind $g, h \in K[X]$ normierte Polynome mit $gh = f \in R[X]$, dann sind $g, h \in R[X]$.*
3. *In $R[X]$ gilt Dedekinds Prager Satz: sind*

$$b(X) = \sum_{i=1}^{m} b_i X^i \quad \textit{und} \quad c(X) = \sum_{j=1}^{n} c_j X^j \tag{1}$$

Polynome in $R[X]$, und ist $a \mid b(X)c(X)$ für ein $a \in R$, so gilt $a \mid b_i c_j$ für alle $0 \le i \le m$, $0 \le j \le n$.

Bevor wir den Beweis von Satz 4 geben und danach die Gültigkeit des allgemeinen Hebungslemmas untersuchen, machen wir noch einige Bemerkungen zur Bedeutung von Dedekinds Prager Satz.

10 Dedekinds Prager Satz

Historisch spielte Dedekinds Prager Satz[7] eine wichtige Rolle beim Aufbau der Dedekindschen Idealtheorie. Dedekind empfand das Argumentieren mit Polynomen beim Aufbau seiner Idealtheorie als unangemessen[8], und suchte nach anderen Wegen. Hurwitz [21] veröffentlichte dann einen Zugang zur Idealtheorie, der auf Dedekinds Prager Satz aufbaute (und welcher ihm damals nicht bekannt war), woraufhin Dedekind erklärte, dass ihm dieser Weg bekannt sei, er aus methodischen Gründen aber seinem eigenen Aufbau den Vorzug gegeben habe. Hilberts Zahlbericht [20] und Landaus[9] Lehrbuch [24] über algebraische Zahlen benutzen beide den Hurwitzschen Zugang[10], während man heute eher mit Lokalisierungen arbeitet (was sicher den Beifall Dedekinds gefunden hätte).

Dedekind [9] gab zwei Beweise seines Prager Satzes; den ersten findet man bei Landau [24] (Hilbert gibt in seinem Zahlbericht [20] keinen Beweis, sondern verweist auf Arbeiten von Dedekind [9], Hurwitz [21], Kronecker [23], und Mertens [31]), und der zweite Beweis führt auf das Lemma von Dedekind–Mertens, dessen Geschichte und Weiterentwicklung u.A. durch Artin und Rees einen eigenen Artikel verdient hätte (vergl. dazu [7,8]).

---

[7] Diesen Satz hat Dedekind in der Zeitschrift der Prager Mathematischen Gesellschaft publiziert, und heute hat sich der Name "Prager Satz" dafür eingebürgert.

[8] Vgl. Dedekinds Kommentare zum Hurwitzschen Aufbau der Idealtheorie in [10], so auf S. 53 ("weil die Benutzung der Funktionen von Variablen mir immer als ein der Sache fremdes Hilfsmittel erscheint") und S. 55 ("Aus denselben Gründen konnte der oben erwähnte Beweis [...] mich noch nicht völlig befriedigen, weil durch die Einmischung der Funktionen von Variablen die Reinheit der Theorie nach meiner Ansicht getrübt wird").

[9] Landau [24, S. 145] nennt Dedekinds Prager Satz einen "Satz von Kronecker"; bei Cohn [5] heißt er "Hurwitz's Lemma". Walter Strobl weist in seiner Diplomarbeit [36, p. 157–161] darauf hin, dass Bachmann in vol III und vol V seines 5-bändigen Lehrwerks über Zahlentheorie detailliert auf den Prager Satz eingeht. Vergleiche auch die Einführung in Edwards [12].

[10] Dedekinds Satz dient dem Nachweis, dass es zu jedem Ideal $\mathfrak{a} \neq (0)$ in einer Maximalordnung eines Zahlkörpers ein Ideal $\mathfrak{b} \neq (0)$ gibt derart, dass $\mathfrak{ab}$ ein Hauptideal ist.

Wir wollen hier einen dritten Beweis angeben, der auf die Beobachtung zurückgeht, dass Dedekinds Prager Satz genau in ganz abgeschlossenen Ringen gilt[11]; damit muss es möglich sein, den Prager Satz aus dem Gauß'schen Hebungslemma für normierte Polynome herzuleiten.

Beweis (von Satz 4) (1) $\Longrightarrow$ (2): Der Ring $K[X]/(f)$ enthält R, sowie eine Wurzel von f. Induktiv erhält man so eine Ringerweiterung von R, in welcher f in Linearfaktoren zerfällt. Sei also $g(X) = \prod_i (X-\alpha_i)$ und $h(X) = \prod_j (X-\beta_j)$. Wegen $f(\alpha_i) = f(\beta_j) = 0$ sind die α_i und β_j ganz über R. Also sind auch die elementarsymmetrischen Funktionen in den α_i und β_j, insbesondere die Koeffizienten von g und h, ganz über R. Da R ganz abgeschlossen ist, liegen diese bereits in R, und es folgt $g, h \in R[X]$ (dieser Beweis stammt aus [4]).

(2) $\Longrightarrow$ (3): Wir nehmen nun an, dass $a \mid b(X)c(X)$ für $a \in R$ und Polynome $b, c \in R[X]$ ist. Dann ist $f(X) = \frac{b(X)}{a} c(X)$ eine Faktorisierung von $f \in R[X]$ in $K[X]$; nach dem Hebungslemma gibt es $r, s \in R$ mit $\frac{r}{as} b(X), \frac{s}{r} c(X) \in R[X]$. Also ist $as \mid rb(X)$ und $r \mid sc(X)$, d.h. $as \mid rb_i$ und $ar \mid sc_j$; Multiplikation ergibt $ars \mid rsb_i c_j$, d.h. $a \mid b_i c_j$.

(3) $\Longrightarrow$ (1): Sei $t \in K$ ganz über R, also Nullstelle eines normierten Polynoms $f \in R[X]$. Dann ist $f(X) = (X-t)g(X)$; seien $a, b \in R$ mit $at \in R$ und $bg \in R[X]$. Also ist $[a(X-t)][bg(X)] = abf(X)$ durch ab teilbar, und Dedekinds Prager Satz zeigt, dass $ab \mid atb$ in R gilt (auf der rechten Seite steht das Produkt des konstanten Glieds von $a(X-t)$ und des höchsten Koeffizienten b von $bg(X)$); daraus folgt $1 \mid t$, also $t \in R$.

Dedekinds Prager Satz spielt in der heutigen Algebra und Zahlentheorie praktisch keine Rolle mehr; das ist, wie Dedekind selbst bemerkt hat, nur konsequent: er ist ja äquivalent zur ganzen Abgeschlossenheit des Grundrings, und anstatt rechnerische Beweise mit dem Prager Satz zu führen, sollte man nach Dedekind konzeptionelle Beweise mit abstrakten Prinzipien wie der ganzen Abgeschlossenheit bevorzugen. Die Geschichte hat ihm da, wie bereits Emmy Noether in ihren Kommentaren zu Dedekinds Werken schrieb, Recht gegeben, auch wenn insbesondere Hilbert in seinem Zahlbericht dem Hurwitzschen Aufbau der Idealtheorie noch den Vorzug gegeben hat. Dieser "Fehlgriff" (vom Standpunkt der abstrakten Algebra aus; Hilbert hatte natürlich gute Gründe für seine Wahl) gehört wohl auch zu den Punkten, die Emmy Noether wiederholt zum Anlass für Kritik an Hilberts Zahlbericht nahm (vgl. [27]).

Damit beansprucht der Prager Satz jedenfalls eine historische Rolle: mit der Abkehr vom Prager Satz begann die Absatzbewegung weg von rechnerischen hin zu konzeptionellen Beweisen und die Durchdringung des untersuchten Gegenstands mit abstrakten Mitteln, eine Bewegung, die Dedekind initiierte, Emmy Noether zu ihrem Programm erhob, und die mit dem Schaffen Grothendiecks[12] einen vorläufigen Höhepunkt erreicht hat.

11 Plus ça change ...

Wie wir gesehen haben, gilt das Gaußsche Hebungslemma für normierte Polynome über Integritätsringen R genau dann, wenn R ganz abgeschlossen ist. Für das allgemeine

[11] Dass Emmy Noether diesen Satz 4 gekannt hat, wird aus ihren Bemerkungen zu Dedekinds Artikel [10] in seinen Werken klar.

[12] W. Scharlau hat jüngst eine lesenswerte Biographie Grothendiecks ([35]) herausgegeben.

Gaußsche Hebungslemma ist das nicht der Fall: das Polynom

$$2X^2 - 5 = 2(X - \tfrac{\sqrt{10}}{2})(X + \tfrac{\sqrt{10}}{2}) = (\sqrt{2}\,X - \sqrt{5}\,)(\sqrt{2}\,X + \sqrt{5}\,)$$

faktorisiert über $\mathbb{Q}(\sqrt{10}\,)$ (und über $\mathbb{Z}[\sqrt{2}, \sqrt{5}\,]$), nicht aber über dem ganz abgeschlossenen Ring $R = \mathbb{Z}[\sqrt{10}\,]$. In der Tat: wäre das Hebungslemma über R richtig, so müssten wir 2 in R so faktorisieren können (also $2 = \alpha\beta$ mit $\alpha, \beta \in R$), dass die Faktoren $\alpha(X - \frac{\sqrt{10}}{2})$ und $\beta(X + \frac{\sqrt{10}}{2})$ ganze Koeffizienten haben. Da aber 2 in $\mathbb{Z}[\sqrt{10}\,]$ irreduzibel ist, kann das nicht gelingen.

Man mag nun vermuten, dass der Grund für das Scheitern des Gaußschen Hebungslemmas darin liegt, dass der Ring $\mathbb{Z}[\sqrt{10}\,]$ nicht faktoriell ist. Tatsächlich ist dies gar nicht so weit von der Wahrheit entfernt: die Gültigkeit des Hebungslemmas in $R[X]$ hat etwas damit zu tun, ob in R der Euklidische Vierzahlensatz gilt. Mittels der Gleichung $2 \cdot 5 = \sqrt{10}\sqrt{10}$ sieht man schnell ein, dass das Element 2 in $\mathbb{Z}[\sqrt{10}\,]$ zwar irreduzibel, aber nicht prim (und damit auch nicht primal) ist. Insbesondere ist $\mathbb{Z}[\sqrt{10}\,]$ nicht Rieszsch. Jetzt zeigen wir

Proposition 5 *Ist $R[X]$ Rieszsch, so gilt in $R[X]$ das Hebungslemma.*

Beweis Sei $F \in R[X]$ und $F = gh$ mit $g, h \in K[X]$. Wähle $b, c \in R$ derart, dass $bg, ch \in R[X]$ ist, und setze $a = bc$. Dann ist $aF = (bg)(ch)$ in $R[X]$, und da $R[X]$ Rieszsch ist, existieren $m, n, r, s \in R[X]$ mit $a = mr$, $bg = nr$, $ch = ms$, und $F = ns$. Wegen $\operatorname{grad} a = 0$ müssen $m, r \in R$ sein. Weiter liegen $G = \frac{bg}{r}$ und $H = \frac{ch}{m}$ beide in $R[X]$, und aus $F = GH$ folgt dann die Gültigkeit des Hebungslemmas.

Als nächstes möchten wir die Umkehrung beweisen: Gilt in $R[X]$ das Gaußsche Hebungslemma, so ist $R[X]$ Rieszsch. Dazu müssen wir zeigen, dass alle Elemente von $R[X]$ primal sind. Ein erster Schritt in diese Richtung wäre der Nachweis, dass alle Elemente von R primal in $R[X]$ sind. Ein noch kleinerer Schritt schließlich ist das folgende

Lemma 6 *Gilt in $R[X]$ das Gaußsche Hebungslemma, so ist R Rieszsch.*

Beweis Sei $ad = bc$ für $a, b, c, d \in R$. Im Falle von $abcd = 0$ ist die Behauptung leicht nachzuweisen; wir dürfen daher $abcd \neq 0$ annehmen. Jetzt betrachten wir das Polynom

$$F(x) = a\Big(X - \frac{b}{a}\Big)\Big(X - \frac{c}{a}\Big) = aX^2 - (b + c)X + d \in R[X].$$

Da wir diese Faktorisierung nach $R[X]$ hochheben können, gilt $F(X) = G(X)H(X)$ für $G, H \in R[X]$. Sei daher $G(X) = \alpha X - \beta$ und $H(X) = \delta X - \gamma$ mit $\alpha, \beta, \gamma, \delta \in R$. Da G und $g(X) = X - \frac{b}{a}$ dieselbe Wurzel haben, ist $\frac{b}{a} = \frac{\beta}{\alpha}$, also $\alpha b = \beta a$; analog finden wir $\gamma a = \delta c$. Weiter liefert Koeffizientenvergleich $a = \alpha\delta$ und $d = \beta\gamma$. Daraus folgt $bc = ad = a\beta\gamma = \beta\delta c$, also $b = \beta\delta$. Ähnlich ergibt sich $bc = a\beta\gamma = b\alpha\gamma$ und damit $c = \alpha\gamma$. Zusammenfassend haben wir jetzt $a = \alpha\delta$ mit $\alpha \mid c$ und $\delta \mid b$, und das war zu zeigen.

Bemerkung. Man beachte, dass man für den Beweis von Lemma 6 nur das Gaußsche Hebungslemma für quadratische Polynome vorauszusetzen braucht.

Wir wissen jetzt, dass in Rieszschen Ringen $R[X]$ das Gaußsche Lemma gilt, und dass aus der Gültigkeit des Gaußschen Lemmas in $R[X]$ folgt, dass R Rieszsch ist. Jetzt würden wir gerne zeigen, dass mit R auch $R[X]$ Rieszsch ist; das geht allerdings nicht:

Proposition 7 *Sei R Rieszsch. Sind alle $a \in R$ auch in $R[X]$ primal, dann ist R ganz abgeschlossen.*

Beweis Sei $t \in K$ ganz über R, also Nullstelle eines normierten Polynoms $f \in R[X]$. Dann ist $f(X) = (X-t)g(X)$ für ein $g \in K[X]$. Jetzt gibt es $r, s \in R$ mit $r(X-t), sg(X) \in R[X]$. Das Element $q = rs \in R$ ist nach Annahme primal in $R[X]$, und es gilt $q \mid [r \cdot (X-t)][s \cdot g(X)]$. Also ist $q = ab$ mit $a \mid r \cdot (X-t)$ und $b \mid s \cdot g(X)$. Da $X-t$ und $g(X)$ normiert sind, muss $a \mid r$ und $b \mid s$ gelten. Wegen $ab = rs$ folgt daraus, dass $\frac{r}{a}, \frac{s}{b} \in R^\times$ Einheiten sind. Aus $\frac{r}{a}(X-t) \in R[X]$ folgt dann aber $t \in R$, folglich ist R ganz abgeschlossen.

Um daher die Rieszeigenschaft von R auf $R[X]$ übertragen zu können, benötigen wir die ganze Abgeschlossenheit von R. Wie sich nun herausstellt, brauchen wir diese aber gar nicht vorauszusetzen:

Proposition 8 *Sei R ein Integritätsring. Gilt in $R[X]$ das Gaußsche Hebungslemma, dann ist R ganz abgeschlossen.*

Beweis Sei K der Quotientenkörper von R und $t \in K$ ganz über R, also Nullstelle eines Polynoms $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$. Dann gibt es in $K[X]$ eine Faktorisierung $f(X) = (X-t)g(X)$ mit $X-t, g(X) \in K[X]$. Nach dem Gaußschen Hebungslemma existiert ein $q \in K^\times$ derart, dass $q(X-k)$ und $\frac{1}{q}g(X)$ beide in $R[X]$ liegen. Da sowohl $X-k$ wie auch $g(X)$ normiert sind, also Leitkoeffizient 1 besitzen, muss $q \in R$ und $\frac{1}{q} \in R$ sein. Also ist $q \in R^\times$ Einheit, und dies impliziert $X-t, g(X) \in R[X]$. Also ist $t \in R$, und R ganz abgeschlossen.

Insbesondere gilt das Gaußsche Hebungslemma nicht über $R = \mathbb{Z}[\sqrt{-3}]$: die Faktorisierung $X^2 + X + 1 = (X-\rho)(X-\rho^2)$ mit $\rho = \frac{-1+\sqrt{-3}}{2} \in K = \mathbb{Q}(\sqrt{-3})$ lässt sich offenbar nicht zu einer Faktorisierung in R hochheben.

12 Cohns Permanenzsatz

Nun zurück zu unserem Problem: wir wollen nachweisen, dass aus der Gültigkeit des Gaußschen Hebungslemmas in $R[X]$ folgt, dass $R[X]$ Rieszsch ist: wir haben bereits gesehen, dass R Rieszsch und ganz abgeschlossen ist; daraus möchten wir gern schließen, dass auch $R[X]$ Rieszsch ist. Der erste Schritt in diese Richtung ist die folgende

Proposition 9 *Sei R ganz abgeschlossen. Dann sind alle primalen $a \in R$ auch primal in $R[X]$.*

Beweis Sei $a \in R \setminus \{0\}$ primal und $a \mid b(X)c(X)$ für Polynome $b, c \in R[X]$. Mit Dedekinds Prager Satz folgt daraus[13] $a \mid b_i c_j$ für alle i, j. Nach der Euklidischen Verfeinerungseigenschaft aus Teil I gibt es eine Faktorisierung $a = rs$ mit $r \mid b_i$ und $s \mid c_j$ für alle $0 \le i \le m$ und $0 \le j \le n$. Also ist $r \mid b(X)$ und $s \mid c(X)$; mit anderen Worten: a ist auch primal in $R[X]$.

Aus unseren obigen Ausführungen schält sich nun folgender Satz heraus:

[13] Für Elemente $a, b, c \in R$ ist die Relation $a \mid bc$ in R gleichbedeutend mit derjenigen in $R[X]$, sodass wir zwischen $a \mid_R bc$ und $a \mid_{R[X]} bc$ nicht zu unterscheiden brauchen.

Satz 10 *Sei R ein Integritätsring. Dann sind folgende Eigenschaften äquivalent:*

1. *$R[X]$ ist Rieszsch.*
2. *In $R[X]$ gilt das Gaußsche Hebungslemma.*
3. *R ist Rieszsch und ganz abgeschlossen.*
4. *$R[X]$ ist Rieszsch und ganz abgeschlossen.*

Wegen ihrer großen Bedeutung nennt man ganz abgeschlossene Rieszsche Ringe auch Schreiersche Ringe.

Bisher haben wir bewiesen, dass (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) gilt, und selbstverständlich ist (4) $\Longrightarrow$ (1) trivial. Es bleibt also noch der "Permanenzsatz" (3) $\Longrightarrow$ (4) für die Schreier-Eigenschaft zu beweisen. Dass das Hebungslemma genau in Schreierschen Ringen gilt (dies stammt von McAdam & Rush [30]) ist also, da die andern Implikationen ziemlich naheliegend sind, im wesentlichen äquivalent zum Cohnschen Permanenzsatz (3) $\Longrightarrow$ (4) (vgl. dazu [29, Thm. 9.12]).

Es gibt einige Eigenschaften, die sich von einem Ring R auf den Polynomring $R[X]$ vererben. So ist bekannt, dass mit R auch immer $R[X]$ faktoriell ist[14]. Auch die Eigenschaft, GGT-Ring (oder ganz abgeschlossen) zu sein, überträgt sich von R auf $R[X]$. Dass sich die Eigenschaft Rieszsch nicht immer überträgt, folgt aus Prop. 7 (und einem Beispiel eines Rings, der Rieszsch, aber nicht ganz abgeschlossen ist).

Während man für den "Satz von Gauß" einige einfache Beweise kennt, scheint der Beweis von (3) $\Longrightarrow$ (4) tiefer zu liegen; da mir auch nur der Beweis Cohns[15] [6] und dessen Version von Anderson & Zafrullah[16] [1] bekannt sind, sei den Lesern daher hiermit ans Herz gelegt, sich weitere und vielleicht direktere Beweise für diesen Satz zu überlegen.

Um zu zeigen, dass $R[X]$ unter geeigneten Voraussetzungen Rieszsch ist, müssen wir aus $a \mid bc$ für Polynome $a, b, c \in R[X]$ die Existenz einer Faktorisierung $a = rs$ mit $r, s \in R[X]$ schließen, für die $r \mid b$ und $s \mid c$ gilt. In GGT-Ringen könnten wir einfach $r = \mathrm{ggT}(a, b)$ setzen; in unserem Fall geht das auch, wenn wir von $R[X]$ zum euklidischen Ring $K[X]$ übergehen, wo K der Quotientenkörper von R ist. Damit erhalten wir eine Faktorisierung $a = \rho\sigma$ mit $\rho, \sigma \in K[X]$ und $\rho \mid b$, $\sigma \mid c$ ebenfalls in $K[X]$. Um daraus eine Faktorisierung in $R[X]$ zu gewinnen, liegt es nahe, das Gaußsche Hebungslemma anzuwenden. Wir zeigen daher zuerst die Richtung (3) $\Longrightarrow$ (2) aus Satz 10:

Proposition 11 *Ist R Rieszsch und ganz abgeschlossen, so gilt in $R[X]$ das Gaußsche Hebungslemma.*

---

[14] Dieser Satz wird oft Satz von Gauß genannt, obwohl Gauß ihn weder formuliert, noch bewiesen hat. Erstmals explizit formuliert und bewiesen hat den Satz wohl erst Hensel [19], obwohl natürlich Spezialfälle wie die ZPE-Eigenschaft der Polynomringe $\mathbb{Z}[X_1, \ldots, X_n]$ bereits Kronecker bekannt waren (womöglich tauchte der Satz auch schon in Algebravorlesungen z.B. von Emil Artin und Emmy Noether auf; jedenfalls findet er sich wenig später in van der Waerdens Buch [39], das auf diesen Vorlesungen basierte). Die Bezeichnung "Satz von Gauß" rührt wohl von folgender Bemerkung van der Waerdens in [39] her: "Der hier darzustellende Beweis geht auf Gauß zurück". In der Tat führt er den Beweis des Satzes mit Hilfe des Gaußschen Lemmas).

[15] Der hier gegebene Beweis ist anders strukturiert als der Cohnsche (dieser geht den Weg über ein dem Satz von Nagata (sh. z.B. [28]) analoges Ergebnis, welches einen Zusammenhang zwischen der Schreiereigenschaft eines Rings R und seiner Lokalisierungen R_S herstellt), benutzt aber im wesentlichen dieselben Hilfsmittel: Verfeinerungseigenschaften in Rieszschen Ringen und Dedekinds Prager Satz.

[16] Ihr Beweis benutzt wie der unsere die Euklidische Verfeinerungseigenschaft.

Beweis Sei $f \in R[X]$ und $f = gh$ mit $g, h \in K[X]$. Dann existieren $b, c \in R$ mit $bg, ch \in R[X]$, und mit $a = bc$ ist $a \mid f$. Nach dem Prager Satz ist $a \mid (bg_i)(ch_j)$. Das Verfeinerungslemma gibt uns eine Faktorisierung $a = rs$ mit $r \mid bg_i$ und $s \mid ch_j$. Damit sind $G = \frac{b}{r}g$ und $H = \frac{c}{s}h$ Polynome in $R[X]$, und es gilt $f = GH$. Das war zu zeigen.

Jetzt verschärfen wir die Aussage von Lemma 6 und zeigen (2) $\Longrightarrow$ (1) aus Satz 10; da wir bereits wissen, dass aus der Gültigkeit des Gaußschen Hebungslemmas in $R[X]$ die ganze Abgeschlossenheit von R folgt, haben wir damit auch (2) $\Longrightarrow$ (4) und somit den ganzen Satz 10 bewiesen.

Proposition 12 *Gilt in $R[X]$ das Gaußsche Hebungslemma, so ist $R[X]$ Rieszsch.*

Beweis Sei $a \mid bc$, also $ad = bc$ für Polynome $a, b, c, d \in R[X]$. Da $K[X]$ ein GGT-Ring ist, gibt es Polynome $r, s, t, u \in K[X]$ mit $a = rs$, $d = tu$, sowie $b = rt$ und $c = su$. Weil in $R[X]$ das Gaußsche Hebungslemma gilt, dürfen wir r, s, t, u so um konstante Faktoren abändern, dass $r, s, t, u \in R[X]$ wird und die Gleichungen $a = rs$ und $d = tu$ erhalten bleiben. Die beiden andern Gleichungen gelten nur noch bis auf konstante Faktoren, d.h. es gibt $\alpha, \beta, \gamma, \delta \in R$ mit $\alpha b = \beta rt$ und $\gamma c = \delta su$. Multipliziert man die beiden letzten Gleichungen und beachtet $rstu = ad = bc$, so folgt $\alpha\gamma = \beta\delta$ in R. Da R nach Lemma 6 Rieszsch ist, gibt es $\rho, \sigma, \tau, \upsilon \in R$ mit $\alpha = \rho\sigma$, $\gamma = \tau\upsilon$, $\beta = \rho\tau$, und $\delta = \sigma\upsilon$. Einsetzen liefert

$$\sigma b = \tau rt, \qquad \tau c = \sigma su.$$

Bezeichnen wir die Koeffizienten der Polynome r, s, t, u mit r_i, s_i usw., so folgt aus $\sigma b = \tau rt$ und Dedekinds Prager Satz, dass $\sigma \mid \tau r_i t_j$ für alle i, j gilt. Nach der Verfeinerungseigenschaft gibt es dann eine Faktorisierung $\sigma = \sigma_\tau\sigma_r\sigma_s$ mit $\sigma_\tau \mid \tau$, $\sigma_r \mid r_i$, und $\sigma_t \mid t_j$, also auch mit $\sigma_r \mid r$ und $\sigma_t \mid t$. Ganz entsprechend folgt $\tau = \tau_r\tau_t\tau_s\tau_u$ mit $\tau_r \mid \sigma_r$, $\tau_t \mid \sigma_t$, $\tau_s \mid s$ und $\tau_u \mid u$.

Jetzt setzen wir

$$r' = \frac{\tau_r\tau_s}{\sigma_r}r, \qquad s' = \frac{\sigma_r}{\tau_r\tau_s}s, \qquad t' = \frac{\tau_t\tau_u}{\sigma_t}t, \qquad u' = \frac{\sigma_t}{\tau_t\tau_u}u.$$

Dann sind $r', s', t', u' \in R[X]$, sowie $a = rs = r's'$, $d = tu = t'u'$, $b = \frac{\tau}{\sigma}rt = r't'$ und $c = \frac{\sigma}{\tau}su = s'u'$. Damit ist der Beweis erbracht.

Es sei noch einmal darauf hingewiesen, dass ein konzeptioneller Beweis des Cohnschen Permanenzsatzes sehr willkommen wäre.

13 Andere Formen des Gaußschen Lemmas

In vielen Quellen wird das Gaußsche Lemma anders formuliert. Ist R ein Integritätsring, so nennt man ein Polynom $f \in R[X]$ *primitiv*, wenn jeder gemeinsame Teiler der Koeffizienten von f eine Einheit in R ist. Ist R ein GGT-Ring und $f(X) = f_0 + f_1X + \ldots + f_nX^n$, so nennt man $\mathrm{ct}(F) = \mathrm{ggT}(f_0, f_1, \ldots, f_n)$ den Inhalt von f. Wie Dedekind (im Falle $R = \mathbb{Z}$; sh. [9]) bemerkt hat, lässt sich das Gaußsche Hebungslemma dann wie folgt formulieren.

Lemma 13 *Ist R ein faktorieller Ring (oder auch nur ein GGT-Ring), so ist das Produkt primitiver Polynome in $R[X]$ wieder primitiv. Genauer gilt: für $f, g \in R[X]$ ist* $\mathrm{ct}(fg) = \mathrm{ct}(f)\,\mathrm{ct}(g)$.

Der Inhalt $\mathrm{ct}(f)$ von Polynomen hat die Eigenschaft $\mathrm{ct}(ag) = a\,\mathrm{ct}(g)$ für $a \in R$ und $g \in R[X]$; insbesondere folgt aus $a \mid f$ für $f \in R[X]$ immer $a \mid \mathrm{ct}(f)$.

Das Hebungslemma für GGT-Ringe ergibt sich damit so: ist $F = gh$ für Polynome $F \in R[X]$ und $gh \in K[X]$, so gibt es $a, b \in R$ mit $ag, bh \in R[X]$. Damit ist $abF = (ag)(bh)$ eine Zerlegung in $R[X]$, und es gilt $ab\,\mathrm{ct}(F) = \mathrm{ct}(ag)\,\mathrm{ct}(bh)$. Mit $r = \mathrm{ggT}(ab, \mathrm{ct}(ag))$ und $s = \frac{ab}{r}$ ist dann $ab = rs$ mit $r \mid ag$ und $s \mid bh$. Also sind $G = \frac{a}{r}g$ und $H = \frac{b}{s}h = \frac{r}{a}h$ Polynome in $R[X]$ mit $F = GH$.

Definition. Wir nennen R einen P^4-Ring (für $P^4 = PPPP$: Produkte primitiver Polynome sind primitiv), wenn das Produkt zweier primitiver Polynome in $R[X]$ wieder primitiv ist.

Wir haben gesehen, dass das Gaußsche Hebungslemma für normierte Polynome in $R[X]$ genau dann gilt, wenn R (und damit $R[X]$) ganz abgeschlossen ist, bzw. wenn auch Dedekinds Prager Satz gilt. Entsprechend gilt das Gaußsche Hebungslemma für beliebige Polynome genau in Schreierschen Ringen. Es ist auch nicht schwer zu zeigen, dass P^4-Ringe zwischen Rieszsch und AP liegen (sh. Abb. 1; tatsächlich folgt AP bereits aus der Gültigkeit des Gaußschen Lemmas für lineare Polynome). Das Gaußsche Lemma in der Form von Lemma 13 gilt schließlich genau dann, wenn R ein GGT-Ring ist.

Nun kann man in beliebigen Integritätsringen das von den Koeffizienten von f erzeugte Ideal $\mathfrak{c}(f)$ betrachten und sich fragen, unter welchen Voraussetzungen die Gleichung $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$ gilt. Die Antwort darauf gibt folgender

Satz 14 *Für einen Integritätsring R sind folgende Aussagen äquivalent:*

1. *Jedes endlich erzeugte Ideal ist projektiv.*
2. *Jedes endlich erzeugte Ideal $\neq (0)$ ist invertierbar.*
3. *Für jedes Primideal $P \neq (0)$ ist die Lokalisierung R_P ein Bewertungsring.*
4. *Jeder Ring S mit $R \subseteq S \subseteq K$, wo K der Quotientenkörper von R ist, ist ganz abgeschlossen.*
5. *Es ist $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$ für alle Polynome $f, g \in R[X]$.*

Beweis Sh. [16, Kap. IV].

Diese Version des Gaußschen Lemmas gilt also genau dann, wenn der Koeffizientenring Prüfersch ist. Prüfer selbst (sh. [33, S. 23]) hat den Satz $\mathfrak{c}(fg) = \mathfrak{c}(f)\mathfrak{c}(g)$ den "Satz von Gauß-Kronecker-Dedekind" genannt.

Zu guter letzt ...

Die Motivation zum Schreiben dieses Artikels rührt im wesentlichen von meiner Lektüre von [29] (darin geht es um das Gaußsche Hebungslemma in Schreierschen Ringen) und [32] (wo die Lücke in Euklids Beweis seiner Prop. VII.19 thematisiert wird) und dem Wunsch her, das dort gesagte ein wenig anders aufzubereiten. Weiter möchte ich Bill Dubuque für diverse postings in sci.math danken, die mir vor allem zu Anfang sehr hilfreich waren. Endlich verdanke ich Heinz Lüneburg und Klaus Volkert, sowie den beiden anonymen Referenten, noch zahlreiche nützliche und hilfreiche Bemerkungen.

Literatur

1. D.D. Anderson, M. Zafrullah, *The Schreier property and Gauss's Lemma*, Boll. Unione Mat. Ital. (8) **10** (2007), 43–62
2. T. Apostol, *Irrationality of the square root of two – a geometric proof*, Amer. Math. Monthly **107** (2000), 841–842
3. D.M. Bloom, *A one-sentence proof that square root of* 2 *is irrational*, Math. Mag. **68** (1995), 286
4. I.S. Cohen, A. Seidenberg, *Prime ideals and integral dependence*, Bull. Amer. Math. Soc. **52** (1946), 252–261
5. H. Cohn, *A second course in number theory*, New York, J. Wiley & Sons 1962; reprinted as *Advanced Number Theory*, New York, Dover 1980
6. P.M. Cohn, *Bezout rings and their subrings*, Proc. Cambridge Philos. Soc. **65** (1968) 251–264
7. Th. Coquand, *A direct proof of the Dedekind-Mertens Lemma*, preprint 2007
8. Th. Coquand, L. Ducos, H. Lombardi, C. Quitté, *L'idéal des coefficients du produit de deux polynomes*, preprint 2002
9. R. Dedekind, *Über einen arithmetischen Satz von Gauß*, Prag. Math. Ges. 1–11 (1892); Werke II, 28–38
10. R. Dedekind, *Über die Begründung der Idealtheorie*, Gött. Nachr. (1895), 106–113; Werke II, XXV., 50–58
11. R. Dedekind, *Stetigkeit und irrationale Zahlen*, Braunschweig 1872; 2nd ed. 1892; 3rd ed. 1905; 4th ed. 1912; 5th ed. 1927
12. H. Edwards, *Divisor Theory*, Birkhäuser Verlag, Boston 1990
13. N.J. Fine, *Look, Ma, no primes*, Math. Magazine **49** (1976), 249
14. K. von Fritz, *The discovery of incommensurability by Hippasus of Metapontum*, Ann. Math. (2) **46** (1945), 242–264
15. C.F. Gauß, *Disquisitiones Arithmeticae*, Leipzig 1801; deutsche Übers. durch H. Maser, Springer-Verlag Berlin, 1889;
16. R. Gilmer, *Multiplicative Ideal Theory*, Marcel Dekker, New York 1972
17. H. Hasse, *Proben mathematischer Forschung in allgemeinverstndlicher Behandlung*, Otto Salle Verlag, Frankfurt 1955
18. E. Heine, *Der Eisensteinsche Satz über die Reihen-Entwickelung algebraischer Functionen*, J. Reine Angew. Math. **45** (1853), 285–302
19. K. Hensel, *Über eindeutige Zerlegung in Primelemente*, J. Reine Angew. Math. **158** (1927), 195–198
20. D. Hilbert, *Zahlbericht*, engl. transl. (The theory of algebraic number fields) by I. Adamson, Springer-Verlag New York, 1998
21. A. Hurwitz, *Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen*, Gött. Nachr. (1895), 230–240
22. D. Kalman, R. Mena, S. Shahriari, *Variations on an irrational theme - geometry, dynamics, algebra*, Math. Mag. **70** (1997), 93–104
23. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Größen*, J. Reine Angew. Math. **92** (1882), 1–123
24. E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Göttingen 1917; reprint Chelsea 1949
25. F. Lemmermeyer, *Zur Zahlentheorie der Griechen; Teil I, Euklids Fundamentalsatz der Arithmetik*, Math. Sem.ber. **54** (2008), 1–15
26. F. Lemmermeyer, *Jacobi and Kummer's ideal numbers*, in Vorbereitung
27. F. Lemmermeyer, N. Schappacher, *Introduction to the English edition of Hilbert's Zahlbericht*, in *The theory of algebraic number fields*; Engl. transl. of [20] by I. Adamson, Springer-Verlag 1998
28. F. Lorenz, F. Lemmermeyer, *Algebra I. Körper und Galoistheorie*, 4. Aufl. Elsevier, Heidelberg 2007
29. A. Magidin, D. McKinnon, *Gauss's Lemma for number fields*, Amer. Math. Monthly **12** (2005), 385–416
30. S. McAdam, D.E. Rush, *Schreier rings*, Bull. London Math. Soc. **10** (1978), 77–80
31. F. Mertens, *Über einen algebraischen Satz*, Sitz.ber. Akad. Wiss. Wien **101** (1892), 1560–1566
32. D. Pengelley, F. Richman, *Did Euclid need the Euclidean algorithm to prove unique factorization?*, Amer. Math. Monthly, 113 (2006), 196–205

33. Prüfer, *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, J. Reine angew. Math. **168** (1932), 1 – 36
34. Y. Sagher, *What Pythagoras could have done*, Amer. Math. Monthly **95** (1998), 117
35. W. Scharlau, *Who is Alexander Grothendieck? Anarchy, mathematics, spirituality*, Havixbeck 2007
36. W. Strobl, *Historische und systematische Entwicklung der arithmetischen Theorie der algebraischen Funktionen von Dedekind und Weber* (span.), Tesis de licenciatura Univ. Madrid, 1980
37. J. Suranyi, *Schon die alten Griechen haben das gewusst*, in *Grosse Augenblicke aus der Geschichte der Mathematik*, BI Mannheim 1991
38. H.E. Vaughan, *On the irrationality of roots*, Amer. Math. Monthly **67** (1960), 576–578
39. B. van der Waerden, *Moderne Algebra*, Springer-Verlag Berlin, 1930
40. W.C. Waterhouse, *Why square roots are irrational*, Amer. Math. Monthly **93** (1986), 213–214