Teilbarkeitstheorie

Im Folgenden sei R stets ein Integritätsring mit 1.

Teilbarkeit
Hat man in R eine Gleichung der Form $a=bc$, so nennt man b einen **Teiler** von a und schreibt b/a. Einen Teiler der 1 nennt man eine **Einheit**. Einheiten sind also genau die Elemente, die ein Inverses bezüglich der Multiplikation besitzen. Die Einheiten in R bilden eine Gruppe bezüglich der Multiplikation. Ist e eine Einheit und gilt $ae=b$, so nennen wir a und b **assoziiert**. Assoziiertheit ist eine Äquivalenzrelation. Eine Einheit ist Teiler jedes Ringelements. Alle Ringelemente sind Teiler von 0[1]. Ein Teiler von a teilt auch jedes zu a assoziierte Element.

Ein Element $e \in R$ ist genau dann eine Einheit, wenn das von e erzeugte Ideal der gesamte Ring ist, wenn also $<e>=R$

Es gilt a/b genau dann, wenn $<b> \subset <a>$.
a,b sind assoziiert genau dann, wenn $<b>=<a>$

Ist $a=bc,$ so nennt man b einen **echten** Teiler von a, wenn weder b noch c Einheiten sind.
b ist genau dann echter Teiler von a, wenn die Inklusion $<a> \subset <b>$ eine echte ist.

Sind $a\,, b \in R$, so heißt $d \in R$ **größter gemeinsamer Teiler** von a und b, wenn gilt
d/a und d/b und $\forall\, c \in R : c \mid a$ und $c \mid b \Rightarrow c \mid d$.

Ist d größter gemeinsamer Teiler von a und b, so ist c genau dann ebenfalls größter gemeinsamer Teiler von a,b, wenn c und d assoziiert sind. Schreibt man ggT(a,b) für einen größten gemeinsamen Teiler von a und b, so ist zu beachten, daß dieser höchstens bis auf Assoziiertheit bestimmt ist.

In einem Hauptidealring haben zwei Elemente a,b immer einen größten gemeinsamen Teiler, und zwar einen Erzeuger des Ideals $<a,b>$.
In einem Euklidischen Ring kann man mit dem Euklidischen Algorithmus einen größten gemeinsamen Teiler berechnen.

Zwei Elemente $a\,, b \in R$ heißen **teilerfremd**, wenn 1 größter gemeinsamer Teiler von a und b ist, oder auch, wenn der größte gemeinsame Teiler eine Einheit ist. Dies ist offenbar genau dann der Fall, wenn das Ideal $<a, b>$ der ganze Ring ist, und dies ist genau dann der Fall, wenn es eine Lösung der Gleichung $xa+yb=1$ gibt mit geeigneten Ringelementen x,y. In einem euklidischen Ring liefert der Erweiterte Euklidische Algorithmus sofort eine Lösung dieser Gleichung.

Eine Nicht-Einheit $a \in R$ heißt **unzerlegbar**, wenn es kein Produkt der Form $a = bc$ gibt, wobei $b\,, c \in R$ beides keine Einheiten sind.
Eine Nicht-Einheit heißt **zerlegbar**, wenn sie nicht unzerlegbar ist.
Eine Nicht-Einheit ist genau dann unzerlegbar, wenn sie keinen echten Teiler besitzt.
Eine Nicht-Einheit a genau dann unzerlegbar, wenn es kein echt größeres Hauptideal als $<a>$ gibt.
Ist a unzerlegbar und e eine Einheit, so ist auch ae unzerlegbar.
Sind a,b unzerlegbar so gilt: a/b genau dann wenn b/a genau dann wenn a, b assoziiert.

1 "Teiler von 0" ist nicht dasselbe wie "Nullteiler". Ein Nullteiler ist ein von 0 verschiedenes Element a zu dem es ein von 0 verschiedenes Element b gibt mit ab=0. Ein Integritätsring ist definitionsgemäß nullteilerfrei.

Satz über Faktorzerlegung in unzerlegbare Elemente
In einem noetherschen Integritätsring[2] R ist jede Nicht-Einheit entweder unzerlegbar oder läßt sich als Produkt unzerlegbarer Elemente schreiben.

Beweis für euklidischen Ring:
Sonst gäbe es eine Nichteinheit a kleinster Norm, welches weder unzerlegbar ist noch sich als Produkt unzerlegbarer Elemente schreiben läßt. Weil a zerlegbar ist, gibt es eine Darstellung $a=bc$ mit Nichteinheiten b,c , also $N(a)=N(b)N(c)$ und $N(b)>1$ und $N(c)>1$, daher $N(b)<N(a)$ und $N(c)<N(a)$. Aufgrund der minimalen Wahl von a sind dann b und c unzerlegbar oder als Produkte unzerlegbarer Elemente darstellbar. Damit ist jedenfalls auch $a=bc$ als ein Produkt unzerlegbarer Elemente darstellbar.

Beweis für noetherschen Integritätsring.
Eine Nichteinheit $a=a_0$, welche weder unzerlegbar ist, noch sich als Produkt unzerlegbarer Elemente schreiben läßt, besitzt eine Darstellung $a_0=a_1\cdot b_1$ als Produkt von Nichteinheiten, wobei a_1 sich ebenfalls nicht als Produkt unzerlegbarer Elemente schreiben läßt. Jetzt erhält man rekursiv Nichteinheiten a_n , wobei jeweils a_{n+1} echter Teiler von a_n ist. Man hat also eine aufsteigende Idealkette $<a_0>\subset<a_1>\subset\ldots\subset<a_n>\subset\ldots$, welche in einem noetherschen Ring stationär werden muß. Irgendwann ist also a_{n+1} nicht mehr echter Teiler von a_n , im Widerspruch zur Konstruktion.

Eine Darstellung als Produkt unzerlebarer Elemente ist nicht unbedingt eindeutig.
Im Ring $R=\left\{a+ib\sqrt{5}\mid a,b\in\mathbb{Z}\right\}$ hat man nämlich mit $6=2\cdot3=(1+i\sqrt{5})(1-i\sqrt{5})$ zwei verschiedene Zerlegungen des Elements 6 in unzerlegbare Elemente[3].

Um zu einer Eindeutigkeitsaussage für Produktzerlegungen in unzerlegbare Faktoren zu kommen, benötigen wir den Begriff des **Primelements**:

Eine Nicht-Einheit p in R heißt prim, wenn aus p / ab folgt: p/a oder p/b.
D.h. wenn ein Primelement ein Produkt teilt, dann teilt es mindestens einen der Faktoren.

Es sind nun grundsätzlich Primelemente auch unzerlegbar:
Ist nämlich p prim und $p=ab$, und oBdA p/a, also $pc=a$, so folgt $pcb=ab=p$. Im Integritätsring R können wir kürzen und erhalten $cb=1$, also ist b eine Einheit. Es gibt also keine Produktzerlegung von p in Nicht-Einheiten, also ist p unzerlegbar.

In einem Hauptidealring sind unzerlegbare Elemente auch prim:
Sei nämlich p unzerlegbar und p teile das Produkt ab. Nehmen wir an, p teile nicht b. Dann liegt b nicht in $<p>$. Also ist das Ideal $<b,p>$ echt größer als das Ideal $<p>$. Weil R Hauptidealring ist, gibt es ein $c\in R$ mit $<c>=<b,p>$. Also gibt es ein d mit $p=cd$. Wegen der Unzerlegbarkeit von p ist c oder d eine Einheit.
Ist d eine Einheit, so sind p und c assoziiert, also ist $<p>=<c>=<p,b>$. Dann läge b aber im von p erzeugten Ideal, also wäre p doch ein Teiler von b. Also ist d keine Einheit und daher c eine Einheit.
Weil $c\in<b,p>$ gibt es $r,s\in R$ mit $c=rb+sp$. Wir multiplizieren mit a und haben $ac=rab+spa$.
Also folgt p/ac und damit p/a, w.z.b.w.

Satz über die eindeutige Primfaktorzerlegung

2 Ein noetherscher Ring ist dadurch charakterisiert, daß jede aufsteigende Folge von Idealen stationär wird. Ein Hauptidealring ist automatisch noethersch, also auch ein Euklidischer Ring.

3 Dieser Ring ist ein Unterring von $\mathbb{C}$. Daher hat man die multiplikative Normfunktion $N(z)=z\bar{z}$, mit deren Hilfe man die Unzerlegbarkeit von $2,3,1+i\sqrt{5}$ und $1-i\sqrt{5}$ leicht nachweist.

Existenz
In einem Integritätsring mit 1, in dem die unzerlegbaren Elemente prim sind, läßt sich jede Nichteinheit schreiben in der Form $a_1 \cdot \ldots \cdot a_n$, mit unzerlegbaren Faktoren $a_1, \ldots, a_n$.

Eindeutigkeit
Ist $b_1 \cdot \ldots \cdot b_m$ eine andere Darstellung desselben Elements, so ist $m=n$ und die Faktoren b_i lassen sich so umordnen, daß für alle i gilt: a_i und b_i sind assoziiert.

Die Existenz einer solchen Zerlegung hatten wir oben schon für einen beliebigen noetherschen Integritätsring.

Die Eindeutigkeitsaussage ergibt sich indirekt so:
Nehmen wir zunächst an, es gäbe eine Gleichung $a_1 \cdot \ldots \cdot a_n = b_1 \cdot \ldots \cdot b_m$ mit Primelementen und $1 \le n < m$. Dann gäbe es auch eine solche Darstellung mit minimalem m.
Wäre dabei n=1, so hätte man $a_1 = b_1 \cdot \ldots \cdot b_m$. a_1 ist Teiler des Produkts rechts, teilt also einen der Faktoren. Nach Umordnung der Faktoren können wir annehmen, daß a_1 Teiler von b_1 ist. Aus der Primalität von b_1 folgt, daß dann auch $b_1 T$ eiler von a_1 ist, so daß a_1 und b_1 assoziiert sein müssen. Also $b_1 = e a_1$ mit einer Einheit e. Kürzen ergibt $1 = e\, b_2 \cdot \ldots b_m$. Dies bedeutet, daß alle Elemente rechts Einheiten sind. b_2 als Primelement ist aber keine Einheit. Also tritt dieser Fall nicht auf.
Wäre n>1, so führt dasselbe Argument zur Gleichung $a_2 \cdot \ldots \cdot a_n = (eb_2) \cdot b_3 \cdot \ldots \cdot b_m$. Man beachte, daß auch eb_2 ein Primelement ist. Damit haben wir eine Gleichung zwischen Primprodukten von verkürzter Länge, was der Minimalitätsbedingung in der Ausgangsgleichung widerspricht.

Also können wir davon ausgehen, daß $n=m$. Es muß jetzt gezeigt werden, daß die geforderte Umordnungsmöglichkeit existiert. Dies geschieht durch Induktion:

Der Fall n=1 sofort klar, da man dann die Gleichung $a_1 = b_1$ hat.
Ist n>1, so hat geht man aus von $a_1 \cdot \ldots \cdot a_n = b_1 \cdot \ldots \cdot b_n$. Wie vorher ordnen wir die b_i um, so daß anschließend a_1 / b_1 und daher $b_1 = e\, a_1$. Dann kann wieder gekürzt werden zu $a_2 \cdot \ldots \cdot a_n = (eb_2) \cdot \ldots \cdot b_n$. Da wir jetzt als n-1 Faktoren haben, haben wir als Induktionsvoraussetzung, daß eine Umordnung der rechten Seite existiert, so daß für alle i mit $2 \le i \le n$ die a_i und b_i assoziiert sind. Zusammen mit der vorherigen Umordnung von $b_1, \ldots, b_n$, welche den zu a_1 assoziierten Faktor nach vorn brachte, ergibt sich die Aussage des Satzes.

Ein **faktorieller Ring** ist ein Integritätsring mit 1, in dem unzerlegbare Elemente prim sind und in dem daher der Satz von der eindeutigen Primfaktorzerlegung gilt.

In einem faktoriellen Ring besitzen zwei Ringelemente immer einen größten gemeinsamen Teiler:
Mit dem Auswahlaxiom beschaffen wir uns eine Teilmenge P aller Primelemente mit folgenden Eigenschaften:

1. zu jedem Primelement in R gibt es ein assoziiertes Element in P.
2. zwei verschiedene Elemente von P sind nicht assoziiert.

Man zeigt jetzt leicht, daß sich jedes von Null verschiedene Element $a \in R$ eindeutig so schreiben läßt:

$$a = e \prod_{p \in P} p^{\alpha_p}$$ wobei e Einheit, $\alpha_p \in \mathbb{N}_0$ und nur endlich viele $\alpha_p \neq 0$.

Hat man nun $b = f \prod_{p \in P} p^{\beta_p}$, so ist $c = \prod_{p \in P} p^{\gamma_p}$ mit $\gamma_p = \min\{\alpha_p, \beta_p\}$ größter gemeinsamer Teiler von *a* und *b*.

Unsere Definitionen sind so gefaßt, daß ein faktorieller Ring jedenfalls Integritätsring ist.
Nun sind aber endliche Integritätsringe Körper, und in diesen ist Teilbarkeitstheorie und Idealtheorie uninteressant bzw. trivial.

Wir betrachten also nur unendliche faktorielle Ringe.
In diesen gibt es unendlich viele "verschiedene", Primelemente! Dies zeigt man am einfachsten mit einem Beweis von **Euklid**:

Betrachten wir dazu die Menge *M* der Äquivalenzklassen assozieerter Primelemente. Wäre *M* endlich so könnten wir Elemente $p_1, \ldots, p_n$ aus jeder der *n* Äquivalenzklassen nehmen und $p_1 \cdot \ldots \cdot p_n + 1$ bilden. Dieses Element ist keine Einheit. Daher muß in seiner Primfaktorzerlegung eines der p_i auftauchen. Aber kein p_i ist Teiler von $p_1 \cdot \ldots \cdot p_n + 1$, Widerspruch!